ID: 481120
Sample Name:
MGrYFpGLQ7.dll
Cookbook: default.jbs
Time: 11:32:24
Date: 10/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

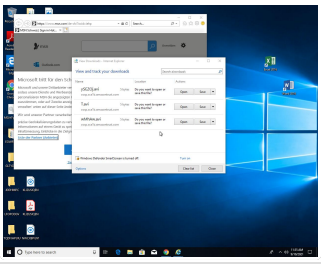
Windows Analysis Report MGrYFpGLQ7.dll

Overview

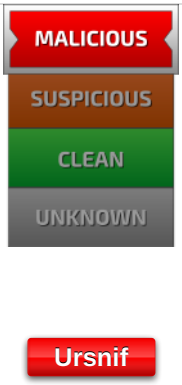
General Information

Sample Name:	MGrYFpGLQ7.dll
Analysis ID:	481120
MD5:	8c7b2ff10596371..
SHA1:	831ece0ae6b5e2..
SHA256:	90d8648b2aac0c..
Infos:	

Most interesting Screenshot:



Detection

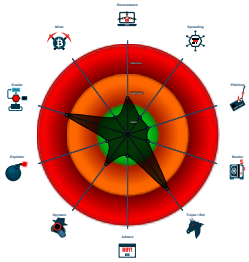


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Found stalling execution ending in A…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Machine Learning detection for samp…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- PE file contains an invalid checksum
- Tries to load missing DLLs
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2880 cmdline: loaddll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3428 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5040 cmdline: rundll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 3556 cmdline: regsvr32.exe /s C:\Users\user\Desktop\MGrYFpGLQ7.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 4728 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 2576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6320 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6424 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6432 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82954 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 7140 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82976 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1256 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17438 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6396 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:83004 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5144 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17452 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5704 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:83036 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6020 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17470 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 2624 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Bighearted MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5352 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Soaking MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6276 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Turnipy MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6536 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Watertight MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6708 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Dithery MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7000 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Anhimae MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1496 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Anostraca MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2964 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1068 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Anaerobian MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6372 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Sparsile MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5908 cmdline: rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,DllUnregisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Copyright Joe Security LLC 2021

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000003.355232631.0000000007528000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000010.00000003.314377890.0000000006878000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.391622099.0000000003138000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000010.00000003.314521084.0000000006878000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000015.00000003.355592572.0000000007528000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 86 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Copyright Joe Security LLC 2021

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Malware Analysis System Evasion:

Found stalling execution ending in API Sleep call

Stealing of Sensitive Information:

Yara detected Ursnif

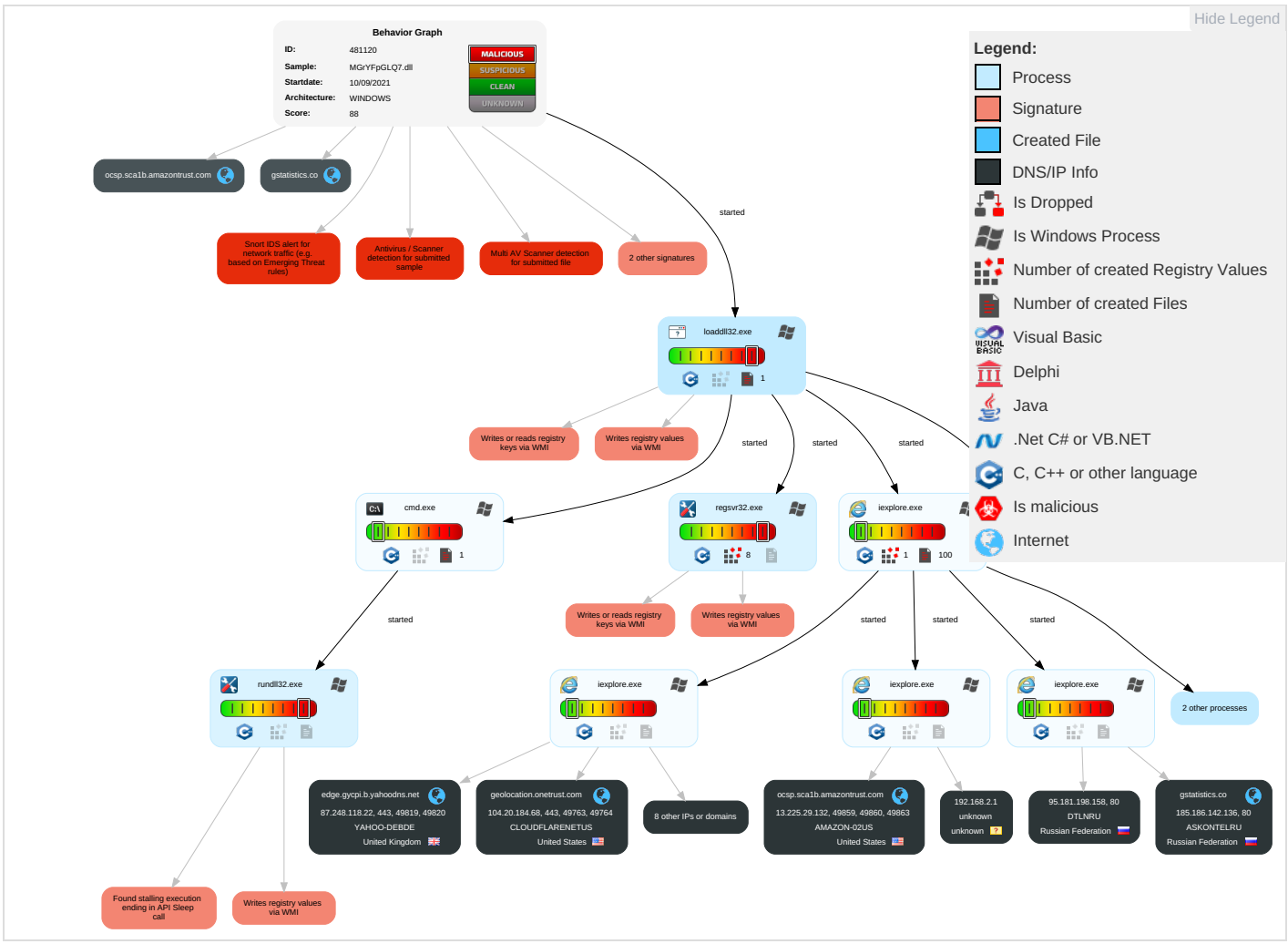
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdr Insecure Network Commur
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

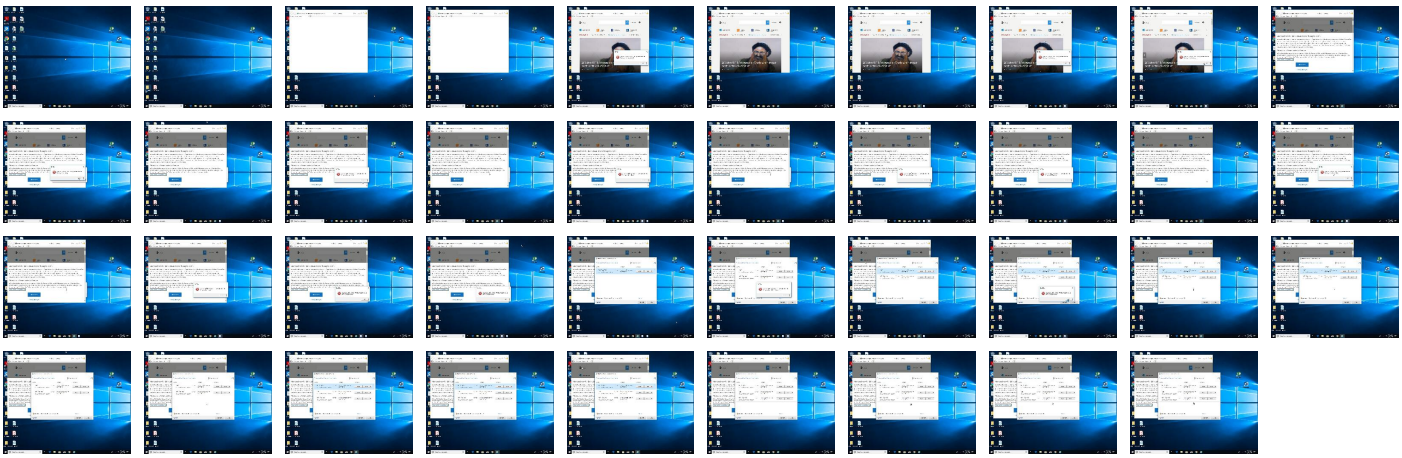
Behavior Graph

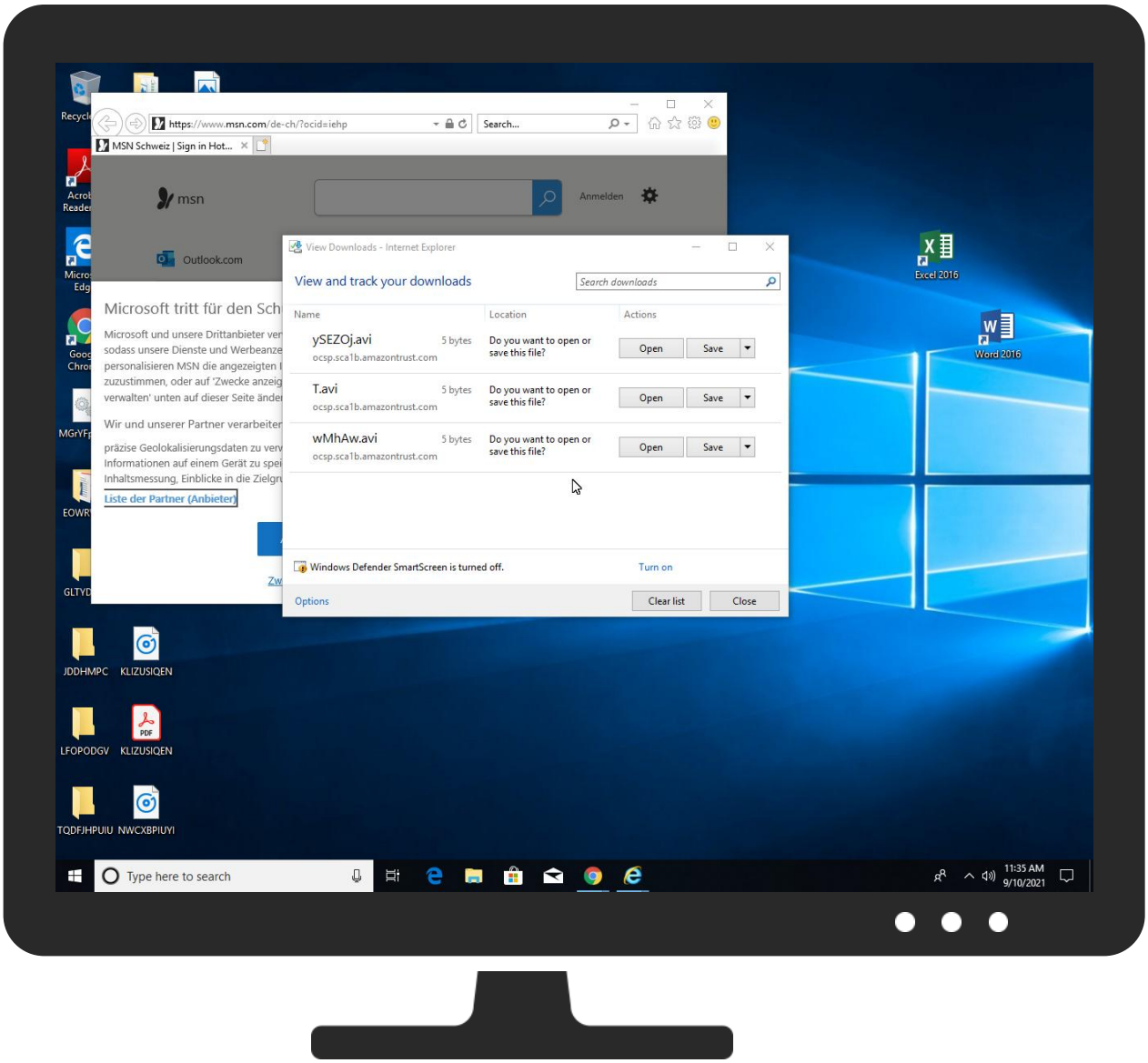


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MGrYFpGLQ7.dll	82%	Virustotal		Browse
MGrYFpGLQ7.dll	59%	Metadefender		Browse
MGrYFpGLQ7.dll	89%	ReversingLabs	Win32.Ransomware.Sodinokibi	
MGrYFpGLQ7.dll	100%	Avira	TR/AD.Ursnif.olrue	
MGrYFpGLQ7.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.1.rundll32.exe.510000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.rundll32.exe.4350000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.1.loaddll32.exe.5f0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.510000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
2.2.regsvr32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
21.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.rundll32.exe.4ca0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
18.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.regsvr32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.loaddll32.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.1.rundll32.exe.8f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.4080000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
12.2.rundll32.exe.4c00000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
21.2.rundll32.exe.4fd0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.47b0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
9.2.rundll32.exe.4bf0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.1.rundll32.exe.510000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.rundll32.exe.6770000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.c70000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.1.loaddll32.exe.5f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.1.rundll32.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.regsvr32.exe.3180000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
16.1.rundll32.exe.8f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sca1b.amazontrust.com/images/GCf_2BVR4BU/cjyHO8rEu0PLMD/ddrHkS9VDXWI2BqJDWdKp/yP_2BPG48oRDpm0g/SrPkMCydca7dHbV/D9P1tAQMBBq8SvLL_2/BTpaf4v7U/VLIzcVH0j4WxrbYHQOZI/wYP1aj2dECCu_2F_2BC/mIwNPWeBCD7IMCmF8HTTO6/vdW_2F0_2BicH/w8p9PjDD/HtrueVxg_2FcH01kfOOydSo/XvV_2FKbIAaOsHpHpe/wMhAw.avi	0%	Avira URL Cloud	safe	
http://ocsp.sca1b.amazontrust.com/images/GosV5rx1jUm_2/FeMYZexn/3AHfZUbwKtZ24NdOcSq0RlX/SFVlCboKYZ/q19iLR0UiFTMXXHua/7HDwQVQwW_2B/P2MZpE_2Fn2/TKqFG_2F5mAVKf/ACPvjzozYdfDpfYzdrt73/e9vTiEyeXLfMugv6/YOqbGPGETO_2FyR/6XOvuQnB29hcTxcqfB/1cP6Y9M6Q/pKhEyMS_2BB/ySEZOj.avi	0%	Avira URL Cloud	safe	
http://ocsp.sca1b.amazontrust.com/images/U6TeZm2GqJwloJv5oZSeI/2t0wwSFx0OdeCqwq/a5th_2BJswZzpBo/iTJZVc_2BHgWPPB64R/K3cCyKXGA/pha07BC_2FbaaosXoWHU/mqeKc0qKA2IsvzCoLJ0/i_2FxmVXC6GOzmCalRHRBS/X4qBHSkzHz0Gv/sQEy9HR7/NTPicd5UJLmarL1TQsRZspC/zIbC4QSojh/SXfsKqnthINSBZ4Hv/INUqZbTg0z/T.avi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
ocsp.sca1b.amazontrust.com	13.225.29.132	true	false		high
gstatistics.co	185.186.142.136	true	false		high
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		high
s.yimg.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Copyright Joe Security LLC 2021

Name	Malicious	Antivirus Detection	Reputation
http://ocsp.sca1b.amazontrust.com/images/GCf_2BVR4BU/cjyHO8rEu0PLMD/ddrHkS9VDXWI2BqJDWdKp/yP_2BPG48oRDpm0g/SrPkMCydca7dHbV/D9P1tAQMBBq8SvLL_2/BTpaf4v7U/VLIzcVH0j4WxrbYHQOZI/wYP1aj2dECCu_2F_2BC/mIwNPWeBCD7IMCmF8HTTO6/vdW_2F0_2BicH/w8p9PjDD/HtrueVxg_2FcH01kfOOydSo/XvV_2FKbIAaOsHpHpe/wMhAw.avi	true	• Avira URL Cloud: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://ocsp.sca1b.amazontrust.com/images/GosV5rx1jUm_2/FeMYZexn/3AHfZUbwKtZ24NdOcSq0RIX/SFVlCboKYZ/q19iLR0UiFTMXXHua/7HDwQVQwW_2B/P2MZpE_2Fn2/TKqFG_2F5mAVKf/ACPvjzozYdfDpfYzdrt73/e9vTiEyeXLfMugv6/YOqbGPGETO_2FyR/6XOvuQnB29hcTxcqfB/1cP6Y9M6Q/pKhEyMS_2BB/ySEZOj.avi	true	• Avira URL Cloud: safe	unknown
http://https://s.yimg.com/lo/api/res/1.2/BWUYr.M5U6.kf035wsX8Lg--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1621266752856-586.jpg	false		high
http://ocsp.sca1b.amazontrust.com/images/U6TeZm2GqJwloJv5oZSeI/2t0wwSFx0OdeCqwq/a5th_2BJswZzpBo/iTJZVc_2BHgWPPB64R/K3cCyKXGA/pha07BC_2FbaaosXoWHU/mqeKc0qKA2IsvzCoLJ0/i_2FxmVXC6GOzmCalRHRBS/X4qBHSkzHz0Gv/sQEy9HR7/NTPicd5UJLmarL1TQsRZspC/zIbC4QSojh/SXfsKqnthINSBZ4Hv/INUqZbTg0z/T.avi	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.29.132	ocsp.sca1b.amazontrust.com	United States		16509	AMAZON-02US	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
95.181.198.158	unknown	Russian Federation		49063	DTLNRU	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
185.186.142.136	gstatistics.co	Russian Federation		204490	ASKONTELRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	481120
Start date:	10.09.2021
Start time:	11:32:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MGrYFpGLQ7.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	46
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:	mal88.troj.evad.winDLL@51/187@14/6

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 74.4% (good quality ratio 69.8%) • Quality average: 78.1% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1979
Entropy (8bit):	4.894078869642119
Encrypted:	false
SSDEEP:	48:LuFsuFsuFFFsuFsuFsuFscFscFvFscFscFyFscFsDFsDFsDFsDFsDFsDFigFsDFigFc:CFnFnFFFnFnFnFhFhFvFhFhFyFhFaFag
MD5:	100B5B5D096FAFBA765C2A1E1FC7B857
SHA1:	66BEE5C30860054D3B1446DD31A41301AFC09A00
SHA-256:	63FF314364FB7EC101777E5C8AD757FD5E7376D6DFF2C60AC031524EA03204B0
SHA-512:	39760EC31E4851D3C7CB30BD03FCCA1506D068770170B0C7E78667A97F65F3089B2F86626AD475FEA6CA5791C679E6A34EB0304AC36F4604CF90D34FF8F6FC5I
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="1589958464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="15899 58464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1589958464" htime="30910066" /><item name="mntest" value="mntest" ltim e="1589958464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1589958464" htime="30910066" /></root><root><item name="HBCM_B IDS" value="{}" ltime="1589958464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1589958464" htime="30910066" /></root><root> <item name="HBCM_BIDS" value="{}" ltime="1590958464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1590958464" htime="309 10066" /><item name="mntest" value="mntest" ltime="1590958464" htime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1590958464" ht ime="30910066" /></root><root><item name="HBCM_BIDS" value="{}" ltime="1590958464" htime="30910066"

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{97212EC2-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	548952
Entropy (8bit):	2.912295206751126
Encrypted:	false
SSDEEP:	768:sqvpzeb3kq+X2RQjD92J5OBDePxXzQ5RMnGp79lduoBhIC9zz51D4qMt34RR5e3G:x
MD5:	8F07F7E2E7034239D814BFC7E1AA0D83
SHA1:	6F0BBC545FEA3CF38BB8262C8F97D44F413B6CCE
SHA-256:	21999DAA2DF2972E522EFAC6A10387FD21EB90873EC087DB25565BA7E5061EE5
SHA-512:	789837447FB127598E3FCA6AD8CB55B1F9A76CCC1ECE6187BA6A7DE0F56BB7DC72075DDAFCB7A64AA72DBAA33C77E0940481E9CC6E98E635EF1B3EFD02CD C02
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{97212EC4-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	364456
Entropy (8bit):	3.6287170988625705
Encrypted:	false
SSDEEP:	3072:pZ/2Bfcdmu5kgTzGtUZ/2Bfc+mu5kgTzGtYZ/2Bfcdmu5kgTzGtYZ/2Bfc+mu5kE:wjyXl
MD5:	6E0E237D75EC5461E223CCD3747F1F70
SHA1:	CB49F7C24F0382D8FD9A1945DC0C02CA835EC2AA
SHA-256:	4F2D1F6945031D80459E94C8CBE93EFBE78E58B688055998D142C4D9136A2479
SHA-512:	A08646A03646074DC1B83274D360A1003172E91F5716E5E0EC25C5F77B259018F7E92CF204C552F0A6F92F1C8ED1940DB5FCB44272D3C6FFAEFE0860F6F44698
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{97212EC6-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{97212EC6-1265-11EC-90E5-ECF4BB570DC9}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27388
Entropy (8bit):	1.8496200615655867
Encrypted:	false
SSDEEP:	192:rXZ4QK6Ukzbjx2ASWgM8OPt4bRPt4etpA:rJh15zHgAR13yu
MD5:	05A9FBD89AD410559088153DF793E95A
SHA1:	F8A04B0DBE00428C2558682F105D794345F6ABBD
SHA-256:	E5931A09C796A8EE5C43790086492931D3FB8E7D4158570230CD9B5CE47EB567
SHA-512:	A640FA0BDA487E3EBAC12EE00820B6A1C43EBF9142BD2043801F01D1EFAD33225D34525CCCA24629C3E0856C65ECCBC0819C04A9185AA80A6A26E418AA07B9F4
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{97212EC8-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27216
Entropy (8bit):	1.8581390295123945
Encrypted:	false
SSDEEP:	96:rVZ2Qi6YBSa0j52xW6MCaado70xedo7jA:rVZ2Qi6YkPj52xW6MCaad1xedmA
MD5:	D081FCF7713E9A1824B1C626DC5F3254
SHA1:	BD57F9302A70F5B53D8F11C3FE88EA9B0C508D57
SHA-256:	EE66B9F80615ECDA6B02D9911E5FEBB5AB3404AF87E116E76D46BE4C77D1E9DE
SHA-512:	0DDAD44B30A2FC016B904395D63167728BA6FADF6258766CC78B8E8E1A831ECBAB98D566FB4F838D372327F70FBF6488214EAA9265947FD4A16B720E89C0844
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D2B8B4E-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5754670009647667
Encrypted:	false
SSDEEP:	48:IwtGcproGwpacG4pQIGrapbSxGQpB2GHHpcAVTGUpG:rzZwQ86WBSLj12AXA
MD5:	AB5683FC22D2315C1F43020D2895D880
SHA1:	87DFC73F1575C047697623483E0AAB7F5FAE62B6
SHA-256:	A4ACF6C0F085C9E0DDFCBDA7E22D483A0085D35B3C15F659AB7996A6A7036225
SHA-512:	8655CDD4337C31B5A0EFBC672177C8A6C19474ABA9A3630F64D8183620D548AC5425B3ED3075AC90CA06D6BDA0C41A0BBFF613C48AF3A21593E90328D705656
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D2B8B50-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27456
Entropy (8bit):	1.8692190494520904
Encrypted:	false
SSDEEP:	96:r9ZeQm68BSejR2RW+M6KPYDCx2PYDC0qA:r9ZeQm68kejR2RW+M6KQmx2QmdA
MD5:	C547AFE53F9D75140BF42C9B8017A4FA

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D2B8B50-1265-11EC-90E5-ECF4BB570DC9}.dat	
SHA1:	DCB4091076C3A35E4EE495CFF4280E71C9C4D5C0
SHA-256:	285C45598BB5EB06C8E030F6367AA55F1E24BFDFFD68A99757DE9D3BF87456DF
SHA-512:	346BDCF20A63E7E2319634F306E8C60EC3E47F4A4D07225BCF06A6E5ED889C3B54518DE8DA90D9A562DCDC4FE0F9446F3EA538D0EFA2DF6D5F56C7836F1E63A5
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A40F3351-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5730104268086544
Encrypted:	false
SSDEEP:	48:IwMGcprxGwpaY0G4pQ+mGrapbSktGQpBGGHHpcjTGUpG:rQZrQYE6+oBS0jF29A
MD5:	FDA040A48E80BB91E6E03095E6FA99B1
SHA1:	322C58A60BDF317CEE5C8CDF775BBEFBD68B779A
SHA-256:	BF6A987A4010E3750ADB12F6652D8E5ED20F89AF19C0018324CE66D9177092D6
SHA-512:	A319F1B517BFD5F9CA3E171CFCEB0C6A4ADB52788B28B12137C03D2E81B99578BC37E694C9682D5972BEDC2291AAE96A2B03FB2E5971D2FB6F7B019712F4826
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A40F3353-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.851425793435613
Encrypted:	false
SSDEEP:	96:rmZlQR6C0BSkjh21W8M3KEGZ7xqMREGZ7xq0GZJA:rmZlQR6C0kkjh21W8M3KL74MRL74bJA
MD5:	39517137A4D08785B85BC823B916EFBA
SHA1:	C7C77E6A96F89C12333E0C956EDDF3675BF53AED
SHA-256:	9A5CC18009E19F3047058DE44EDF67D6985DE52904A5C877BC8C43B53B67D80C
SHA-512:	AAB5D6784262D3C5134B59ADF3C90E9483C2F731E3B6FA4DFDF6F15D9F009296BE01BE6514C5D32C6BFA8C90E61FA511BEE1CA72C9DF969AC43939BDB8116F07
Malicious:	false
Reputation:	unknown
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A40F3355-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24632
Entropy (8bit):	1.7253076886306955
Encrypted:	false
SSDEEP:	48:IwmGcpr/GwpaDG4pQnGrapbSXGQpBKGHHpckQTGUp8kpGGzYpmklQFGopwWlYYYa:r6ZJQ167BShjR2BW5MByjYr4Dg
MD5:	6AB092D3A42B4F044F7C46CB9EC60610
SHA1:	68A89971B446E145567C932D48FFCAE52944E672
SHA-256:	0C6718229D1A44EFF1366819C57F9BA1CC4C3CCA39203D80F8AAC73F95AECE34
SHA-512:	D54D91755A4DB9C311720FB5266F9816617289A6480FFC1D3228B68B4D19C1FCF5D8EAEACFCC6164D3CDA3BE34F267E6B27E0AD8595A2DCD0A6849BA3565043
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A40F3355-1265-11EC-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A40F3357-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8489960886864234
Encrypted:	false
SSDEEP:	48:Iw5GcprMGwpanG4pQnGrapbS+GQpBOGHHpcDTGUp8sGzYpmk3Gopw+7+xoVKmQoN:rfZkQJ67BSWjd2dW4M4yGVKXRGVKhxA
MD5:	CBB501CB3A3718EEAC50366B0BCD043F
SHA1:	19443A5F4B88F87C840B51485AC13F1861E35388
SHA-256:	D9778604E6C9A2A78B1C0CD4A870FC0512E874C06F13F7F08B7B8A02BCBDEE3D
SHA-512:	B4B633DDE5A02CDF04D55AD82642424122D64F489E0DB57BEE3079C3DEEFDA8E702BDF7B3456F419216B02993B59B63AD92281914808C40DA21FBF1B957448A
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A67-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5693511883858517
Encrypted:	false
SSDEEP:	48:IwPGcpriGwpa2G4pQWGrapbS6GQpBqGHHpczTGUpG:rFZKQG6YBSCjx2NA
MD5:	8BC960261C70FC42240DDA8DA39B3AA2
SHA1:	4936AE23EDB269DDACDDF401A2F3795AA1039194
SHA-256:	9757CA569D046D6CBFC001B254CB21375DE24A5C460ECA81AFFA3025312D3E7E
SHA-512:	AACC0068F076AA4BCCB2A0BE9D874B7841A4B3FE436FEE848F9B14E4612FB6265E6EDBB2A8ED4EA13A0796AA770E61CD4BB93DD5844EB3A12993F447FA7262C6
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A69-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27444
Entropy (8bit):	1.8669764177537533
Encrypted:	false
SSDEEP:	96:rrZ8QM62BSWj92tWiM6W33VyNOx33Vyn3QNA:rrZ8QM62kWj92tWiM6W3FSOx3FUgNA
MD5:	F6C26927851D3856A2C32670DEC831B3
SHA1:	A5C17925E630BFA922EEDAA3703C0962F3DDC762
SHA-256:	68AAC5753A75797B2F7E2AA65770F0762235C07077DB66A7FA3D735402DC280D
SHA-512:	7EDAFA1486345846AE1D20CEFAB207B6CDD62F9C3C135F306F3ECA7C2F0CD25D69A68C360948C683237A750084171465252D6A5BCE2BB55E066FB0A178013D0
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A6A-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A6A-1265-11EC-90E5-ECF4BB570DC9}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5832873970840036
Encrypted:	false
SSDEEP:	48:IwPGcpryGwpaXG4pQXGrapbSwGQpKKG7HpRETGIpX20GApm:rFZ6QZ6rBS4AlTAFrg
MD5:	406105571938AF78DA4A542934F2C0AF
SHA1:	5727254801FC20C634B0D596F04ED544886E8DAA
SHA-256:	9A39162B37C0F38F5BF62633FB3FB213475EE322E9889DD95E203D354AAE9A9A
SHA-512:	AC8B7792579D5B66C745C17E67015CF55ABD7D4D34276770E1740C03A9EB10F094E325C39A4C5601695F6611CD1C510C01A3A090362E56CD201B548BBD92ADC
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A6C-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5739616130679477
Encrypted:	false
SSDEEP:	48:Iw5GcprQGwpaR7G4pQpGrapbSwGQpBllGHHpcl8TGUpG:rfZ4QRd6JBS4jlo2l0A
MD5:	D099F77A8677C3ACD4CDD89445CD0EDE
SHA1:	096990181ED6C83828CF3FA51B80EACEDAA4C16B
SHA-256:	A5C041364AFE6D0C183EA33FEF931A1D2961F949943801D107CCDFF49356C5E2
SHA-512:	D6B1CBAB05444222D510B319F40993DAC022EFD5D7848C2AB4652195FC8ED6581B3DDBAFC7006492BC6E26AE003959BAE0E07F2A2264BC1CB09EE5D188FFCE 83
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{ABDA8A6E-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.8481283944195614
Encrypted:	false
SSDEEP:	96:rHZYQI6yBSPjg20WOMiKY+hfrPRY+hfrLA:rHZYQI6ykPjg20WOMiKDPRDLA
MD5:	48222DFE446ACED9840C42872B680857
SHA1:	015CF243725862E13E8E2797D4D348058597C933
SHA-256:	B80C378D6F9333E67FDEB3E35571014FD7A8AF7DB5ED50B362732ABC2B5FB2EB
SHA-512:	777144B8CA1926189BB576B60EA4C07BEAB2FC62E4F3B2D0FAFFE39B0A6F004F32EAD83C63D6E34D353C677601E98DEFFA781FD188DDB708A10B10FA202E16 DF
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D93678-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27216
Entropy (8bit):	1.8566710772880282
Encrypted:	false
SSDEEP:	192:r6ZNQh6rkojF2zWoMca2i7UAYx2mi7U3A:rmS8wq8KNbbgE

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D93678-1265-11EC-90E5-ECF4BB570DC9}.dat	
MD5:	648989DA779F40589B6523C3835EEDAD
SHA1:	010C1188F513CA8AB5C7BEFF92F3B8DE5233754D
SHA-256:	51E4D5507F5F1B7AB482DC5A6B3658200E3C413FD1C8C008E1501253B786C518
SHA-512:	13AA62DD620D8B8B7F89185D85EE05BACBB19FC985B6459C561AA4514A115E0674DCD30493668FF17AA2E3C09C23CE94C65A3E812716236032FC5F3A56CC522
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D9367B-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27404
Entropy (8bit):	1.8572823639685336
Encrypted:	false
SSDEEP:	192:rTZUQA6CkXjx2HWuMie+LObtv8x+LObt0pA:rVdr7Tg2HtfFEfj
MD5:	DDB7C72B2B1C8B2B5071F7A5565D896D
SHA1:	508C00D7367AA3A67D677F5E32314A1E1C047709
SHA-256:	57DA8C2AA237F6FD25BADDBD27E96E72925C97F6ED0BA7EA0A658EB6769F1649
SHA-512:	80DBBA7480D83EB8F6A1F16969E3645236BAF5348901D02EC54AE4EB96A11BC55ABDE6F0C12032795B4A3F951F3ED67CBE3CEED0A279DBCFB42CDA150CF3B BB3
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D9367C-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5983526464503603
Encrypted:	false
SSDEEP:	48:IwrGcprqGwpaoG4pQoGrapbSrGQpBaGHHpcsTGUpQKNGcpm:rxZyQ462BSFjh2k6Ug
MD5:	CC0FE0FF58AE555D6656C15E677D54C0
SHA1:	6E384C2313C2830C32F8BAAADE358BC9B62206B5
SHA-256:	4DA66904C9D7605A78AF2DE03AD5EB4CAF7ECA60B973BBA03DDB5D0B8EFCB8D0
SHA-512:	A96DBEC54CBFFF31E69F5B6D6B6B73E33F0A6B35C67899B2BC84C174A46E9293F80C9A2040F8CB67BA90AB36C0C139C841BAB5FD4DFB1AD57736D2281E0EE D6
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D9367E-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5986649966212345
Encrypted:	false
SSDEEP:	48:IwIGcprRGwpa2G4pQSGrapbSkGQpBxoGHHpc7TGUpQI9Gcpm:r8ZLQG6UBS8j52V6qg
MD5:	9F4A3AF3995F42AAEAE382092E9311D2
SHA1:	AA667B30303BC530E2F2E6DA9A54E25E3BF442D8
SHA-256:	1812AE11D447451E6756B21B57C16D5F0AEFD3B8B4A31A3F933B127F4E352B77
SHA-512:	100FB524336AD4F58E95B55185632A38358AA4BBE553BDFDC18EA2804DEC3DE346A3B7F8BE8712DE73EABA1240894FF9DA93B7031009F4156C10BAEA5DCFBB 1E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2D9367E-1265-11EC-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C376A120-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5994990011009769
Encrypted:	false
SSDEEP:	48:Iw2GcprDGwpafG4pQHGrapbSSGQpBKGHHpcPTGUpQLXGcpm:rqZdQx6bBS6jR2Z65g
MD5:	1F421F839BBF29CAEFEE5CBEC2E5196A
SHA1:	F97343BE05CA4E4A0241221D420511DB28E18DBD
SHA-256:	85E11E77FF763117461C7884C2C09C121FBCF19DFF1B1236300E3C48843D751E
SHA-512:	A30EFEB5EFF6492078C0C9489F4DA999003BA807DFF39DC5BE133319928B855AF26D7D3E7561796F246AC90BAAEA74187AAAEF1EB8C052A12EF1051A8B00A2E3
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{C376A122-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27928
Entropy (8bit):	1.845594841204007
Encrypted:	false
SSDEEP:	96:r0ZHQv69BSpjh21WFMZS0+GGyvR0+GGy5+XJr:r0ZHQv69kpjh21WFMZSRGzvRRGzsZr
MD5:	4651C2F105BCCBA8410CE678679F1B0D
SHA1:	A6CF948D4AC230B4EF320ABCB3BC80F0959A0B1A
SHA-256:	1EEE98F97BCA82DB7694D56E342A43680F97A699B6E3C8DE59B6EFD9CC8A5BDB
SHA-512:	48BDA631B7E1ACB622A31E844864700BEFA88718845AE950F135E41B288E25D92DBAFF52F1FB7DC1B42D2B033BE9F73FA2395188D07A3803CB97A15EB6F0E8CE
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{D67A7CCD-1265-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	16984
Entropy (8bit):	1.5741886878119258
Encrypted:	false
SSDEEP:	48:IwFGcprEGwpaoG4pQMGrapbSrGQpBOGHHpcDTGUpG:rbZ8Q46KBSFjd2dA
MD5:	C37E7E25B5720A5BDE17831E9AE077DF
SHA1:	F9AFB370E0CD3876D93D541855A406B540BA67AF
SHA-256:	155A43009544CA7CBFC5BFF24D3B91B868CA3A350DE2C8B81901C83316C28454
SHA-512:	D265763710D03140A4F88CABA34E17047FDB0DDC07025EAC2F60B92C1557B468CDC8B93B7F29FF94994516D6154FE862DA566A40203692B7ADFD88A093B87E7
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.017170527854778
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upG7On:u6tWu/6symC+PTCq5TcBUX4blOn
MD5:	DF8CCBBD66B03F497CEFE9D8F8A7F52F
SHA1:	482F587B4EB67EEDB562BF16DC9625F4506574F1
SHA-256:	2B9F8426386CB2AD99329C4A2291D6F4E225718FA1E4A03E9DB3C69FE8E6B320
SHA-512:	6496B7A39F5B2E8692853471418549036F9D73654AE31CFAED9F1C146E80DF93ED9A4E1B7504B8402701FA861831DB424C42BFADD59DA05CC32CF8E432D0C4C
Malicious:	false
Reputation:	unknown
Preview:	E.h.t.t.p.s.:././/.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .;a.....;a....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
Reputation:	unknown
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\264bf325-c7e4-4939-8912-2424a7abe532[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	58885
Entropy (8bit):	7.966441610974613
Encrypted:	false
SSDEEP:	1536:Hj/aV3ggpq9UKGo7EVbG4+FVWC2eXNA6qQYKIp/uzL:Di3gyq9Ue7EVsCjeXuS
MD5:	FFA41B1A288BD24A7FC4F5C52C577099
SHA1:	E1FD1B79CCCD8631949357439834F331043CDD28
SHA-256:	AA29FA56717EA9922C3D85AB4324B6F58502C4CF649C850B1EC432E8E2DB955F
SHA-512:	64750B574FFA44C5FD0456D9A32DD1EF1074BA85D380FD996F2CA45FA2CE48D102961A34682B07BA3B4055690BB3622894F0E170BF2CC727FFCD19DECA7CCB D
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,.,..".....E.....!...1."AQ.a q..#2.B.....$Rb...3...C...%&4.r.....B.....!1A.."Qa..2q.B.....#..Rr.$3b4....%CDc.....?....]..l;.q.`.e...=..??n.\..)..".."..[K.W.u('d+.c...;.....R...(... .N.~.J,g...-.....-H.[vI....n!.g.....F... ...r..>%..*b.l..".....~7.k..s..r....u...0...).....x.....4.(lk...*EM.S...n4rN.V..88.J..~.....Q.FJ..A.D.-D.tk'?.F.....IY.].....O~=*3.N....rr.u(.....'.h}.,..... ..3[[...q.....g...&.O.....z...k.n.:~.)-S(..M.....:.?(?.2206..g..."..S.....~.#.....=.....~.<,G.....B..\l6..@Jr=...(.....N.....xi.....}...o.:F@$...>.N8..~.....6e&51.Rzd$....A.l.lw..b... _.....t*b]|`.t.....w.....KLp...'.F.?....._.....b.a..6T...P...HIRv.F..1..A.M.....2:...C....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	251398

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\2d-0e97d4-185735b[1].css	
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
Malicious:	false
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	396665
Entropy (8bit):	5.323973786488522
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/jgyYZw44KfhmnidDWPqIjHSjalCr1BgxO0DkV4FcjtIuNK:CW/VonidDWPqIjHdg16tbcjut
MD5:	EBE291FBFB5808D09F5B5BE3D0A5A25E
SHA1:	7DAE03E3E55EEE92453095B5A4AE26A4F492AA6E
SHA-256:	FC248BEFAA53648F714231D548349AF87DBB3F2C283586BF441B0DF7E2A98E76
SHA-512:	8F069F360A2607B906D20A62A3EE04D9A19077812713A9CD6A4C79EC1EAEAAF04412A27F616D1C857D92F858039155A251E1CD09F8992457288383998C460C5B
Malicious:	false
Reputation:	unknown
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929ED
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E.'.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(...<..\l...7T.....U..G..,a..N..b.t..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAMqFmF[1].png	
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.# .H.....\\|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AANT3y4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	modified
Size (bytes):	28887
Entropy (8bit):	7.909497836335464
Encrypted:	false
SSDEEP:	768:IgaJ65BYqO+B1DOZFA3oZgD3iE+8wdlirV:IzoaqdOZ9grK8wdsrV
MD5:	CF05D5EA1D6AF4CABD89F2A00C0E8AD2
SHA1:	D9FB635C8CF27B6655B5A585F0F76D801B6E6423
SHA-256:	4F83E4BD355BDF6CC520A7868DA0DCB6EFCA840B20E5CAA51FC5F5F227EAE4BC
SHA-512:	D00256BF16B34B2962275187E5210450CFDC57C795CA8E0BBF06EDDA4BC4CCBB1589CFBBE8537B76F96FE9CEE84ED856C617E7AF787B698254F12BA70AF606 D
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..5..R6.i...Bf%..+#6....H.<..@p.....V.-@.a.LF.K..)\.V....1.F9. Xo.Hc3.&.E8...Ut%.&.jJ."...E._#....X.E<Ve.Z.....C1YH$..#.). ..!.c....P...-.....&..D.-...5.....y..c..<...W..1=h.....qR2_1...%.F"...H0E.`.L...hH.1|.. .$.....G..z..kx.....7Z,.....,.)0...&....G4.'.v..'.#.jLe)d...$....\Ev.$.$~5V..9.k.@I...Q.$.)..... }..K..`..(.em.C/.z..@J...y._Z.r....Hc.=h.,.t.....pG..A..Z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AANg50h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	40569
Entropy (8bit):	7.954892481469937
Encrypted:	false
SSDEEP:	768:ILhyA//Akly9981n74czNrDrLjXGik/48pcO0JPX3SEebK:IEmAkQ81Ug73UfefSEj
MD5:	B0989E31EDD523B96803E1AF9153AA0C
SHA1:	F0E256D8E5C95FF66618EAE588B074E4E5BAF831
SHA-256:	2F64ACD4B6DDBC2291738375B81AF48DFE287A731ECDF5AF977DFC53E3EB763A
SHA-512:	06A87F74E757AE2A341CB37AD6C9BD5351964B951D460FB52F25E44329B6283AFB456639E731A504EFD2BF49A2B4FD0691FF04FBA3C00E8AC031A7795992A3FC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..?..b...{...m.z.T...1.:.n.P..x..f..q[.iN.....lFCP...f82b.$MR.*.....@.0.\.....k,g.....O..|Z...R....p...L....+.....&s.....}.;.k. [.)..v..y....L9K..^.R....SI..%..*(.-..._2...>a..t.y...R....n.l....Q.2.W.Z..eQ..9..K@.nv..2.....;..)2...,l0.H...?...l..^....W;..u*...+jR..nu'S...g]....y.v,..kN.....E...Zw..E..}.w...../..Qt..... ._..t"....{x..e.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AANg9R8[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	27866
Entropy (8bit):	7.9012317290639515
Encrypted:	false
SSDEEP:	768:I2Zq3LwC9rPFs42M/6+qsP2BvpTRohxC9HW9M0dAqT:I80drPhR6HuvAqT
MD5:	22A765E78393D6675377E20F60E382DE
SHA1:	94F6AF29EA57274BFEEE6CCD41EDDB14F0583F24
SHA-256:	E621E02B6BB36B9FE5FD1F2E47D08EBCC8BAC15275F3F70569FBC7E116E6F342

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AANg9R8[1].jpg	
SHA-512:	B2AAC7B7BC88BEE4BEC9D6EFFC252924B3E7D923C5B9E2FECB90260F29A48BE9A7A16CF04FF0926461CA98AE2E69C116D138335C228A863EB0D8C27F98D02(83
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....x...8"..N.5.....Y..0}..k.....ib...'..)I..1..@..Sb..0...W#...jYS...+SN.n..{qJ.l.>.8.w.1..`.... .U.$c.5.[..kxF]..*.Hm....@....Ur ...6."..mI..L..;2,.i...>R3.Ab.]@.]....Y.RF ..$T.4U.c$.TX.....1I#H.....B.....3z.|.L.p.=..;.|.${.n.nN./p*....'Ke...7e..U._...../.E...G.....a.?.....O...4C8.?*Wab6...).....qr....N..q..) .....~])....c.....<.-...4.I.C.`.=...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOfZRW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	3093
Entropy (8bit):	7.883981124809078
Encrypted:	false
SSDEEP:	96:Qf7EjVwJE8Bk2ppZBt6s5sdskI5Gxo9y3:QjKwDBk2ppZrisJny3
MD5:	7C5FA8940D22DC4F3D60519B642B8C28
SHA1:	8D0F3497374593EE162727BE3A81915A55EF5578
SHA-256:	68A4A72586D9238169A10DE1D1FF65383240747BF93F88F527942D0E9B019F92
SHA-512:	DBBA752921646D24051236E2DD7CFFB3B611E3CAF3D300EC948FC1D8B51036D7B6E97E4590340306E8A2E3770088CE21D9BE553AAF0562E703067B06E4972699
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..HB..z.U"IS....0%..I>...z....a.s..HM.P[.....$.8.<#..,.O5....s.iY1..&./#y..._..h.Av..jv...y....F.*^^.].Y....A..fT...-.eG.Q..~.@.. .*Qn..3..\.$d....n.....ad..\..._....v...U.r.d.L.Z....C+...Y[8..7..BK+o2I.....8.Rq...y..#...1.j.A...B.....-.....*.N@'....q5bO..Rya[=4.bv<..N.Q.ym.D...<$:I.#.k..W.V)...4...{...n.....Z.. FtzM.....#..Q.C,_@.X.P`...SL.k....n.\.R.....5/m...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOgLtL[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	12204
Entropy (8bit):	7.760356414393578
Encrypted:	false
SSDEEP:	192:Q2ocxYvdubJzbjF4rcDHiz3U68cXNsT0t16iDUVVH6Gb029cbDc1+fCYyGqqpo2r:NosSuF3WggFk0tgioVV0dCYyGXn11sA/
MD5:	809C75ECB371E6428E0D21641C6758FD
SHA1:	06EF08CCC013EFF1AAD201C7F1BD3C288350B274
SHA-256:	3B7A81B0CEC9930FDAF2EE0BDCBD475ED69656DF7237B4795C8B021E3A71A725
SHA-512:	52D3EDCD559F525D6E941E63D88CC243A0F11212D7172AA089B672505D9DB94DB68BE1300E9BAB00D150E1E644891999483FFBDF0791E8E2EE8ECBA66E25D8 F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...eX3@.&h..4.f....f.."..u....7P....u....7P.n..-H.d...~.x.....Jo.h.g...W.....>..?.....O...\..F...._.c..vb.(M.B....eow..|.....>F.....}..... <Epq..s..O.w.1..|k}.....8..rD\._..^....?.o.4.b..3$.....n.f.'.t.?.4....C.Qly.....o..4`.Y.....RC..@.3E....=.?..w/...B..~...n..E.....ZW..>..`..L...J....fd...W....e..P..E...>.....o.)|..G.>...=..1y. 7..@.q.....#....+.....b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOgbmq[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	6289
Entropy (8bit):	7.851523332145787
Encrypted:	false
SSDEEP:	96:QfQErg7WA8UKQ9FQeAAdE7XqMnyVvzoTUtmnw66zfMcg84pGEuji9zoybBbqr:Qoag7WA8liF669N36eEtjpG9jFY2
MD5:	07F426B9CCD868F4A649262096340195
SHA1:	0FBB15A464AA610660FA0C4FC0DC541AF1714797
SHA-256:	D2CB2DD7DAE25A68EFB5F3365A6ECCF7D1754A497FA0CB933DF6753E395A5CB9
SHA-512:	5E79975D852BF819A942CD6FAE7744AD75A081EC1562F4F243CD01B86B5CCECEF7976D239AED3D30A215922D5CD239F329BA2E970364365571C8CB7CDD833B C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOgbmq[1].jpg	
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..j.....N..w.....Z.....h.....H(..@....@.a@.#..g\.@...&M!.:.....f.q.;..D.@..%.....p..4.C@.4....6.....<..8..x.....".#<P..6..P..4G..&..c.7.q....v.M.s.U\,t5D.@.....3@.@...P...m!.h..."j.e.(...@.....p....l....t...#....&....f"..=.(..jr...@.{.Y"..@..7..&9..P.(....@.4.F..`..(.<.....P..$..}0..@#.(...."../ulZF.CRY.u.o.8..,V}3gj..=^.....a<....:.....f.P.y. .;x...PX..9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOggwL[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	12998
Entropy (8bit):	7.957875205331213
Encrypted:	false
SSDEEP:	384:bOhTptS/mgGPq4AQF+2SK2Fdtlr0voY49wNPci77P:bOhbSugGPq4zFotlr0uIP
MD5:	1D942C6E3EDD1A02F198321F9F653842
SHA1:	CB8A9BCC50B7001222AA6ED0070701A91E8D48E1
SHA-256:	8C71199E78444BF4AF8F2FB06A29084CB7A3B79605DC8C7027A01AE146BCDCC2
SHA-512:	245C76AFABA723A5F404DBEF1FDAA3A35B97D58B9C0A5AF4467D64E4821A0B8A9CF8BCF4E46145A9E39D224C996AC06A4D625BDF21C0DBD6C5C027B70AA3D37E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:@...*9`M0.9.y....N2zR.(...4l.g?5&.p...].....d.D.0.T.J...%..,....(e!...iC...].....b....b....O..A..d4Ykg)...G1\..8\.....94i.S.N.6.e..7...X....X.r...}+D....&....@...G<u...]+\.<P..id..y$....++.....`.<..-.....=j#.F5.4...G.cr.....ZZ....>l..;..Z...s.Z.....`% .T.N0(...pN=..(...^.9..-...~.'..`RJ.B0:....n....O"n.....kJ7..IY....B.....P2._1C..Q-...M..:b.Y.H.....q.../..v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOguTA[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	8913
Entropy (8bit):	7.92704245333277
Encrypted:	false
SSDEEP:	192:Qo4x+X1wBOZURMxGfEa2Nbe/e33DLBH86cg2w:bnXqB0sVEa2Y/03xH8zw
MD5:	6A4DF2C42DA5EA53EA4B3A6CD2EDB5D2
SHA1:	10B2E4A7F7730E8D6BF42F121D42432C26CFC089
SHA-256:	D33985B0529FA6B886C455C39EE3946F11CB18336F038C72BC710C6D36CFCF03
SHA-512:	062B790B4B455BE51348700A0065E5C35D13A14ECFADB4AFFBF51578FA03D77BB579D745C031FA84C0E612E30729E91FABB4D626178240A868F74F7C05782D39
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....(...4....P..R...^H..."...../v~?!@.W.$.....h..s.....5.M....9=.....R.W)4.....:;.....,.!K.....Jv..p....:...r.n.Xu.CHd"....3..v&....!_.'pN..Z...I.v..Kk.....$.qh.".W.8>.D....(.....J.(.JC..k0.u>....r.9..1.Mu.Y.....;..8....?.R.R...z.r...#.,O..k6.j.c...9f$....3.....RD.0I...{Qa\k..(....6'.....6...#..h...FF>o.Z..q.....jC.%rs...>q....dw.....4.cwJ...U$..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.) ../'~.....<.3.#....V....T..[M..I).V.a.....EKI-4...b... 6JY...V.t2.%....."Q....`.....`.5.o.)d.S...Q..D....M.U...J.+.1.CE.f.(.....g.....z(..H...^~.:A.....S...=B.6....w..KNGLN..^..^.o.B)..s?P.... v.....q.....8.W.7S6....Da`..8.[.z1G"n.2.X.....2>..q...c.....fb...q0..{...GcW@.Hb.Ba.....w....P.....=.)...h..A..`.....j.....o...xZ.Q.4..pQ.....>.vT..H..'Du.e..~7..q.`7..QU...S. .....d...+..3.....%*m|.../.....M..}y.7..?8....K.I.|;5....@...u..6<.yM.%B",..U..].+...$...%$.....3...L....%.8...A9..#.0j.\lZcg...c8..d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAud6Gv[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	356
Entropy (8bit):	7.101459310090333
Encrypted:	false
SSDEEP:	6:6v/lhPahmpAKG4NDBbCySVUc3/qF9Hio9hbifyZQw+bS2LblMid1Rc9ruhiFp:6v/73bCLVYHio9h8kQw+7BMW1W9rAir
MD5:	A94D5FFB98CBCA323E6AEA6A826B9ACF
SHA1:	D4F20C419292258A27A06511955A02400C767723
SHA-256:	7527C0E97B871894A7AC475D714D51E82F51BB965848DCD03657B12D5808BCAB
SHA-512:	D2B0D68C085457161F612B50508548D9FD6F7F48DE74AEC8009C65375A0CF0D58469BC8B93AC2705B4AB4A0F0D3FE07E8207500AD896FFC676D7D50649643A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...j.A.....A..y..X....$.E.'.b.:.h!.bc%...:.FlD..L.@:...F...o...u..+.>nvf..v..n.;08..<.,C....-|A.x.D1.Mx....B.R>.....3..d@.... %....v.Z...5.C....3@.a.[..iku.....%.(....p.h..m.](..s>F.&...q.^..dH.....0<a1...4. .z.Q.@<W...,....4..?M.b.....@{X..L..x...|:.B..B..K...j..k6/..LE@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	29565
Entropy (8bit):	7.9235998300887145
Encrypted:	false
SSDEEP:	384:I1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PIVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc
MD5:	6B79D1438D8EFAF3B8DE6163107CEC71
SHA1:	E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0
SHA-256:	2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8
SHA-512:	745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7 B7
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4.m.!....4..i..4..I.C..u .pi....dRe#J..\..t..bC3.).:I.".W.#..&.....-&2.".&.(I..y...r...cE.7..h(#.....t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y.....A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy..'h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.....~....(..".~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1fdtSt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	438
Entropy (8bit):	7.245257101036661
Encrypted:	false
SSDEEP:	12:6v/7DHVT2T6ESAN2ISAy22UaU8Pa7+/LB:4Tq0AN2IjyPaqV
MD5:	3F46112E8E54A82D0D7F8883CF12A86F
SHA1:	AA1A3340F167A655D0A0A087D0F6CBF98026296C
SHA-256:	E4472117124 78A81E419A9794678B6377AE3ACA057DEA78FC9EF6A971E652CFB
SHA-512:	EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49 A6
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....hIDATx...O+DQ../]....f..(,.,-.!.L..X..ee.,.. .I.D..h..P,&.|.c.L.i.E.{.k..~.}.}.....t...W...*.5.2..0)X0I.c.wbU.....N..,....-F...J#lSq.;....a. ..*.....D .w.g..N.....F)l.....`_..s..A;?.4..+..ob.....Qh.H.:A.....(...;.z./..?.:...t.[.e..b.....{..t.A....M..0.>8&_"... Ev.Z`.."...=/..F.}X....#|.Ny. Z.....W...{HX;..F..w..M:...?W.<4B..!.I. ....l.o...s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7hg4[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...l.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:.8..8@t._...1.".@C....i&Z.'...A1...!....R...}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmlZII+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....|....."FX.3.v.A.....1..Rt...}.....;....BT.....(X.....(....4...-...f ....0.8...|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.....g...+.o.]. ..J...$.8:.F..I.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBK9Hzy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	480
Entropy (8bit):	7.323791813342231
Encrypted:	false
SSDEEP:	12:6v/7BusWIjbykLNgdQLPhgZPwb6txC3nUPuZZcb:MW6bykxgSh6a6TCStb
MD5:	163E7CEBA4224A9D25813CD756D138CC
SHA1:	062FFF66A1E7C37BAE1ECE635034A03C54638D50
SHA-256:	14525F17E552171DEE6D57C932287048185BE36D9AC25DA79CB02AD00657DEAF
SHA-512:	C37D77C1414B75CE6E3A90087B3C1E9D57AF6BCA4C140F1F4F43503D89C849EE1143315260A4DF92F1DD273305C15121FF199C04E946FA3BBD98B9B1D663606
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R=H.Q.}...?....!... ..0h.B.....!!.....h.j.....%i.J..%.5.:._c.u.x.=....wQ...?.L.\E..] ...O.&.m..l.U.z..M6.....9.....(....3...x.O !3.....o&}.....]*.w....x..s.%..4.E.WX..{..!....4...2hB...c.m...]m0W."Y.,.2n.W..P.U.a .p...f.\gV....:0.4e.....^s 4.j..0...u..*..t6....v..4...c8.4...0./i.Dh..../[t..h.5...!E$.....+..r..C.v.....T <.....S..*z#.:....p.B.....").}R.....=.....w.e.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBX2afX[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBX2afX[2].png	
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,I"...)...z.....>.OVObQ.....d?|.....F.Q!$....qf.s....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S.....&...T...?.X)${.....s.I."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v.....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....\|c(,.....l.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@....:.E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29IC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+...]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q...._...h...L.....X.{i... {.. &.w.:.....$.W.....W..."..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F57
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0..."..0....a....<....<....y..qS.....m..k..%.'|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[.. ..0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^|.P..5.0....?...&.A.K..|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/... .Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\NewErrorPageTemplate[1]	
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\NewErrorPageTemplate[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	unknown
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	unknown
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vllJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\dnserror[2]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	unknown
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\log[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.081640248790488
Encrypted:	false
SSDEEP:	3:CUnl/RCXknEn:/wknEn
MD5:	349909CE1E0BC971D452284590236B09
SHA1:	ADFC01F8A9DE68B9B27E6F98A68737C162167066
SHA-256:	796C46EC10BC9105545F6F90D51593921B69956BD9087EB72BEE83F40AD86F90
SHA-512:	18115C1109E5F6B67954A5FF697E33C57F749EF877D51AA01A669A218B73B479CFE4A4942E65E3A9C3E28AE6D8A467D07D137D47ECE072881001CA5F5736B9C0
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nrrV27452[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	90611
Entropy (8bit):	5.421500848741912
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillux5Q3Yzudp9o9uvby3TdXPH6viqQDkjs2i:atiX0di3p8urMfHgjg
MD5:	1EB648466B92897E80D5F3A64D02C011
SHA1:	624EE532FED7CCBC60DF3433DC3369AADE0F9226
SHA-256:	1C9605652D3D876ACA145E7F46F92E669E6A92C4AB27A1CBB454882BD58A1386
SHA-512:	1B7CEED799A6994991DCB8938A3B00BD64E1CEC17EC0775FC1CE844604805FEB20BEC3D72823730712BD0CB45B278F30FDD2CBA7319AD605323F667F39BF80C
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otFlat[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12282
Entropy (8bit):	5.246783630735545
Encrypted:	false
SSDEEP:	192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYLp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAk
MD5:	A7049025D23AEC458F406F190D31D68C
SHA1:	450BC57E9C44FB45AD7DC826EB523E85B9E05944
SHA-256:	101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5
SHA-512:	EFBEFAF0D02828F7DBD070317BFDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A96
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otFlat[2].json	
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCIgcm9sZT0iZGlhbG9nIiBhcml hLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpdiBjbGFzcz0ib3Qtc2RrLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZ D0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNkay1jb2x1bW5zIj48aXRsZSI+VGl0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0b GU8L3A+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRhaW5lciI+PGgzIGNsYXNzPSJvdC1kcGQtdGl0bGUiPldlIGNvbGxlY3QgZGF0YSBpbiBvcm9zaWRlOjw vaDM+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRlbnQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9 kaXY+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90LXNkay10aHJlZSBvdC1zZGstY29sdW1ucyI+PGRpdiBpZD0ib25l dHJ1c3QtYnV0dG9uLWdyb3VwLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IENs sb3NlIEJ1dHRvbiAtLT48ZGl2IGlkPSJjbG9zZS1wYy1idG4taGFuZGxlIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IENsb3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBp GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otPcCenter[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	47714
Entropy (8bit):	5.565687858735718
Encrypted:	false
SSDEEP:	768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI
MD5:	8EC5B25A65A667DB4AC3872793B7ACD2
SHA1:	6B67117F21B0EF4B08FE81EF482B888396BBB805
SHA-256:	F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988
SHA-512:	1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F20 68
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IENsb sb3NlIEJ1dHRvbiAtLT48ZGl2IGlkPSJjbG9zZS1wYy1jb250ZW50liBjbGFzcz0ib3QtcGMtc2Nyb2xsYmFyIj48aDMgaWQ9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBp GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\4996b9[2].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAKFpl8[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	585
Entropy (8bit):	7.555901519493306
Encrypted:	false
SSDEEP:	12:6v/7Zllj1AmzyaeU1glVfGHTT3H7LhChpt+ZnRE5b3Bz7Mf0Vg:S31hzm1GHTDbL0hpt+rE5bBY0Vg
MD5:	C423DAB40DA77CC7C42AF3324BFF1167
SHA1:	230F1E5C08932053C9EE8B169C533505C6CA5542
SHA-256:	3441B798B60989CF491AE286039CA4356D26E87F434C33DE47DC67C68E519E4B
SHA-512:	771F92666BE855C5692860F42EDB2E721E051AC1DC07FE7F1A228416375F196B444D82F76659FFF9877FD2483B26D1D6B64615803CA612BC9475BA3EE82A9E0D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAKFpl8[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=O.P.=..h.....".*.....Tu..a...*F..,.....R.....K.....$V.!.c.....F.e..{.y.{.L..J..s..=>...2.M.2|:..4,"...ag2(7"d..>...7.xA..~m. ... ..07ZP....6.|X\}.+`.?....~^.....A...p.6N.....`...*z.....S.].h3.J....~..t...T.4c..{..P|b.....C..l.y.....D.....6.@o.!.....".}.a....B.+.....n...Z...+.8..z.._.qr..c.....J.R.[./u.KYO.RZ....X#S.-.. G#..vR..S.4C ...w..HT3}|...y.?.[....R..&1."u.....e..j..b/..=S../..'.T.!.~..u.....xQ.U..q.&...M.....lH.W.D.aC....}.1...@.h...\.br..k.....zar.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOfFRV[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2754
Entropy (8bit):	7.844425834747859
Encrypted:	false
SSDEEP:	48:QfAuETA+wjpk5kCLsIZDP21yDvkDHCIY1x3pf7nM4kR1izuW3keUpEpso:Qf7EElWkCLjP21yADHCtx3pfyREj3kUN
MD5:	C830ED87471EDAE5A549A8374D0E44AA
SHA1:	ECCD1AD8688D25F74D6F9CDDEB938D0316DC5672
SHA-256:	D565D9A2812A5FF3057ECD3F8450174294FE18A604B5174B6808CFFFFE49155C
SHA-512:	4B72FC23FE713F9BD21E4B8077F99AAAE969749FF4DDA41B1C411E32D9F50C50B2B7141D82D5C305E1C181813FD3FA68E2E54402D3CAA3D9D14269528F97D2F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Z4x.n2.s]/S..u[!k6...Ep.g..$sZ....p....k.p.e\.{...<.*$...w....N.{kY....X#|I...E;\..._....r.....Q6.P.Z.Q-.....b.p.b..J ..8..h7..}l.`` ....Rr..Q...qiqat.s.....{...+.M.9.....Z...3..:~.gii%....J...iA.v]E.....o]g.F.....}..}...U...k.ft.4z..y.;.g.....q..._Fk..;..y.L.G.LU.....E...X...kQ..aA^Z...q & ...I...r.t....Cw.;...>... zWH9X...A...3...E...Z..X.P.}n.U..q..*.&..2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOfKbP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9208
Entropy (8bit):	7.93658004874926
Encrypted:	false
SSDEEP:	192:QoZjbcNMrOy2jZoc2apHaejRWSNIHxLf5T0yjPpWYcTxxx9e3rCA:btcC6D12C6SkVr5oylTUxI3rCA
MD5:	13E43269EC124CC169F9E7EAE844908C
SHA1:	0D953E27B371182B613648BF1BA585E268CA571E
SHA-256:	9F6AB9EF0637CBA274ADC44222A53F9D7314E6A73B722F501F2C8ADBF8C34180
SHA-512:	AFB631ACD7B3F71CAC612A0ED607CBF17C2B731A5A2C293711AFB29490E7ACE6C3D7EC78393D3225466A62E13B288141243A5F14D0FA0AB78401B1BE0F2C8DC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..F.....a....s...h...n..6.E... .....>c.....J....n..T.b(.L_...1.....Tc?0..W.B..-)VD*G1.....\"i....`..-._..t....\|.. ..>.....L...{....S..b5..H'$ g>..P...*H8'.$z....(.a.....fB.....?....Y<.Cee\`..O_.+.s>.B.3.....p..D....>.....3l.s...|...c?.....d.XX|.3...Q.u..e-nS..s..[.{.z.;"".....W..n.....S..z.fG3.....y.d.....u.li.....).(.P.x.!. .e.....Wp.....4-.=.G.F{...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOfNp5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	21488
Entropy (8bit):	7.956074967094666
Encrypted:	false
SSDEEP:	384:NK8ca6taiPAEHF8X/lQuWgJyiaHcwnI143gZ4UTuRavxmg4hBcm0n:Nv4l8PGuWCyiaELZdCk67y
MD5:	766190A0D6ACA6A6D464679662CF7E37
SHA1:	96B3FEF16953B6A65C61E9A10D94CAE57B60D901
SHA-256:	1538E167FBD736AD5A25A064C203D4A4AF609028171C2BC159CB546318D8986E
SHA-512:	E35464583A4AE460573C68460B15B9F0369AD11D7F4401A0F502EAB3FFCAD61B5E88F2CE1BF93AC3B2460D482A73A97D63D08E56A5105FA74DA8212A2FF34775
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....-.Tt..3..#.....2?.fl.T..!.0..9..e.U.>.,u.7.".p\.:..zRG...bT{..d.V....&.B(..1<.gf.#.Q..!.c4..8#.....c?i2>..s..R(.o.5.l2.6...@.m. xC.O#.5%Xm...-.e?.M..jI.<+....c..\|....i..$..l..z.\...<aJ...ERBfD.Io'.:...j....\...CE..4..{4.....7|R.)L...I...l}..2.3~;.e.$RH.3.d....G.)X...m..pN.y...3n.....f.Y.X.e..=*.CDM R.[l.....E.b$ .a.*r..C-.K".b5.G^:.Cdpl#.....T.&..]T..=8..f..b. ..m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOfNp5[1].jpg	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgHFd[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	21510
Entropy (8bit):	7.93214218371982
Encrypted:	false
SSDEEP:	384:NJVagIW3hw0e48faTXMp8GwYja65bYSAPcHhAX1lMrLscTgRqDQpCy3wtf/jYqzh:NJkgIW048fqy8hYjHLA0HhcnqgkRhrYG
MD5:	D7C74F83DF0021841F6F9617790A0EF6
SHA1:	6E465534385ACAE8D6455957E69B157CECAC5634
SHA-256:	E3F4D729DECA7D45A33DD425174430FCE43F425F625187A1CB7717EE8D847B9E
SHA-512:	8238125680B90938A0C89DBF225861F4D780DB7B5BDA80B849CE54BF9A6CDFD8FF7910A9E2B9068CE4B78D59F949DDD0831585311DEBA23B1D70254B83D4212
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..e..!.}).....n1.1.J.Y^89'....`+...V.....%p.#..f....X.6.s.f '.z..l.r..d.}.....w.py..N`q,.5W...Ut...!*..!O..D..i...-...4g8`..Nz...;..h.e4r. ..Y... .q.^.gt...i.J.2[:...3.....Ui.^.v.&.p....F.#.. #....".%...24.SF....9.9....IMsZ.-l3I.[]>..-.We."...O..aR..I.Cr.K*...PYd.j..F:Vs...7/.].u.L<a.....k*..y`=..J.k..a..9.1.rx..8..)].9...h7:-.....;..- ..9..6.>...+.r.....Vo.Ki.pHv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgJ6C[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	9430
Entropy (8bit):	7.764531777068338
Encrypted:	false
SSDEEP:	192:Q2sGHXqF6UeKGo3/VvhzFYjSpwT5B9sYDlCLBoSvRqg5ej4zKiAUH0Y8:NsG3qHP5/VvZFYjVsYDluAg5ej4zJAew
MD5:	DA3EF5D61CFCF919A9B3C8244CF1A338
SHA1:	6D13CC7968F716BC4A4B44DA6B48D5C5156A2A82
SHA-256:	26783E83884E406E82D42417274A97129D68F717B29B64D844397BDDF412634C
SHA-512:	BF62219E2BD0B0D261594B1E9597E30C695B661AE3BC59F62CB4770FE0F9D3539063B23C4B9B357FF33C360AEDCAA2A13C228046BD5BBE66D2A591E3EA511C 2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..@%...-.-.....(.h.R..1(....."....&..c).%.:..R..@.f..&sL..Ha...P ...E..P.....0..4.Fi.9i.u.4.bc).!.a@...Z.(...%.....p4.qwR..&. ..d.@.(....!.....zT....F.i.Q@!i.CL.P!M.#c.11....H...7Z.X..m...x.....@.Ha@.(.....3@..%...%..).}.....s@.GJL...H...D.().Ha..9W..F.&B...E0%QHb...dg.R a...a..8P.....P.@.@. ..LP0...0.....J.(.....c....Hb.4...q7Q`.....c....Hd.qHc...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgLVz[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	16649
Entropy (8bit):	7.922396366675045
Encrypted:	false
SSDEEP:	384:NA5v/9KF/LSZhyMDpqN6teoBMj+8sn+V5VaQmWjO:NA5ozSZhyBEYoBErsnEhmWK
MD5:	4035F9FD75175AB6DE70B4BDAD9A055B
SHA1:	7587562801349B57565E1992094B9704EC74EA0B
SHA-256:	BE74D2288FFD9CF5A34F65FF988A5C6ACD9273EFFFD62F875674B3A1DB1E6A2D
SHA-512:	5D429D4DA9598AB5FE06C74A55F549B7486C8D98E817455B6FAC487080DFD5A38A5CD828DDD77A35BA8E6249D440FFB0BCE02D936A76342DC4FB05569CD918 F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgLVz[1].jpg

Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..FOAX\.vC...S..Y.........`.~v.;....m.9?Z..T5......1...t.....S)_....zU"l';....i..''..M.s...,7q.!i....i.{.M.K..\..p.Z..]d}....cax.T..K...9'9.;.Es. ..;...q.E...r''..x.=...Y8...;.$.\6..+..l..z.Q.!.g.....Y=.X.H.zQ.......B.....8..6.~.O(...S....1......0*..;.q.av.F.\.q......0..%{.....dqN..FzR.\.....&@...+.....R:e!.........#*;b..E!.X..".)\.J..).0..p).NBl.. {SH\......0.:.....c;....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgcCY[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9028
Entropy (8bit):	7.9350546837322895
Encrypted:	false
SSDEEP:	192:QolvGgtNJQWCay/eOlV2ewOS3q/SlD+7ZtADA1CuO5EaHv:bXJEeOrvS3qalqZtADA1CuOqQ
MD5:	2D03D150765EA0FE3F5E0C06384CF7C1
SHA1:	F660B5FF7316F286CFF39EE9E9E986EB33CE9704
SHA-256:	198758ADC6AF0D2BC46D952FFE2ACB2B702D50643E263CE3E0F7C5FF240B10DB
SHA-512:	9FB6D545582786C6BA93A7179551903817DBCB65E92558FD06AF669FAEA3B13C1823DEE0EEE2FE97E669872D593BD78E484441F07BC0710E03482A949E0C0B34
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..1RP......(.. .P...m...`...........b..P.H.....P......"s.M...I[..v..l..F)X..gq.....4........wP...7b...@..@.h.(.(...@.@...@...tSE.J.....\.t.;.a\. ,....;..O.u..".D...I.%..\........=.X;H4..|....@..H...A@....f....P....z.@.T..).`.*....E...Jz.a\.4...v......E.rAm....w.S.....v............+...S..q...a.P..X..)\.u....(......h.........2.4X..`;.SN..!......M...c..... Bl.M....)....,...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgez4[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	21892
Entropy (8bit):	7.955770750433599
Encrypted:	false
SSDEEP:	384:Ny8WEBvNCSVYaHHa5EKBPgd/qbvbUILLgEU4XC70WmmhPeVvcj5:Ny8bRNJVPKB4hqbvbdGuCYmN
MD5:	6819354E52C961069FDDF9DE793F5C33
SHA1:	9E0ED179F2053E59F0A481FA81FC78CB020B8C69
SHA-256:	F43FF336156026D7712CCBCC671E8E7F939325CF5A0F81C09BA0E53E17E9CE50
SHA-512:	BDBA5E43A5693EFCA81169F5C28D16FF7A17C2FC0682B3C7D5BA9B24916D95FC5381F6F3AF3FA03047BF997E69F650370FD498A17267EBC07E73FBE39F7497E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....1@..-...P.@.......c...Au.f6-.s.A...h.....k.......0I...Z.......U.....@"....(......(......(....yK....+....b.95bcb.*..."....0....Afh.j.km..b.K. ...../..r#cYCcZ..i..m.BF22......i..f.u.,.{..T..D.........dtS\..#...j.0..wm'..3P..O.Z.]..xwP@.V...{6@..<.$....OOz9.D?f..X....h.q......'vRj*..k$..Q......M.-.W..y. ..<.|.zh6..o..>T.fX.K..q..T.+.. ..Z.(........u#.:H.....q.=..3<L......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgg4w[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	34427
Entropy (8bit):	7.918466298596994
Encrypted:	false
SSDEEP:	768:I+HFDaHrcAEP0XopJxu7HSOGTD4GO23d7IGbKjfGZ:I+BaHTEP0+JxEHyDs23d8sKSZ
MD5:	8A893F65E7371978DBB67255A0EC14C2
SHA1:	E718E3AABA11B0D5879A00C27DAA901F93D2A7B5
SHA-256:	4DB575F619B4A904FA76FC2F85A217971B39FD20B61B3779C9D4FF6701984D44
SHA-512:	AD3D6E1A48D2F2E59B2516F563CB31E586BEE00C47F2B85E6B95D31ECDC77703FBA4E4A477EB5E4C98B3975195EBA296436DB03C25D49DEEEF774F886B13DF 93
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgg4w[1].jpg	
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..+B.*.@..E.(...4....FM... ....;.Z.\.LC....H...qC....C.Tc.W..w..<t.".Pc.1..\}..L`...R...E!...vn ..y85.#F...-...P.@......P.@......P.@.. ..P.@....P.@....P.@....P.@....P.@....P.@.@....P.@....P...L....3@.@.h...yJ.V@.E........P..~8.._Z@H(.ni.t......i..8.....-.x... .P.L..r).qR..@.l.3..UnE1.........u.c6Ra..(....@..-...P .@....P.@.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@.@.......b..P

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgp9E[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	14628
Entropy (8bit):	7.959506953267804
Encrypted:	false
SSDEEP:	384:bwM39WfUCDAX42fh2ls85sV8AXQPTo7xpU3fxUw9:btIffD2th2lHiWxP6xpU35T
MD5:	BB5A568CDD23107E26783D614B7C47FE
SHA1:	F4FC12CAD2D2953D43A71D0729A352713237FC79
SHA-256:	1E37EC6DFDBEA9D1DC959A301B8A82094A0B908D411EBD2744A206EBDD4F4BFD
SHA-512:	B47604BEEFF49C5BADC79339AB6886760B21092FF1C5198D97C972E8AE50FFE56AB42D6FF3A14300726FF97B3928CFCC19E9B09A4094D3C63C7F77C6B7DB5FE 0
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....l.....3@.....u-..*T.'CX5+..^Kw....a.V....k6.."..hl."8fe..@=?.^.fa.#...*.Xt....*.H.w!.C.w.kP/=.i..L..y#.....J...[.&....<..MNH.W.\|.. s.p.9....]6.........p+..q....nr..{]1..&..W9.........".<V..$F&..wo.G...{.l.l.............Mn..7.dFR.n9..=..Y.7...Fi......nrI.J..w+.p...9`....g....*.{..Z..y..=..p.....T..k}....;A!,..V9..".....A.....{.. .W.s....Q.FY..v.F1.u...4..?S.KP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOgvnc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	13697
Entropy (8bit):	7.848115090089445
Encrypted:	false
SSDEEP:	192:Q2W3xN4uVWuPUZ3taz4XwR6SrWyBOvf/MWnxdmYpCgco83DCFxPoCOS1YAOHJpwt:NW3xN4u8yUZ3Iz4XwR/mmn2FxP4AO0zX
MD5:	F4EFBC68289CAF3A7B9073AF2E9E0BD1
SHA1:	46C041D8BBC0AF52E388432795B49D050E7A0A43
SHA-256:	4EB34F73471CABFCBC78439D42AF69831807D25F5ACD8151559BED13139D8DE1
SHA-512:	BE7E716E94EF3FC30C33D62EE15851E0F7CF635197901C088446AEB3F2B1BF8CC20F7D5B4C2F055A478EB3E622ABE981C0CC3754C0B144E485D5ADC79D0B36 3
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..t...,(.B..P.P..v.0).]..4..u.<....W.f....P..y9....,.p.x=...j...F..Rk.iLJ2..;..R\l.....d..C...v...p. .\|.!.}.qL....@...#.4.;.$z.`..q....... ..3.. ..p98..d#.$P.RJ......1....1.Ua....N....^{.@...F.....P..^..2H.$.... &8....=.+.Uq...v..7$u.p.&..s@.Hga..q.s..B..@...}.h...=h.U.P(...g..T.....b......|....<.=(..K......q.EyQD.B...g.0*.!.<F..@.h. $X.....$.C.n...s.5....4V.^..O.C.......I=.:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAzb5EX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	322
Entropy (8bit):	6.966129933463651
Encrypted:	false
SSDEEP:	6:6v/lhPahmKxf8jCAw4DGQJe1kvnxIekdOgcKOtQExGTFDDv4bp:6v/7lxkjyzQEyaI1QmGTlW
MD5:	89E1141C659F2127DD80809F71326697
SHA1:	3262110C91000071FDBB0D33893EC1EC8026ADEC
SHA-256:	98763AAD3E2B7507E7729711ACD2DACCBD56164FE6DDB10410047B212275C279
SHA-512:	1D32DF0DB191F0A3FA152BC47F5F463234224F215A283A26E4EBAF95095A0977ABF5B9D9804FA4DDB276CA8DAE2865789802BB8A18B02B232A9DBB22D5F19E4 9
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAzb5EX[1].png	
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..=..@..C.....K..`-(.`...vb.....vV...`g.!D....!....7..../Qg.Z...Y.....c....t.....c..).....)@.:.....8..t1{P_\.1..3Ao.....A].....5G _.....\5..x5R....'...VS.....|.`...~.....+....H^..1E^...0.,').....qJ8!..D.!O}.i1..E(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA0 6
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#l.....x\|...\...& .T6..~.....Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u .....Ic....,7..(..&...t.Ka.]..,.T..g..''...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%"......[.=a.....X..j.. <725.C..@.\. ..`.._...'...=....+.Sz.{.....JK.A...C\[{.\|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....N.A..=.....bC...RR..`'.....v.{:.^..... ."1.2....P..p.....nA.....o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.....C.D8.D.0*.DR).... kl..|.....m...T..=.tz...E..y..... ..S.i>O.x.l4p~w.....{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N.....g..W...}w:.....@].j ._$.LB.U..w'..S.....R...:^..[\.^@....j...t...?..<.....M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1kc8s[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.702979580339968
Encrypted:	false
SSDEEP:	24:5yrGVrpvzYKWJzgT7w2CGZi1/BwIBCHL/P:srG1pLYPJzY7w/G4OIKLH
MD5:	CD8DFD7D16B4BA3E2873EE06DB780B06
SHA1:	E8A79F0671D287E116C76FAA5F0E8A4099E0BD23
SHA-256:	88E6642487D0F944C6A020133CAE030781CFDCB518802419F10AD78937BDA6DF
SHA-512:	199AA29EF33317A43D1C6DF434DD5F9D0FF54BF363CCB1948A970C7EC6889B083565E85E0A140FCDFC38B675CA3EB24DEA0659897EF0450CEF43444E1CEFDA B
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....;0.....pHYs.....+...../IDATx..]H.Q.....LG.LW..Ha...?.f_l...l.a.....z.a.e.=)....D...'c.E_...F.&).\...4....x...:...=..g.?.....>...'.....b.....l=.*.Z...V.o.....O.....i 4.....9qjpWWW.P(|.T*M....}@0 .....Es .x...}.n..J.?....C(...V.UY[[.`.....R.v..wvv.....g.....v...H.....x.....4.0..b.\v:.v\kN^'.`.....gb..y....FX,.y.J.....~.s..x<?.+...l6qYY..hT.. .A^^.....#.H....q}.^..r.o....WWW?....S.)...D..)..Qz.`0..f..T.t.VVV`ss.0:PQQ.MMM....p8.....`.....H*..#'=.....o.H$.....L&.,?..x.....(%.....c}.0DPPP@.3.....t....=Xb.r.`aa.....dr.E ..u....6,.j-c;11.....p8..(.LJ.d2..n..BaL...(..6.-...e..Z?.<...M...5hmm...\|*.....`4.qjj....d$..CsQtLUUU.%.....N....Wn~~.:....=.....(===..$Z.....h4....$.c.q.LM...xgffl...r.O.....} ....(.Y.{{{.+.2.M..8.P..89"g6...B.l..Z.....o.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBZ3zrM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBZ3zrM[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	763
Entropy (8bit):	7.621723844116318
Encrypted:	false
SSDEEP:	12:6v/7N5fvaQCJmEzDuMi5ld08fuKGi9o4eUTE5xDgic9NEm652PPanadeh7jteQ8c:IBihmEGMi5ltfDPu4E5iic9NEp52kl9
MD5:	CFE739AEAE33DC7C7BB02D24E081F0CE
SHA1:	CBE000F23A34635EF4518C919A234DC4A3635C1E
SHA-256:	A1F6D07C79B387A99C2550B0E24AD030964EB42ACBA18F21F2D790A05499BAF3
SHA-512:	E8CD4F90716E62E4A0A8B9817794F55517CA52EC75F634E55462BBFDFB288076C1992298DB5578C84EC695D3B23BE6FF1AD80EDEEBA8435AAF96B6B32C711C5D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]SKO.Q...s;e:.}.}@.._....hb..b..kw.....M\..t.0j...|"..E.2..C...S..M...s..;.~W..<.....=>.....J.P..?.L.....Pf.eB.BU...@.^"1(..05.]UA0....g..N.....H.K.L..P..z...;N..O.pi<...{oVpc*.[..D...@6.a,2....<..sq.h.h~.s.*..l.@L.....h8.....)$.4.B.*.....3...m.&..H.....1...8.7...0...u..k.)d..\.;@...:m..*.Tc.....$.v..a..v.x.(;{..G...+...QY..L.N....;E.....T..>@r(.;"d...0...../.nT.01...P!...5...P....`...b.Q....k6.*..l....R.....P.Pw.t;..T.R...6[...\l.7'Gpq$...[.Z.%....jb..`e..T.X...C.Y#.W..\.....B.B..mR...p.0.?.J..[.....K...Sl....."B.b.A...@.-..w.`E*.-.w..@<(,Ki.^O...zY^.. 7..4E.oyN..e..'.j.4...4ST .?.D.G....(...C..<.....8E...<?...../..X^c..j....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3224
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	48:5m73jcJqQep89TEw7UxkZCm73jcJqQep89TEw7Uxkk:5nqrehEw7U6ZCnqrehEw7U6k
MD5:	3A35614D9A6156057F7D30C91C1ED4F2
SHA1:	7DDE5D14A15F465C9BFD0B0C0B3416175E69D1BC
SHA-256:	D544FAC44B7B2CD937726C401B5C9C726F900CEF22980A7B39F8756581901B73
SHA-512:	8A31C0C90EF443E3B7AC5B930466CD8CEF1D540D2D436A7DC4D12F386863683038 82A9610A57B2A1CF9AB973DB684FDA0B1831B116EAEB4D86BE816FDD627C8
Malicious:	false
Reputation:	unknown
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2...V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I...u.....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a..&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9...R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21628
Entropy (8bit):	5.304819777739522
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt
MD5:	DDD356C3D15DF3F06EF6772D05ED53D7
SHA1:	4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6
SHA-256:	62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398
SHA-512:	9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D473
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21628
Entropy (8bit):	5.304819777739522
Encrypted:	false
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt
MD5:	DDD356C3D15DF3F06EF6772D05ED53D7
SHA1:	4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6
SHA-256:	62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398
SHA-512:	9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D473
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21628
Entropy (8bit):	5.304819777739522
Encrypted:	false
SSDEEP:	384:3OAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:I86qhbS2RpF3OsfQWwY4RXrqt
MD5:	DDD356C3D15DF3F06EF6772D05ED53D7
SHA1:	4A34AC5B1AD6F7B7A960AA55405625CD60BF4FE6
SHA-256:	62812A69A8398073B8F53B582C04B6FD214D07146A580035611F646E74922398
SHA-512:	9C8C6264D621A6D2EEA15B1BB627D221ABA1CB367030137B00B440E50CB1641B623C6A7E0C49220D2B35AAE93D1DEA4E819046982808BE596CAB7619E947D473
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\de-ch[2].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\de-ch[2].json	
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Reputation:	unknown
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	unknown
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\httpErrorPagesScripts[1]	
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	unknown
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
Reputation:	unknown
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2481
Malicious:	false
Reputation:	unknown
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otBannerSdk[1].js	
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[]).next())})}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otTCF-ie[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
Reputation:	unknown
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AANf6qa[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	432
Entropy (8bit):	7.252548911424453
Encrypted:	false
SSDEEP:	6:6v/lhPahm7saDdLbPvjAEQhnZxqQ7FULH4hYHgjtoYFWYooCUQVHyXRTTrYm/RTy:6v/79Zb8FZxqQJ4Yhro0Lsm96d
MD5:	7ED73D785784B44CF3BD897AB475E5CF
SHA1:	47A753F5550D727F2FB5535AD77F5042E5F6D954
SHA-256:	EEEA2FBC7695452F186059EC6668A2C8AE469975EBBAF5140B8AC40F642AC466
SHA-512:	FAF9E3AF38796B906F198712772ACBF361820367BDC550076D6D89C2F474082CC79725EC81CECF661FA9EFF3316EE10853C75594D5022319EAE9D078802D9C77
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....bIDATx..?..a..?.3.w`.x.&..d..Q.L..LJ^.o...,....DR,.$.O.....r.ws..<.<.|..|..x..?....^..j..r...F..v<.....t.d2.^...x<b6....\.WT...L".`8.R.....m.N'..`0H.T..vc...@.H$..+..~..j....N.....~.O.Z%..+..T*.r...#.....F2..X,.Z.h4..R)z..6.s:...l2...l....N>...dB6.%..i...)....q...^..n.K&..^..X,>'..dT)..v:.0D.Q.y>.#.u:.,...Z..r..../h..u....#'.v ....._&^....~..ol.#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOfJsZ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2490
Entropy (8bit):	7.830846007357338
Encrypted:	false
SSDEEP:	48:QfAuETASNLIt+OSmfUyYuQ8tUnAGtl2hZZL1zG4tTCJ:Qf7EplyyUyfntUnAOlW1zGIy
MD5:	6FA342BB2DAD0272A38CCF9D8B599264
SHA1:	65FEE20BEB7A5735412D9759B2E5FA1CAECA27A1
SHA-256:	74C1C1A5A96916E147002ECA860D303A57942161D3D7F9F2AAAA6A1CF4EB30E2
SHA-512:	2CA505CD6D2B18A510785187B69BED0F3A7050EC15D157AEF187901E1FE149AFFD8A6CF67C1BA628A323CA4252F4D723A4E29D3D5C5BBDF8C06816A78477C3B
Malicious:	false
Reputation:	unknown

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOfJsZ[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.. ..k..7.9_. [. ...0.P....M..'....V..2.. =I...nm../.m.&.SQ0..q.....Y{w}.^...N.5/.,.:.....U...H.U.!..!.D..A.}*[."5D.....Mq.7..k.;....J...f.....8
.iV(.....m%v5..A...c..l.nn...W.....\N|.C.....x^.....#.j|.e..2.5....K...V..FV....Z...1..*....9]..Vfi.3.b....&4Fj.=:d1....7fm-Q....7.t.#6..[....s.,.}.O..e..N....d.m..].ls.L}.:.I)3.0..M.>..F.&.b?.A......
1...]NjQ....k..{x..}...h...</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOfsCY[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	30752
Entropy (8bit):	7.906234754194529
Encrypted:	false
SSDEEP:	768:ITUs9uf7dj9BrZJEhs9zMVbj7xUp+6rqaxiatR8MiCqeB:Izuf7fhPE2zMVbh2rqaJnLiCLB
MD5:	AD584D72D7932711DB1D30832190E067
SHA1:	290EC377BC938991D3BDA888D74666EAD6CBB18A
SHA-256:	848B429A0185010DD921D927A29D5DFE2ED332D379E008CE465FA6508EB35948
SHA-512:	DB034AB85381270E3AFFBAD3B15FB94A9C1E894F2E1A84B13A0FB4D6D66FFDE158B70377068668BD721CA500D6AAB3788CEE6C830A7AFC8C48044A01E6AC2D EC
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..Z`-...P.(.h.......A..J.3@.Z..4.....P........r.n..j.5...}@.9....q@.@..Asp..$.Uj.q..15F....k.`...$..(..]?^.6X...a...<D&$..GZ....z..... ..x..,&.E.X7.:.p)^#.%......ac.{.V#<..].$....4.o.\....Q,.........zCM.-..2m1..x:MZ..$..&].#*...........<...4<..c>.E..>e....s..T..YjV..J...2q.YC.R....r....@pEw....f.X.#u.a]...-...+7..4....V.-0. @%0..C.sHc.h.E...1..&h.h.....@.@.a.I..:pk9#H.">O...l..^H.J...`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgGQ4[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	26435
Entropy (8bit):	7.859283933483462
Encrypted:	false
SSDEEP:	384:IfBCgXWkx0RXMuUEMClBLZq2D3tkInTQu7N6m0eqLi4ivk6guSSi/JR8ypJ/sbrp:IRXsyEMMZq27PQu0myLif86E3/JRFgp
MD5:	BEB948AAC940AF84538BE16878295A12
SHA1:	45E817191F2714065A688665051C407182E4066B
SHA-256:	58F3F86421160FE5176BB87B8F61B2913FD8F424EEDF71276CE6A8D81CC706C1
SHA-512:	4FF5E0F33C3744AC4AAEC39CBE1845F4053EE7ADCAF439CB6C16D38641A24E9212EDA4601FA7FFCB600C1AEFBC2E937DED78108A2DFAB0CD403C4E26B6F0 647
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..j..f.........0..@...qHh..}....LB. .h.P.@.@......Z.(`..P .b..@.........1@....(....A@.......(........(.(......(...4...P.@..%...P.P..@......b..`. .P.@.....@.(.E.-...... R..P..@..E.....@.@.{R....t....w.............(..................(......(....... ...H......R.)...(..........%.....P.@.@..........O...(.....J.(.4.P.@....p........R..P..0.H.4.f......!.OJb.t.l (.P......Z.(......Q@......P.. .a@.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgIQG[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	4394
Entropy (8bit):	7.030110019355473
Encrypted:	false
SSDEEP:	48:Qf5uETAGK88888Z1sHvq2WNK0NVuwmS9CapNiWWWWd:QfQE9GHz0/mSTpNiWWWWd
MD5:	16BDA1AE195B38579F194CD823D801F8
SHA1:	A216736D1818913D2856B46D4FFB45661105AC34
SHA-256:	5923487B64BB2CE31EE68CAC5C68C4FF3992EC21AC7135CA9C84293E3FD711BC
SHA-512:	6C95E99091B76DE8994405AB13BE73427534B83A858FA6B9929419858935B30BBC1686BB60094FA82585646B07497FF83F5777F13CBC5F3D0B0E7DE68382415E
Malicious:	false
Reputation:	unknown

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgIQG[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?....(......(......(......(......(......(......(......(......(......(......(......(......(......(....<...}k..O...Y.3....0........Z......|/.Q...3......I....?.......?.0........Z......|
/.Q...3......I....?.......?.0........Z......|/.Q...3......I....?.......?.0........Z......|/.Q...3......I....?.......?.0........Z......|/.Q...3......I....?.......?.0........Z......|/.Q...3......I....?.......?.0........Z.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgQuh[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>20560</td></tr>
<tr><td>Entropy (8bit):</td><td>7.937929871385382</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:NRsH8HzZZclei6WeMXHl7Sp+fAtdzY8M8D2VCjFjCudbXbVzbO:N0u7cqMXZLi55jo</td></tr>
<tr><td>MD5:</td><td>A01C83C62C30D97DF34FEFBB82A71BC0</td></tr>
<tr><td>SHA1:</td><td>A41A9927BFE2EEE48929AF2CC733F1C08F21F4FD</td></tr>
<tr><td>SHA-256:</td><td>A177ADFF17E51F55AAB7D919C77705142CA703B2E15CE2396597DE6F21D12F5B</td></tr>
<tr><td>SHA-512:</td><td>545FBA728BFDD27CFB811B42150CC0AE7BA644A2407B460CA697A904AAED58E9E9D7D976FA65B1E96D947D22A304BC60EB7AF7B3E1A8BAA82F09D6A3F28323
0E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...=U.I.8<....$......-...P.@..P.9..P.@.?..H...#Ka.>.......:..........q^N[..r......L.m..GX.E(..^H...L.<...\...O.V.%...<.n..f<.~4.H.L@.H
3.'.M....h....=3..=..+_q.[cv..+|"..c.=i.....l...`?...:....-.}.}...V.~.:...soq..SV...FN.?.Wl=Y?..F....&.....1$..Z3.......k.P..g.".......}..S)X.....K}KZ..7R0S..-.r..#..y..i.......$n.c....RH.. c..(..`u..
c.h.....).;....1[...3tQ.?.\`.2.[.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgh94[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>24289</td></tr>
<tr><td>Entropy (8bit):</td><td>7.8927009680659035</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:IpRJkRtiLu2XyZ/QZSplX9F5Y+qa78OfyyT3Yn3SHUvyHaUVhOyKAouCbUqFyBIx:IvKRUK2Xyygph9F55qaLDrY35jUVm34w</td></tr>
<tr><td>MD5:</td><td>E7E05927E7E3C1833D7F9E3B8BF0667C</td></tr>
<tr><td>SHA1:</td><td>91FD68F02453FEB6FBF7BE324C9EF22051900635</td></tr>
<tr><td>SHA-256:</td><td>0861EFDDBA661DF1C1B78A61AD7CBFD4FAD6FDF4B97CC05C8D7859C685EEE680</td></tr>
<tr><td>SHA-512:</td><td>E8CA13376FDCAFC7289E51B3F500681DABF06489099310C84E2107C7700EFE1D34E9CCB0768833EBD866CC48CA252F7152363721524F7280C4478803348E7484</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...>tQ@.u.B.`-.......JBc.JB.P...Lb.@.OM......J8.b...u.b...u .....:....I..C@).. ..0$.A...p....V.*=...X...1._3......y....s....F~..$.#...<br>.......gh.`4m!..fr<.uc.i.....#".%a..".....0..W....E..ec9v#-....I12......;.#.\<..[8.v...R..?{...U.b..9`.Tw....y.HO...P+D..)=.......5.E.j.C..+N....N.<...d8..e`.........p....h.Xk&i.V......m..A.
...h.b.$.*X........... ..4CV .....@.@.4..4.6...%</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgkHA[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>8589</td></tr>
<tr><td>Entropy (8bit):</td><td>7.917883695837637</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:Qo6znNwgr1T/regmhcvAa31b1TMu2UQa9uQEEa1Wkfq1:b6znNvRzycvj1TMurxET1bfq1</td></tr>
<tr><td>MD5:</td><td>464362B49496E353AABF75DA5015B426</td></tr>
<tr><td>SHA1:</td><td>51C5A1291B3B5746BB5602CD19F68ABA7FFCC838</td></tr>
<tr><td>SHA-256:</td><td>3F86873DB8AF0970856EE5493C1712D11444B75DA21B3F90E27495BA0AA4B943</td></tr>
<tr><td>SHA-512:</td><td>D51C63F9D6296FF7035B1D5AFA7973E22250B5A36CB56834F09045ABF87950B4F5F94763578D833B27626AA3981CE0C679C6730AE10CC248CD723E8F5645E2C1</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgkHA[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...Y.&h.....@.M1..`..AH....V..qd.b....J7Bn.....F.[..G,{..m.....S.7..xy..j]^~...z.\.U2w.*4...>y...G....#.}+M..<.+...G.....-.....v..... o..B.,.....q..n..f.bkV.cT#..[...lJw.....D.;q.S..(.....!..c...v.\....q\].h.\.n....8...ihk....F....x.y...=.z.m.H.2M(.....C$8..y5zc.R.....@.4..`..f..I..O.3E.l.i..p#.T.....>a..X.2[7.b.A..4..E.]3g.Z2.. ....0...q....._....WX.E.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOgmIX[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	12089
Entropy (8bit):	7.904789531773816
Encrypted:	false
SSDEEP:	192:QtIaSD1Y9EN+brlhrr8hJ+sDbecdnERkmMtGLhsDmZrgnbLGKnVDXZJ/29qtJXmq:+IaSD1XEbYn+sDbecy/MtGLhrdWdX/2A
MD5:	545034BC80A1AACF34CC4EDC5C66F0F4
SHA1:	AB11903457FF4F7CCF18CD685EF33CD037BF1965
SHA-256:	AE3C9594D1A49BB4B2F04659BF6131D989BE980275C1E12DF7683A2FE804E4B9
SHA-512:	EBA05B272F6FF630B31551EC7508B470F18B1817B30988D74B1A80FB4C5BA220E153CBED4E9BE5FC6638B26178E80934F1A2872F69898FB33B916D86CB54E8FA
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..zb..Z.J.Z.(.h.(.....@...C...zS.6..R.>d>..."....p..h.....Y..QrUW$.).....f1K[Y.e.d.....U...!...{.....P.t{y5e....vo.]RD...c..#s..g...Y.. <)o#.....?...W.kH.{;.i...6...c_|f..Y=.J.l\X.....(..)\..(..P..... P.I&..(.h.....@.....Z.(.....(....Z.;S.....)..1@.I4.C-.Jr...E."..2J.M..I..9..x.4.m..d.#..O...8V.N....R.6r.....g..I..[M[bH.$.....;=.....M.....(....(...

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.251166232775736
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	MGrYFpGLQ7.dll
File size:	136704
MD5:	8c7b2ff105963718fa3c26989e206041
SHA1:	831ece0ae6b5e2f373f75352e582abd61b5dd0d7
SHA256:	90d8648b2aac0c837286a4c042f02064cfbb12f45b3dc6b00b2beccc7fc35422
SHA512:	4a2c9b3ce6d2548660189aa247020c9e19127c57fb50859e36f61ea25c9f84ca792820898fae16fb172e1171e02172081f01c1b9b1946daa1310f6a6097e8f13
SSDEEP:	3072:0aWbgDTa51CF1J27oLaPfdWeu0JMNzfpodOCwdAf4:0XMDdJ2hPIeBCj
File Content Preview:	MZ.....!..L.!This -7Aframcannot be run in DOS mode....$.....PE..L..... .....!.....>A.....@.....G..... .....e.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x40413e

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 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:	3c5ce00825859dda51eb5de893c2c46c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb0ac	0xb200	False	0.587671172753	data	6.63369052343	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x440	0x600	False	0.302734375	DOS executable (COM, 0x8C-variant)	2.79332490305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe000	0x1c43a	0x14400	False	0.654079861111	data	5.49862585867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x2b000	0x994	0xa00	False	0.833984375	data	6.65585202764	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/10/21-11:34:16.615251	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49859	80	192.168.2.5	13.225.29.132
09/10/21-11:34:16.615251	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49859	80	192.168.2.5	13.225.29.132
09/10/21-11:34:19.499046	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49863	80	192.168.2.5	13.225.29.132
09/10/21-11:34:43.724298	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49907	80	192.168.2.5	13.225.29.132
09/10/21-11:34:43.724298	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49907	80	192.168.2.5	13.225.29.132
09/10/21-11:35:30.222900	ICMP	399	ICMP Destination Unreachable Host Unreachable			10.200.16.217	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 10, 2021 11:33:32.696270943 CEST	192.168.2.5	8.8.8.8	0xa44	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:36.086319923 CEST	192.168.2.5	8.8.8.8	0xe127	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:36.695192099 CEST	192.168.2.5	8.8.8.8	0x3680	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:36.758147955 CEST	192.168.2.5	8.8.8.8	0xd023	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:39.525027037 CEST	192.168.2.5	8.8.8.8	0xb102	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:40.234529972 CEST	192.168.2.5	8.8.8.8	0xee12	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:41.667709112 CEST	192.168.2.5	8.8.8.8	0xc5a9	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:45.004209042 CEST	192.168.2.5	8.8.8.8	0xdc30	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:46.175139904 CEST	192.168.2.5	8.8.8.8	0xb92f	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:16.528331995 CEST	192.168.2.5	8.8.8.8	0xdcd5	Standard query (0)	ocsp.sca1b .amazontrust.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:19.421375036 CEST	192.168.2.5	8.8.8.8	0x5ea4	Standard query (0)	ocsp.sca1b .amazontrust.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:43.664731026 CEST	192.168.2.5	8.8.8.8	0x68bb	Standard query (0)	ocsp.sca1b .amazontrust.com	A (IP address)	IN (0x0001)
Sep 10, 2021 11:35:15.510564089 CEST	192.168.2.5	8.8.8.8	0x1fb0	Standard query (0)	gstatistics.co	A (IP address)	IN (0x0001)
Sep 10, 2021 11:35:43.641175985 CEST	192.168.2.5	8.8.8.8	0x2bf9	Standard query (0)	gstatistics.co	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 11:33:32.725291014 CEST	8.8.8.8	192.168.2.5	0xa44	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:36.136873960 CEST	8.8.8.8	192.168.2.5	0xe127	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:36.734420061 CEST	8.8.8.8	192.168.2.5	0x3680	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:36.734420061 CEST	8.8.8.8	192.168.2.5	0x3680	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:36.796466112 CEST	8.8.8.8	192.168.2.5	0xd023	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:39.570903063 CEST	8.8.8.8	192.168.2.5	0xb102	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:40.270116091 CEST	8.8.8.8	192.168.2.5	0xee12	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 10, 2021 11:33:41.702008009 CEST	8.8.8.8	192.168.2.5	0xc5a9	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:45.029160976 CEST	8.8.8.8	192.168.2.5	0xdc30	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:45.029160976 CEST	8.8.8.8	192.168.2.5	0xdc30	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:46.203030109 CEST	8.8.8.8	192.168.2.5	0xb92f	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.n et		CNAME (Canonical name)	IN (0x0001)
Sep 10, 2021 11:33:46.203030109 CEST	8.8.8.8	192.168.2.5	0xb92f	No error (0)	edge.gycpi .b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 10, 2021 11:33:46.203030109 CEST	8.8.8.8	192.168.2.5	0xb92f	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:16.564980030 CEST	8.8.8.8	192.168.2.5	0xdcd5	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.132	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:16.564980030 CEST	8.8.8.8	192.168.2.5	0xdcd5	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.199	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:16.564980030 CEST	8.8.8.8	192.168.2.5	0xdcd5	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.191	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:16.564980030 CEST	8.8.8.8	192.168.2.5	0xdcd5	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.204	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:19.446614027 CEST	8.8.8.8	192.168.2.5	0x5ea4	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.132	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:19.446614027 CEST	8.8.8.8	192.168.2.5	0x5ea4	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.199	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:19.446614027 CEST	8.8.8.8	192.168.2.5	0x5ea4	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.191	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:19.446614027 CEST	8.8.8.8	192.168.2.5	0x5ea4	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.204	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:43.695419073 CEST	8.8.8.8	192.168.2.5	0x68bb	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.132	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:43.695419073 CEST	8.8.8.8	192.168.2.5	0x68bb	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.199	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:43.695419073 CEST	8.8.8.8	192.168.2.5	0x68bb	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.191	A (IP address)	IN (0x0001)
Sep 10, 2021 11:34:43.695419073 CEST	8.8.8.8	192.168.2.5	0x68bb	No error (0)	ocsp.sca1b.amazontrust.com		13.225.29.204	A (IP address)	IN (0x0001)
Sep 10, 2021 11:35:15.549719095 CEST	8.8.8.8	192.168.2.5	0x1fb0	No error (0)	gstatistics.co		185.186.142.136	A (IP address)	IN (0x0001)
Sep 10, 2021 11:35:15.549719095 CEST	8.8.8.8	192.168.2.5	0x1fb0	No error (0)	gstatistics.co		95.181.198.158	A (IP address)	IN (0x0001)
Sep 10, 2021 11:35:43.676727057 CEST	8.8.8.8	192.168.2.5	0x2bf9	Server failure (2)	gstatistics.co	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - geolocation.onetrust.com
  - s.yimg.com
- ocsp.sca1b.amazontrust.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49764	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49820	87.248.118.22	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49859	13.225.29.132	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 11:34:16.615251064 CEST	5257	OUT	GET /images/GCf_2BVR4BU/cjyHO8rEu0PLMD/ddrHkS9VDXWI2BqJDWdKp/yP_2BPG48oRDpm0g/SrPkMCydca7d HbV/D9P1tAQMBBq8SvLL_2/BTpaf4v7U/VLIzcVH0j4WxrbYHQOZI/wYP1aj2dECCu_2F_2BC/mIwNPWeBCD7IMCmF 8HTTO6/vdW_2F0_2BicH/w8p9PjDD/HtrueVxg_2FcH01kfOOydSo/XvV_2FKbIAaOsHpHpe/wMhAw.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ocsp.sca1b.amazontrust.com Connection: Keep-Alive
Sep 10, 2021 11:34:16.704760075 CEST	5258	IN	HTTP/1.1 200 OK Content-Type: application/ocsp-response Content-Length: 5 Connection: keep-alive Accept-Ranges: bytes Cache-Control: public, max-age=300 Date: Fri, 10 Sep 2021 09:34:16 GMT ETag: "5f457bf7-5" Last-Modified: Tue, 25 Aug 2020 21:00:39 GMT Server: nginx X-Cache: Miss from cloudfront Via: 1.1 19fefe7d41cfedb99873c7b5cd95d411.cloudfront.net (CloudFront) X-Amz-Cf-Pop: CDG3-C2 X-Amz-Cf-Id: M-AVApgN7Rkkcakg6nE3Nv191fRyl2z84hxWoQa7t177Bd0qw-f4xA== Data Raw: 30 03 0a 01 06 Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49863	13.225.29.132	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 11:34:19.499046087 CEST	5260	OUT	GET /images/U6TeZm2GqJwloJv5oZSeI/2t0wwSFx0OdeCqwq/a5th_2BJswZzpBo/iTJZVc_2BHgWPPB64R/K3cC yKXGA/pha07BC_2FbaaosXoWHU/mqeKc0qKA2IsvzCoLJ0/i_2FxmVXC6GOzmCalRHRBS/X4qBHSkzHz0Gv/sQEy9H R7/NTPicd5UJLmarL1TQsRZspC/zIbC4QSojh/SXfsKqnthINSBZ4Hv/INUqZbTg0z/T.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ocsp.sca1b.amazontrust.com Connection: Keep-Alive
Sep 10, 2021 11:34:19.584824085 CEST	5261	IN	HTTP/1.1 200 OK Content-Type: application/ocsp-response Content-Length: 5 Connection: keep-alive Accept-Ranges: bytes Cache-Control: public, max-age=300 Date: Fri, 10 Sep 2021 09:34:19 GMT ETag: "5f457bf7-5" Last-Modified: Tue, 25 Aug 2020 21:00:39 GMT Server: nginx X-Cache: Miss from cloudfront Via: 1.1 2114f6e9c6130b946922a303f84256b1.cloudfront.net (CloudFront) X-Amz-Cf-Pop: CDG3-C2 X-Amz-Cf-Id: tDWkQ5VaW6mmrKey-_nhcm8ul9DXL3MsBdVucq2JGp99X83JAJ70vg== Data Raw: 30 03 0a 01 06 Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49907	13.225.29.132	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 11:34:43.724298000 CEST	8736	OUT	GET /images/GosV5rx1jUm_2/FeMYZexn/3AHfZUbwKtZ24NdOcSq0RlX/SFVlCboKYZ/q19iLR0UiFTMXXHua/7H DwQVQwW_2B/P2MZpE_2Fn2/TKqFG_2F5mAVKf/ACPvjzozYdfDpfYzdrt73/e9vTiEyeXLfMugv6/YOqbGPGETO_2F yR/6XOvuQnB29hcTxcqfB/1cP6Y9M6Q/pKhEyMS_2BB/ySEZOj.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: ocsp.sca1b.amazontrust.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 10, 2021 11:34:43.813817978 CEST	8737	IN	HTTP/1.1 200 OK Content-Type: application/ocsp-response Content-Length: 5 Connection: keep-alive Accept-Ranges: bytes Cache-Control: public, max-age=300 Date: Fri, 10 Sep 2021 09:34:43 GMT ETag: "5f457bf7-5" Last-Modified: Tue, 25 Aug 2020 21:00:39 GMT Server: nginx X-Cache: Miss from cloudfront Via: 1.1 8513b0b4c77c9a98d13a007d589042ff.cloudfront.net (CloudFront) X-Amz-Cf-Pop: CDG3-C2 X-Amz-Cf-Id: z_2pXzoy7ZS0VGBTG-mGcX3sT0nCP35aKr_YKxPqwR30sLgMBdt69A== Data Raw: 30 03 0a 01 06 Data Ascii: 0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49764	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:36 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-09-10 09:33:36 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 10 Sep 2021 09:33:36 GMT Content-Type: text/javascript Content-Length: 182 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 68c7a7e13b42dfd7-FRA
2021-09-10 09:33:36 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 48 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 38 31 35 32 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 34 33 30 30 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 30 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49820	87.248.118.22	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	0	OUT	GET /lo/api/res/1.2/BWUYr.M5U6.kf035wsX8Lg--~A/Zmk9ZmlsbDt3PTYyMjtoPTM2ODthcHBpZD1nZW1pbmk7cT0xMDA-/https://s.yimg.com/av/ads/1621266752856-586.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: s.yimg.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	1	IN	HTTP/1.1 200 OK Content-Length: 195845 Access-Control-Allow-Headers: X-Requested-With Access-Control-Allow-Origin: * Cache-Control: public, max-age=2592000 Content-Type: image/jpeg Edge-Cache-Tag: 343450606465613470501122455183989970294,415930648339712111872285657998251086336,ae7a14591aaf8d474cdb3f92111c923e Etag: "441833de41dfe8d94ac6f8ce4e751eba" Last-Modified: Fri, 18 Jun 2021 09:15:35 GMT Server: ATS Timing-Allow-Origin: * Accept-Ranges: bytes Date: Tue, 07 Sep 2021 10:42:04 GMT X-Served-By: cache-wdc5536-WDC X-Cache: HIT X-Cache-Hits: 1 X-Timer: S1631011325.879705,VS0,VE1 Age: 255102 Strict-Transport-Security: max-age=15552000 Referrer-Policy: no-referrer-when-downgrade X-Frame-Options: SAMEORIGIN cld_cache: HIT cld_hits: 1 cld_by: cache-wdc5536-WDC cld_latency: 1 Connection: close Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff
2021-09-10 09:33:46 UTC	2	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 96 00 96 00 00 ff db 00 43 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ff db 00 43 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ff c0 00 11 08 01 70 02 6e 03 01 11 00 02 11 01 03 11 01 ff c4 00 1e 00 00 02 02 03 01 01 01 01 00 00 00 00 00 00 00 00 06 07 05 08 03 04 09 02 01 00 0a ff c4 00 49 10 00 02 02 01 03 03 03 03 02 04 04 03 05 03 0d 01 02 03 11 04 05 12 21 00 13 31 06 22 41 07 14 51 23 32 61 08 71 15 42 81 Data Ascii: JFIFCCpnl!1"AQ#2aqB
2021-09-10 09:33:46 UTC	3	IN	Data Raw: 8a 4e e5 8a 81 16 51 83 dd aa a8 00 2d 5f 23 9e b3 b3 0f 8d 4f ac 6e 25 ce c0 89 40 d8 a8 76 7a 66 34 ac 39 30 f1 5d 84 31 c9 0c 66 34 98 bb 90 4f b5 55 55 56 b6 56 e5 04 0b bb 03 8e 3a 59 6b 7a 7f 8e 64 8c f6 7e 77 66 ca 0a b0 ea 0b d2 c5 f5 73 93 7c 56 d0 5f a5 9c 7e cc 70 86 52 85 a4 44 53 cb 9d f2 31 da 37 71 c1 e6 eb c1 ab be 3a ec bc f6 6d 37 d3 6e 5c 84 79 12 eb 8f 31 57 ae 87 6a 73 f8 b1 be 0c 04 c6 91 8c 64 49 11 37 43 29 97 6f 6f de 79 1b 47 36 4f 23 91 f2 0f 34 3c 9f fc 8a ea 2a 39 67 9d 9b cb 48 60 2b 19 03 41 50 33 d8 b7 5b f2 89 fc 68 18 2c 70 c8 57 72 c8 d4 db 8a 87 7e 05 82 4d 02 49 26 f9 ff 00 ea c4 b5 2c 11 86 dc 9c 3e 7c f9 11 eb 07 48 4b 31 a1 16 ab 5b 26 f4 82 4c 78 65 8f 12 49 44 28 f2 3d c7 17 05 9e 8b 2a 82 8b c3 6e 04 1f 1f 8f 27 Data Ascii: NQ-_#On%@vzf490]1f4OUUVV:Ykzd~wfs|V_~pRDS17q:m7n\y1WjsdI7C)ooyG6O#4<*9gH`+AP3[h,pWr~MI&,>|HK1[&LxeID(=*n'
2021-09-10 09:33:46 UTC	4	IN	Data Raw: b9 db a7 f5 10 9a bc 97 ff 00 2b b8 59 15 d5 80 51 b5 0d 6d 74 0d db 3e dd a0 7c dd 1f e7 80 cf 9b 32 80 07 09 c8 8c b6 b7 36 e5 a9 30 d4 99 48 15 17 55 5e f9 d1 bd 3d 48 a4 08 ea 09 28 13 f7 03 4b 22 22 88 76 95 00 4e 25 57 57 57 f3 b0 ad 0f 68 f6 91 55 d2 0a 52 d4 ca 6a fa 58 f2 ef 94 5a c9 f0 04 dc 11 9e 54 ad 45 a9 f2 5e 07 16 77 90 02 20 dc 7b 87 ba 0b 00 36 84 fd 52 6c d8 27 70 e6 ff 00 70 04 0e 96 71 a8 f3 86 8a 19 8a 4b bd 4b 0a bb ec 4b c4 7c fd b5 13 2b 23 21 48 d8 ac 9b 8d ac 21 4e d2 c4 f9 fc 9a f2 48 fe 07 50 52 93 2e a0 87 56 e6 a5 bb 06 22 02 d6 a0 95 33 58 53 b3 95 c8 2d a9 cc 5c cf 09 79 98 d3 22 45 ba 42 db a4 db 17 1b 4b a0 34 05 fe 09 23 fe dd 01 33 26 62 bd fa 6b 6e 43 d2 90 e4 c9 28 09 0c 58 b3 e6 f7 6c f3 d8 df d8 77 28 c6 42 3c 44 Data Ascii: +YQmt>|260HU^=H(K""vN%WWWhURjXZTE^w {6Rl'ppqKKK|+#!H!NHPR.V"3XS-\y"EBK4#3&bknC(Xlw(B<D
2021-09-10 09:33:46 UTC	5	IN	Data Raw: eb b5 35 6c 7d 8b 37 6d 80 f6 ef 48 55 94 ff 00 d6 c1 87 4c 28 e2 00 1b 82 0b ec 2b eb de 90 ba 2d d6 22 75 82 f8 19 19 71 62 c2 9a 86 3e 33 41 3c 45 17 df 11 cc 98 ab b4 ad 66 9b 1b 25 54 95 27 98 df f8 e2 49 1f 77 08 71 47 7b fa d3 6d f5 8f 4e 51 49 0a 17 4b 11 e4 9d f9 d8 db ac 39 3d 0f a8 c1 ac e9 fa c6 21 79 00 9d 37 60 c0 bb 58 47 91 87 73 a6 d8 c8 35 20 72 c8 2f ca f0 05 75 51 3d 38 66 10 cd df 4a 45 ac 83 f7 65 8c 65 8f 2b 1f 87 ea d5 77 b4 0a e0 64 63 60 ea 9f 68 15 9a 1d 50 bc 32 19 58 06 dd 37 bb 14 85 0a cc 0a b9 78 5c 96 20 15 50 00 f1 d3 25 64 a1 58 18 e9 7d ad cb 28 59 84 a5 83 6f 62 c7 cb 62 33 f2 62 74 98 68 d2 41 2c 38 b2 87 c7 69 02 19 03 d9 48 cd 4c e4 02 15 d5 d1 85 03 e4 1b 1e 38 1a 14 43 62 37 bb e4 7b e9 05 52 c2 43 bb 05 7c d7 af Data Ascii: 5l}7mHUL(+-"uqb>3A<Ef%T'IwqG{mNQIK9=!y7`XGs5 r/uQ=8fJEee+wdc`hP2X7x\ P%dX}(Yobb3bthA,8iH L8Cb7{RC|
2021-09-10 09:33:46 UTC	7	IN	Data Raw: 4b 56 70 ae 14 bc 2e 0e 23 41 4c dc df ba 98 3b c6 65 4d 7a 4f b7 05 b1 e4 5c 55 88 80 11 25 11 c4 b1 f3 56 04 74 83 75 1a 07 c0 37 d5 6c d2 4c b7 51 7f 0a aa 74 19 5c 3f bd a2 cf 86 41 13 09 51 2c 75 62 1f a7 5d eb 4b 45 c1 fa 71 a9 88 da 08 25 00 56 39 04 25 a9 1b 68 ec 50 b5 b1 54 96 7d e6 8b d0 1f 8e b3 7c 62 53 f6 94 58 67 e5 5c c3 fe e3 5f c0 aa a1 a8 ca 48 a3 37 e2 b4 f7 02 3a 35 f4 91 3b ff 00 e1 b2 99 04 ac 44 4c 06 e3 7b 45 ec dc ae 7c 80 2a 87 07 f7 79 eb 17 c5 f8 4a 80 e9 e6 73 71 dd 84 6f be 9f fc 52 73 38 8f 51 6c f2 e7 7d 62 fb fa 64 23 c3 0b c8 3b 45 58 3f f0 3c 6d 6b e0 94 a1 f1 cf 93 d5 08 f1 2d 4f 5b fe 3d b7 df 73 a6 45 50 97 ad 99 fb ef 94 3b 34 d7 41 80 ef 1b 72 cb 2c be e1 fa 64 3a ed dd 1b f2 d6 cd 44 21 e2 fc 73 7d 0e 64 a7 0c 90 Data Ascii: KVp.#AL;eMzO\U%Vtu7lLQt\?AQ,ub]KEq%V9%hPT}|bSXg_H7:5;DL{E|*yJsqoRs8Ql}bd#;EX?<mk-O[=sEP ;4Ar,d:D!s}d
2021-09-10 09:33:46 UTC	8	IN	Data Raw: 12 0c 69 24 95 55 56 15 0c 66 51 20 31 47 2b a9 da 84 d1 12 2d 5d 55 03 e3 a8 89 47 1e 16 0d f0 7c bb cd e0 c2 69 7f 19 7c ea 7b f3 be fa 6e c4 c1 26 c9 9a 6c 39 00 87 da a6 03 1d 92 a0 34 8d 2c 6a b6 aa ca 46 dd bf a6 f7 cd 1e 3a 94 b4 04 aa 60 29 06 a4 0d 1c 5a bc c6 63 dc c7 66 b1 4a 14 15 71 6d 39 6d 97 b1 88 7c b9 72 a4 8e 39 22 c7 c6 c8 42 f7 26 46 44 9d b9 12 46 53 da 51 1d 13 50 c5 56 76 7e e0 40 24 74 b4 e9 6b 55 9c 10 72 0c 5a c0 65 e5 a5 77 86 b8 40 97 67 06 e4 f5 60 3f 11 b2 23 94 e0 a7 66 28 e4 0d ba a6 9c c4 43 08 58 f7 da 20 b5 20 50 59 94 35 02 c5 40 3d 77 ed 78 03 b1 50 cc 1b bd b9 9b 1e ac 22 33 3c 33 14 c4 90 f6 7d ed dd 2b 4a 46 ae 3e 65 65 4f 18 44 8a 28 82 38 56 5b 9c 97 14 59 68 dc 96 e4 b0 40 dc 02 6c f1 d0 93 2c e7 db fb 69 1d 5a Data Ascii: i$UVfQ 1G+-]UG\|i\|{n&l94,jF:`)ZcfJqm9m\|r9"B&FDFSQPVv~@$tkUrZew@g`?#f(CX PY5@=wxP"3<3}+JF >eeOD(8V[Yh@l,iZ

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	9	IN	Data Raw: 30 35 cc 29 b6 be 8d 97 8e ad ed 06 e2 95 fe c6 52 68 6f 0d 13 ac 6e c4 51 0c 47 e7 a6 d2 01 71 ff 00 a9 6f 4d 8f 7e 51 5c a9 aa 0a 00 0c 20 ac 5b 30 69 cb 2f cc 7d f5 3c a5 e7 c4 d6 31 98 45 8d a8 e9 65 e7 48 32 94 ac 99 6a ca b9 b1 3a a8 f6 c8 93 45 1e 44 40 d9 1d c6 bf 27 af 49 49 48 50 38 aa 68 0d ab 9e 75 cb 6c aa 5e 19 9e 31 60 52 54 c1 81 20 35 68 2f 7b f9 c1 8f d3 8d 72 3c 7d 4d 65 44 45 74 93 17 50 28 1c 28 99 e2 db f7 49 19 01 54 b4 91 fb 90 1f dc db 94 dd 75 5f c6 a1 45 44 8a 5e ba 8b f2 ee d0 d7 06 ba 94 a8 92 90 41 ec f3 de 9b 03 06 be b9 d3 56 1d 79 a7 d3 24 58 63 93 22 3d 57 0d f6 8a 68 e4 5f bb 44 17 75 b6 61 22 14 f1 c8 af 83 d7 38 36 28 29 23 c5 67 39 3f 3d c5 e0 bc 42 5f 53 9f 2e ec 07 e2 36 f1 f5 01 ac a6 46 48 78 fb 98 3b 5a 55 57 0b Data Ascii: 05)RhonQGqoM~Q\ [0i/}<1EeH2j:ED@'IIHP8hul^1`RT 5h/{r<}MeDEtP((ITu_ED^AVy$Xc"=Wh_Dua"86()#g9?=B_S.6FHx;ZUW
2021-09-10 09:33:46 UTC	10	IN	Data Raw: fc c4 78 8f f8 e5 b2 74 6a 9c 87 3a 9d fc e0 2f d0 58 bf 6f 93 36 a1 3e 43 76 73 70 a5 c3 Data Ascii: xtj:/Xo6>Cvsp
2021-09-10 09:33:46 UTC	10	IN	Data Raw: 48 ec bc cd 3e 3e 27 70 b8 86 82 ac 6f 57 bc dd f9 fc 74 f7 1d 30 a5 92 1b 41 7e ad a6 4c 47 c4 03 81 94 55 f7 14 68 1d d8 55 a8 68 73 ee f5 82 0c 4c b3 3e b0 15 57 66 31 91 d5 36 10 86 35 b2 68 12 42 85 f9 1c f1 ff 00 7e 91 50 2a 43 33 00 0e a6 a5 9e b4 1e dc e1 e9 6b 26 94 7c 66 d4 00 06 d6 87 99 f4 ca de fd 32 22 0e ca a4 68 d2 10 18 3b b6 e4 1b bd c5 19 d8 9d ee c2 b7 9a 08 ab 4a 07 24 8c df 1c a6 05 23 f8 83 57 15 d5 e9 4a 07 ca 35 7f 4d 04 b3 1f fa d0 bd fc da f9 3b de 3a 4d f4 7e 6e ca e1 cd 2a 2c c1 02 28 29 45 23 f2 65 66 09 54 bc fb 2c 5f 03 f3 d6 3b 8b 0e 4d 59 cb 53 a5 3b d2 37 bf 4f 55 13 8a c1 2a 72 37 6c f3 cf 98 8b db e9 62 b2 c2 88 1f 73 6e 54 11 90 fb 80 65 de 08 07 9d bb 3c 15 1c 9a fe 7a a6 fb 58 4a 89 71 76 d3 5d 2b e7 1a 89 2a 74 82 Data Ascii: H>>'poWt0A~LGUhUhsL>Wf165hB~P*C3k&|f2"h;J$#WJ5M;:M~n*,()E#efT,_;MYS;7OU*r7lbsnTe<zXJqv]+*t
2021-09-10 09:33:46 UTC	12	IN	Data Raw: 38 7b 8c 4c ce c0 b1 7c 85 0f 4e a0 e9 15 93 65 a8 2a 68 04 e1 01 da 8f 7c ff 00 0d ae 51 35 36 33 e4 ea 59 11 a3 e2 ce 11 e4 37 08 32 63 c9 92 9b 64 19 8a ac 47 75 5d 58 85 69 02 94 36 54 73 d1 43 aa 61 0a 23 0b d0 81 5c c9 7a db d6 20 85 61 40 24 29 c8 04 e2 ab 6d 4c ee f5 6a 5e 37 21 c7 18 38 c9 9a c0 4b 97 32 7d c3 62 e2 46 0a 08 63 7e da c9 18 a6 5f d8 ae 54 b8 dc 84 15 03 f2 c2 65 32 dc db bb 67 e9 f9 81 99 bf 73 ee 01 42 91 6f 36 04 ee 6f fd 44 84 b8 d0 1c b5 c7 d2 e3 2c d9 c8 eb 1e 26 5f 73 be d8 ca 8a cd 3a 30 01 1c f0 de d0 4b 6e 5b 0a 38 00 a6 4a 31 a8 84 e7 53 ae 75 7a 54 3f 47 bc 42 5c f5 aa 4a cc c5 a4 2a 59 60 40 64 dd c3 e6 f7 f7 c9 a3 1e a1 87 8f 32 e2 ba 44 0c 10 64 45 8b 3a b0 64 c7 91 55 76 bb 80 36 b3 4c 1e 91 8c 9b 56 38 d8 b1 a0 0f Data Ascii: 8{L|Ne*h|Q563Y72cdGu]Xi6TsCa#\z a@$)mLj^7!8K2}bFc~_Te2gsBo6oD,&_s:0Kn[8J1SuzT?GB\J*Y`@d2DdE:dUv6LV8
2021-09-10 09:33:46 UTC	13	IN	Data Raw: 52 99 2f e1 c4 fb f5 d7 6e af 94 5a cc 96 11 88 b7 86 a6 b7 3c e9 cd 8f ea 14 39 d9 cf 14 b9 c4 c6 89 3e 95 99 95 24 65 23 91 58 5b be 6a 22 b8 da 8d bd 19 ca 6e dc 00 fe 07 57 65 58 e5 a5 46 f8 40 ff 00 f9 be 00 11 5c 58 a9 58 46 7c f2 0e 6d df b0 6f af 73 e2 69 fd 2b ac 76 c0 db 2b f7 89 81 89 da cc 04 81 a4 1f b9 96 49 22 63 c5 2c 4c c3 c0 e9 b9 04 24 33 ff 00 90 6d c8 10 84 d7 24 9a 17 16 af 3f cb 0d c1 84 f6 b7 a6 43 22 6b da 24 6c a5 75 08 26 7c 72 c2 c2 0c a2 26 54 dc 79 dd 1e 5a f0 16 89 62 3c 0e ac 65 2a a0 d2 ae 0f 79 3c 55 cc 4e 15 15 33 11 61 e9 cf 2d 7f 10 b9 d1 f3 a5 ce d2 66 4c 98 d5 72 70 b2 71 dd 1e 2d ab dc 2c bf 67 96 0a 1a b6 3f a5 2c 8c 3f e9 27 e2 83 64 00 c4 3d 72 39 02 39 1b 3d b9 c2 ff 00 71 4a 26 d4 76 67 d6 db ed ac 4c 7a 70 c9 Data Ascii: R/nZ<9>$e#X[j"nWeXF@\XXF|mosi+v+I"c,L$3m$?C"k$lu&|r&TyZb<e*y<UN3a-fLrpq-,g?,?'d=r99=qJ&vgLzp
2021-09-10 09:33:46 UTC	14	IN	Data Raw: 55 92 72 18 b8 35 b1 3c ff 00 55 bd db 78 e4 b1 f7 53 50 d7 2d 53 6b 6f 9d 1b 68 d5 f5 8e 4c 18 b9 b9 b1 09 a1 9d 24 c0 8c 19 11 80 11 2b 94 99 61 23 ce fd dc fb ab fb f5 c9 72 88 20 85 3b b1 a0 66 a6 c7 a1 f3 8e 15 e0 0c 29 4a d6 83 be ef 0b 1c 8c 84 96 0d 38 58 da af 32 6c 5b 3b 37 c8 65 de 6f f6 82 68 58 be 7a 70 78 45 de ee 7a bd 7f bd 21 39 85 44 96 56 6f 6e b4 ab 6a 1d b9 46 ef aa 72 ce 37 a7 b5 05 46 b9 e7 c6 59 00 22 d9 11 80 50 a1 79 07 da b7 cd d0 f8 f1 d7 b8 45 62 9c 0b 67 af 53 bf 77 d4 5c 59 f0 b5 2d 7c ec fb fc 1f 68 5e fd 3c 9f 26 7c 98 84 cb 2b 63 61 2b 66 34 96 c5 43 39 5c 67 4b 17 fe 49 2c af e0 1f f5 b3 e3 90 92 10 e1 dc 05 68 77 af 2e cc 2d c1 2c 83 31 20 e6 c0 66 36 d3 f2 3c 81 22 65 ee d5 1e 1d b5 30 ca 9d 4a a1 2a a9 db 62 a0 71 c1 Data Ascii: Ur5<UxSP-SkohL$+a#r ;f)J8X2l[;7eohXzpxEz!9DVonjFr7FY"PyEbgSw\Y-|h^<&|+ca+f4C9\gKI,hw.-,1 f6<"e0J*bq
2021-09-10 09:33:46 UTC	16	IN	Data Raw: 28 ff 00 36 e0 7e 39 b5 43 2f 09 7c 2e c4 3d 6a 75 27 bf 9a 1f b4 50 a2 85 07 a9 00 97 01 22 a2 ba fa 8c 9e d1 fa 6c d4 93 1f 13 be 12 45 2e b1 ba 34 c1 0b 27 04 d7 ff 00 9a 95 b2 c8 0c c8 7c d7 4c 7d c0 90 42 ab d7 2f 86 bc 47 ec a9 0b 2c 5d 98 fc 81 73 b7 ea 36 9f 18 a7 db a3 af ba 20 d3 42 f2 12 2a 09 b6 c8 ab 61 7d e9 ec da 1c 6e a6 70 07 14 3a 82 12 95 28 97 39 30 22 c4 ee f9 e5 a5 76 8f 2e 70 62 f2 ec 1c d7 d4 69 9b 0f 46 8f cb f7 38 f2 c7 8b 1e 34 86 09 56 65 9a 58 a7 65 5c 7f d1 79 92 50 e2 8c 65 e3 f6 bd f2 c5 59 76 f0 7a 3d 52 06 6d 97 37 cd fe 20 2d 2e 60 49 42 b0 a8 2b 11 a3 d3 30 0d 2e 59 f4 ea f1 2d 89 ea 28 1b 03 4f c2 86 59 12 6c 86 8e 19 70 a5 4c 61 1c b3 25 c5 8f 24 5c 07 79 1d 69 cb 1f 61 43 6d ee 1c 90 cc 42 80 4a 49 42 8f 5d 77 17 f3 Data Ascii: (6~9C/|.=ju'P"lE.4'|L}B/G,]s6 B*a}np:(90"v.pbiF84VeXe\yPeYvz=Rm7 -.`IB+0.Y-(OYlpLa%$\yiaCmBJIB]w
2021-09-10 09:33:46 UTC	17	IN	Data Raw: 36 0d 7b d8 87 fe e3 e2 5f ea 94 2a 57 1c 85 25 e8 b2 4a 6a 01 a9 07 c9 f9 06 de 26 be 9e e4 e3 64 e9 ba 86 13 aa 1e ce 44 53 53 50 68 d2 47 68 32 29 3e 01 46 52 df 8a f2 78 1d 57 7d 45 04 4d e6 a7 07 9e ed ac 17 81 5a cc a1 47 1a 54 69 4c ee ec c4 36 95 86 47 d2 d9 64 d1 3d 7d 3b a4 6d 01 c5 83 29 2d 07 c0 99 79 4f f3 57 bd 24 5a f1 57 64 5f 55 df 50 40 3c 32 54 ff 00 c4 16 0d 7e 56 f6 83 cb 52 7e f8 18 19 e9 7d 43 9b 0e 96 7f 38 b4 de a5 9d bf c4 b0 f0 30 de 56 3a e4 70 6b 39 6f 23 db 19 10 c6 72 a3 f3 6a cc 17 b8 3f cd b5 9b f9 ea a7 86 07 f9 3b 0f e5 95 46 ee d9 74 30 e4 d5 e2 c4 92 08 0e da bb 16 35 a5 ad 4f 48 56 6b b2 26 16 a9 ea dd 39 6f 22 19 74 bc 59 a2 2e c7 bd 16 40 4c 8d ae aa 58 92 92 46 4c 65 81 f8 50 40 be af 64 91 32 50 6b 54 3f 25 57 95 Data Ascii: 6{_*W%Jj&dDSSPhGh2)>FRxW}EMZGTiL6Gd=};m)-yOW$ZWd_UP@<2T~VR~}C80V:pk9o#rj?;Ft05OHVk&9o"tY.@LXFLeP@d2PkT?%W
2021-09-10 09:33:46 UTC	18	IN	Data Raw: b5 9c 92 14 32 a3 03 44 85 3e 0d 75 12 e8 27 16 65 c7 b7 c0 fe a1 91 61 a3 0e bd ef 14 6f 5d 49 70 f1 f2 73 24 0b 34 93 c2 21 85 91 44 6c a7 ba 48 1b 05 85 0f 4d b4 73 6a 06 eb 3d 49 cb 36 50 65 87 66 bf 91 63 6b ef 10 3a e9 13 be 0e 20 90 8d b1 e2 63 cb 15 0a dc b0 92 ca 17 cf b4 96 0f e4 00 77 0f c9 20 05 29 51 ff 00 2a 37 2b 9a d7 95 3d 63 ae 03 20 e7 ce f9 9f 31 e6 c2 30 c1 20 c7 5d 47 51 30 03 fe 2b 2f d8 62 b7 72 96 2c 5c 32 a9 23 24 63 9d c2 96 88 3e e0 2b c0 e8 4a 52 9b 91 73 57 a5 47 97 79 41 12 c8 35 a3 a4 da b7 de d9 33 9b 75 0e 0f eb 79 a0 19 d9 cd 8c 4b 47 2a e2 46 c4 30 6b 65 c7 46 de 00 ff 00 ad 89 43 cf 14 07 9e 9c e1 d8 83 b3 be ad 71 7d 7e 22 bf 89 2b 49 7d 74 f2 a7 ce 7d 20 30 a8 8f 1f 0b 9b 79 e4 3b 81 20 85 46 60 bc 01 47 77 03 69 be Data Ascii: 2D>u'eao]Ips$4!DlHMsj=I6Pefck: cw)Q*7+=c 10]GQ0+/br,\2#$c>+JRsWGyA53uyKG*F0keFCq}~"+I}t} 0y; F`Gwi
2021-09-10 09:33:46 UTC	19	IN	Data Raw: 82 18 b5 7c 69 82 62 99 bb 47 71 53 93 c9 73 72 59 53 22 da c8 5a 53 4a 4d 82 14 8b 00 f5 31 34 02 71 79 36 be 9e f0 a4 ee 15 40 26 64 b0 05 41 cc 5b 5c eb 4f 6e 5a 8b 91 83 95 36 f8 98 3a 49 13 24 6f 24 8b 09 59 a3 2d bc 18 c8 b0 b2 32 83 bb 70 1b b9 e4 f4 25 94 a8 8c 1d ed de f0 70 16 90 26 93 5a 78 41 2d 9d 0b 5c 6d cb 50 23 c8 cd ca c3 8d 50 10 a1 ac b9 7b da 96 09 86 4e 03 06 07 75 16 e6 e8 73 5e 64 95 a9 34 62 c3 40 fd f3 8e 99 69 9a 52 a0 c4 9a a9 e8 c4 e9 9d 4f 3f 76 f5 26 b2 ef 16 32 49 8c a0 45 b6 37 90 4c 1e 29 6d c2 86 f0 3b 6c af 27 04 5d 5e e3 56 68 c9 5b a6 ac 0e 84 81 9d fc ab e6 d1 15 48 00 a8 96 b0 04 0e 5d 29 ec 3a 08 9b c4 d5 56 31 1b 24 93 88 e3 96 38 1a 37 7e f0 45 8c fe 90 25 c9 b8 98 fb 0d 9e 2c 7c 57 52 0b 63 76 ea e0 ee 7f 76 84 Data Ascii: |ibGqSsrYS"ZSJM14qy6@&dA[\OnZ6:IoY-2p%p&ZxA-\mP#P{Nus^d4b@iRO?v&2IE7L)m;l']^Vh[H]):V1$87~E%,|WRcvv

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	21	IN	Data Raw: c6 ca 15 3e b6 f4 89 92 ac 36 6d 6b d0 b0 ee 90 80 f5 39 79 32 9d a3 47 67 85 b6 33 3b 52 ab 21 50 8c aa 15 b9 64 dd 64 f1 b8 df 1d 32 84 60 14 b1 01 86 e7 99 e5 ce 06 70 80 71 33 5a 95 eb 46 cf b7 14 42 fa db 14 cb 85 9d 0b 45 7b c4 84 10 b6 00 a6 05 49 16 78 5a bb f2 7c f4 dc 82 02 c6 56 fe bd 46 d1 5b c5 25 c3 8f e2 1d eb 56 cb 47 ec b5 23 83 3f d5 76 93 f6 de ac c8 c8 8d 02 ac ab 24 6d 22 b2 a3 2b 02 d2 47 e7 82 aa c8 09 00 59 3f 83 d7 d3 fe 80 b0 b9 49 4a 4b f8 43 bb e8 c4 9f 3a 53 38 f8 cf fa bd 02 5c df b8 52 40 2e c6 e6 e1 8f 97 b9 dd 95 ff 00 4a f3 73 32 a4 d4 9d 16 39 a2 c9 d0 e6 9b 20 d6 c6 82 5c 69 f1 54 ca 09 f2 46 e2 cd ff 00 50 b6 af 3d 4b eb 52 c2 40 60 71 59 f9 33 69 af b6 f1 4b f4 8e 24 cc 18 43 b5 89 63 93 7b 82 fe da c5 8d f4 5e 11 1e Data Ascii: >6mk9y2Gg3;R!Pdd2`pq3ZFBE{lxZ|VF[%VG#?v$m"+GY?IJKC:S8\R@.Js29 \iTFP=KR@`qY3iK$Cc{^
2021-09-10 09:33:46 UTC	22	IN	Data Raw: 40 09 21 43 4e 9a 5b d2 3d 32 6c 53 41 bb 8c 46 da af da c0 81 67 c9 03 fe dc 5f 37 d1 94 c1 2d cb de 38 9a a8 ab 2b 37 94 66 14 11 03 fb 4b 78 14 4a 1a 07 68 e2 b9 e0 10 0f f1 c7 4b 2c 38 a6 bf 98 32 02 82 81 00 9e ea 79 57 ae 55 80 6f 5b ca cb 85 89 19 21 53 23 2d 0c 94 48 12 ec b3 1c 35 6d c3 39 56 22 a8 85 1f 1e 00 e0 3b 5c 0d f9 d7 e7 9e b7 9a d2 43 11 53 47 66 7c ef cb 3d 05 e2 ae fd 6d cd 5c 68 74 3f 4e 87 92 5c bd 56 61 3e 6b c2 4a 08 b1 95 90 f2 54 58 55 b0 00 34 2e c1 fc 75 14 61 15 7a f3 6e f5 88 9c 5f 70 00 f8 5c 6a d5 66 cf a9 da 39 41 f5 fb d4 11 eb be b7 d5 52 12 a7 1b 47 8d 34 f8 64 55 42 24 96 38 c2 bb 6f 4a f7 01 ec 20 a8 20 dd 92 3a 94 da e0 3f fa 87 ce a6 b7 87 00 2c 18 16 11 57 35 72 d3 4d a7 63 49 1e e8 cb 77 8a d9 dc 56 12 42 6e 1f Data Ascii: @!CN[=2lSAFg_7-8+7fKxJhK,82yWUo[!S#-H5m9V";\CSGf|=m\ht?N\Va>kJTXU4.uazn_p\jf9ARG4dUB$8oJ :?,W5rMcIwVBn
2021-09-10 09:33:46 UTC	23	IN	Data Raw: 62 cd e9 dd 7b 06 5c 19 20 89 a1 58 f3 b1 64 05 48 a2 db 50 fe e6 f8 b0 ad fd ac f5 53 30 4e 90 Data Ascii: b{\ XdHPS0N
2021-09-10 09:33:46 UTC	23	IN	Data Raw: 0a 02 16 5d c6 24 82 46 e6 95 a0 ee 91 71 2b 89 92 b6 38 90 ee 4e 55 6a f7 f2 61 97 a7 fa 81 33 37 42 b2 c3 90 17 73 7b 72 96 18 94 93 7b c0 04 db a8 fd a0 bf 92 40 07 ae 4a fb 8a 43 1b e9 9f b5 75 39 7b 43 89 9a 92 1d 0c 46 d4 f8 d2 27 60 d4 21 54 66 99 96 15 52 ae a0 37 7c bd 8d a5 d8 17 23 68 5f 9b 0d 64 f4 25 4c 0f 84 8d 41 c4 1a a0 ea 0b 79 43 09 a2 d0 42 c0 7d c3 0c c8 3e 87 b3 12 58 f3 e3 4c 9d 90 b2 24 45 cb 99 22 09 b4 c6 47 e9 a8 55 6d aa bb e9 ad 98 15 04 06 06 cd 81 46 5d 40 00 93 4a 00 e0 e4 7a 5f 3f 28 77 11 c4 41 73 66 2c fe ba 72 fc 46 2e f1 8d 84 4d 47 77 77 6b 3b 6e 92 43 c9 16 46 ea 36 00 e0 90 07 00 7e 60 0e 17 a0 53 db c2 e4 0d 1c 6f af ee 18 96 92 92 0d 07 86 a4 9d 4d 03 6a 05 44 7b c5 5e e4 c1 e3 21 6c 01 23 02 09 0a cc 0c 8a ea 69 Data Ascii:]$Fq+8NUja37Bs{r{@JCu9{CF`!TfR7\|#h_d%LAyCB}>XL$E"GUmF]@Jz_?(wAsf,rF.MGwwk;nCF6~`SoMjD{^!!#i
2021-09-10 09:33:46 UTC	24	IN	Data Raw: 6f 40 5f ae 43 21 4e b2 4f d5 e6 a9 4c 95 1c 39 87 21 b5 70 da 5b d3 6d cc 8f ae fa fe 3e 49 d3 9f 39 b5 2c ac 93 14 18 93 45 0c b9 dd 8c 57 89 89 19 5a 24 98 f9 0d 0a ce 87 b9 2c 93 2e e7 6a a2 2f 6f 49 ff 00 b1 48 2c a9 45 20 58 94 96 6d 46 af 40 34 d3 47 13 c6 a9 54 13 6a d6 c5 57 a7 f7 ad a0 a7 d3 bf 55 3d 4f 06 a5 16 7e b1 e8 99 33 70 db 15 53 13 5e f4 84 11 e8 ef 8e ce 8c 21 6c bd 1f 3f 37 0d 32 19 58 7b 84 2f 1b 86 3f b4 75 09 dc 37 0c 12 c9 5c bc 65 9c 0c 2e 3a 69 ad 76 2d 0c a3 8a e2 6f 85 6c 2a 49 b5 eb b1 d0 06 11 21 a4 7d 64 ca f5 81 ce 7d 3b d4 1a 8e 8f 9b a3 30 33 e1 6a 58 53 e1 41 42 72 b2 2e a3 8d 26 74 c7 64 82 23 ba 5c 55 74 a2 07 71 87 26 b8 7d 3d 28 26 63 d2 b4 6b bd 2d 43 7d 29 9c 59 4b fa b2 f0 84 00 45 89 39 06 2e 74 db e2 09 f4 2f Data Ascii: o@_C!NOL9!p[m>I9,EWZ$,.j/oIH,E XmF@4GTjWU=O~3pS^!l?72X{/?u7\e.:iv-oI*I!}d};03jXSABr.&td#\Utq&}=(&c k-C})YKE9.t/
2021-09-10 09:33:46 UTC	26	IN	Data Raw: 43 b7 dd 41 7e 07 47 54 e2 06 02 18 16 21 56 fe 47 d6 cd 5e 7a 40 93 2c 27 c4 f8 b0 be e7 46 d9 af d6 fa fa fb 96 97 4a 86 3c 73 18 1d 96 88 39 6b 77 97 1c 09 a3 e2 c0 64 9e 36 a1 e2 b6 9e 7a 1a 50 52 a0 48 f0 ae bc db 53 af 5d ed 58 9f dc 4c c4 a8 20 36 1b eb a0 07 3b d3 7e 90 53 e8 4c de ec b9 5a 6c 8a a4 6a 58 b2 65 40 11 68 45 91 00 26 54 00 f9 68 9e 32 17 9d bb 5b 82 28 92 45 a0 2b c4 08 1c 8e 7e de ba eb 1d 92 5d d2 41 6a ec 29 df ae d0 f8 f4 4e a9 fe 1f a8 66 42 76 a2 e5 c2 aa e8 ae 42 94 94 7b 52 fe 01 7d c0 d7 00 9b 07 a1 89 6a be 22 c0 ea 1b 95 e0 13 a8 48 2d 52 05 7a 7c c7 43 be 93 fa 89 32 b4 74 81 a4 69 1f 4d 58 f0 e7 62 e4 83 8e cc 16 09 90 12 49 50 4e cb af 2a 79 3d 5b 70 ca 61 47 ca d5 39 9c c1 7a 79 eb 14 7c 5a 0e 23 84 3d 28 d7 b1 7f 5a Data Ascii: CA~GT!VG^z@,'FJ<s9kwd6zPRHS]XL 6;~SLZIjXe@hE&Th2[(E+~]Aj)NfBvB{R}j"H-Rz|C2tiMXbIPN*y=[pa G9zy|Z#=(Z
2021-09-10 09:33:46 UTC	27	IN	Data Raw: c7 b2 88 eb 10 8e c9 37 74 94 fe 2d 21 60 0f e2 92 0f 4d ba 6f d6 2d b8 49 02 64 a7 6a 9a 24 59 ce 56 d4 d3 d6 1a b2 7a 1f d6 9a ce 1c 8b a9 68 59 8f 86 c6 28 e5 38 da 72 e5 e4 ca a8 a0 77 e5 ef e4 42 67 89 36 29 38 f0 94 32 0d c0 ee f1 d2 8a e3 24 a2 66 2a 79 83 ad ad a7 33 16 69 e0 27 4f 97 85 8d 1a 96 e5 7e b7 62 76 80 dd 4f e9 f7 a9 23 c7 c8 c7 d1 f3 a0 9c e3 21 0a 27 f4 a1 d1 e5 80 b3 31 0a a5 da e5 ed 30 ed 90 fb ee c3 06 22 ad fe 1f 8d 42 88 7d db 96 5b db f5 08 71 1f 4f 9c 80 40 2c 45 5a ce da ee c2 99 64 6e 21 25 a8 fa 7f d6 b2 3a a7 aa 75 bd 5f 4b 89 04 8b f6 98 98 93 61 63 55 83 1b 34 98 6a b1 48 cc a4 51 66 2b c9 b1 75 56 a8 9f 20 86 71 88 d4 d4 3f 22 de 95 a8 0f ac 54 ab 85 9b 89 41 40 b0 fc 69 97 94 07 64 7a 37 58 c2 ca 77 c1 d5 8b 24 c6 32 Data Ascii: 7t-!`Mo-Idj$YVzhY(8rwBg6)82$f*y3i'O~bvO#!'10"B}[qO@,EZdn!%:u_KacU4jHQf+uV q?"TA@idz7Xw$2
2021-09-10 09:33:46 UTC	28	IN	Data Raw: 15 1f d7 df d6 46 97 a4 65 47 87 a0 68 7a 8f a8 65 7c df b1 95 31 67 83 02 79 55 45 7d cb 1c 88 a4 86 23 dc 14 a1 ca ed fd cc 80 10 0f 93 8a 63 25 0e 49 6a 8e c4 09 52 90 81 89 53 48 06 c0 1a 6b 6a 8e 99 eb ad 48 fa a9 fd 5c ea 73 47 92 26 d4 74 5f 47 66 63 a3 f6 b4 bc bc ed 5f d4 1a 93 7b d4 a4 f2 e5 e3 9c 3d 32 29 08 0c 1e e0 ed 00 7f 4f 75 5f 47 ff 00 61 c4 12 14 47 86 dc ef 7a 8c b9 e8 ef 00 57 19 c2 21 25 01 58 d6 03 b9 0f 5a eb fa cc 47 38 fd 63 fd 55 fa 97 2b 3f 51 ca d7 75 dc 23 81 8a 64 5c 6c 6f bb cd 9f 3f 3f 64 a0 c6 d8 98 22 46 8b 03 10 ef 3b b2 e7 5f 7f ed 85 6d 83 1b ee 17 e9 52 95 29 cd e9 88 90 fd b7 58 cc f1 7f 59 28 99 87 47 6a fb 79 02 3d 36 aa 7e ae fe a1 fd 4f ad b1 cc 74 c5 d2 34 bc 5c 86 9a 39 b0 d7 54 4c ac b8 8b 10 21 2b 1e 4b 24 Data Ascii: FeGhze|1gyUE}#c%IjRSHkjH\sG&t_Gfc_{=2)Ou_GaGzW!%XZG8cU+?Qu#d\lo??d"F;_mR)XY(Gjy=6~Ot4\9T L!+K$
2021-09-10 09:33:46 UTC	30	IN	Data Raw: 6c a4 a6 66 2a 12 a2 1b 73 fd 0a b6 96 63 16 3b d0 99 cb a9 7a 6b 23 1c 97 4c ec 0d 78 e4 c7 96 1b 7c 4e f1 b2 72 0f 06 27 64 3b 19 2b 92 3f 1d 65 fe a3 27 0a ca f3 05 8b 74 bf 42 d6 d7 58 d3 f0 93 5c e0 2d 40 03 59 f2 ea c1 af e9 78 b3 98 a7 ef b1 b1 e3 9f bb 8d 23 42 30 a5 21 8a 2c 93 ac 72 98 df b6 0d fb 25 8d 37 5f ef 59 14 01 cf 54 81 08 33 31 2a a1 de c1 e9 0e 2f c0 95 a7 57 2c 28 2f 6e bc a1 3b f5 09 26 c4 c7 c5 8e 48 42 66 69 93 2a 53 22 b7 72 3c 84 75 49 ce f5 3d b6 50 55 d0 f9 b4 0a 07 1d 5f f0 6a 42 c0 52 3f 8d 00 1c 8b 1a e7 bf 48 a8 e2 43 24 75 2d cd 59 53 cf 78 07 d5 85 83 a8 09 4e 5c 33 e1 e3 e6 0e ce dd c9 38 8d 53 35 54 ad 82 54 09 a6 0b 47 6b 29 15 e7 ab 11 75 74 7b d4 d5 bd 36 ce b0 94 2f 22 ef 62 e7 e6 66 61 ce d9 06 2c 51 96 d1 82 49 Data Ascii: lf*sc;zk#Lx|Nr'd;+?e'tBX\-@Yx#B0!,r%7_YT31*/W,(/n;&HBfi*S"r<uI=PU_jBR?HC$u-YSxN\38S5TTGk)ut{6/"bfa ,QI
2021-09-10 09:33:46 UTC	31	IN	Data Raw: ea a8 f1 6d ac 6c 61 12 86 77 65 90 c9 1a f7 0b 05 34 0b 3f 2b ce ea 16 3a f2 0b 06 ad ef a3 db 95 6d 48 2b 25 61 d4 40 36 bf 31 6b f9 7b 98 5c 2c 08 b1 fd 9d 28 fb 8c f8 77 aa 82 0f b9 b6 f9 6f fc 56 7d e4 71 76 01 e3 a3 2b c4 97 20 3a 45 4d 6b 7a b6 bc 88 81 06 42 a9 9f a8 1b 6e 1f c8 44 6f a9 25 49 32 33 0c 63 f4 57 26 54 4a 5a 04 06 da c4 11 c1 b0 bc 55 9a 35 60 55 97 86 48 f1 68 10 aa 6a cd 97 5d ab 71 58 84 f5 e9 fb 03 b7 ee 91 1d aa e3 45 95 a5 60 4a 0f 21 72 90 d2 93 4f 1c e8 c0 31 3c 05 11 b1 e7 e2 8d 0e 89 28 00 ad 3b 6e b4 b8 cc 42 a5 45 89 36 cf 4e c5 ff 00 51 17 e9 78 6f d4 1a 6c 0e ad 4d 98 25 26 ce df 7b 00 08 27 8e 54 13 43 cd f1 e7 a9 f1 9f f8 fc ff 00 6e fe 54 cc 08 3c 8c 0a c2 1f 5a ef 71 4a 66 f9 ec 43 b4 48 7d 4d af f0 cd 7e 38 db d8 Data Ascii: mlawe4?+:mH+%a@61k{\,(woV}qv+ :EMkzBnDo%I23cW&TJZU5`UHhj]qXE`J!rO1<(;nBE6NQxolM%&{'TCnT< ZqJfCH}M~8

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	32	IN	Data Raw: 64 73 22 03 bb da 59 40 3d 67 f8 9e 07 ed 90 45 aa 5d bd 29 a8 0c 6b b5 e3 47 27 ea 22 62 d0 d6 03 52 c4 83 b9 df 5e 9a f4 2f d0 fe bc c4 d6 34 f8 72 a4 92 31 23 41 01 da d2 26 f6 66 05 f7 47 11 da 4e e9 0b 02 e1 c8 03 e3 aa e5 4a 0e 42 c9 0c 1e b9 b6 f9 79 53 d2 2e 04 f2 e1 b4 ae 74 d3 fa 7f 28 38 6f 53 33 4a 8f 8f 32 08 c9 dc 62 8b c2 05 60 5c 94 05 89 20 9e 49 db ee f0 39 e8 64 0b 0a 8b 7e a1 f9 4a 04 8f 17 8a 8c 9a 87 a1 7f 2e 70 c2 d2 75 8f b8 89 24 0c ae 26 1b 42 05 21 c3 6e e5 81 3c a1 b0 3d ca 01 23 a2 a1 61 29 20 e8 47 f5 1d 52 14 14 54 e4 85 1a 75 7f 7f cd 60 ea 0c 54 c8 44 cb 81 56 4c 86 07 70 a2 24 e2 f7 92 76 93 60 0d 9b 78 05 bd c1 88 eb c9 94 54 87 ae 67 37 e7 ed 6b c1 a5 cd c2 9c 07 d4 e8 72 cb 68 26 86 4c ab 34 e4 6d d8 d4 ca 2a 30 14 2d Data Ascii: ds"Y@=gE])kG'"bR^/4r1#A&fGNJByS.t(8oS3J2b`\ I9d~J.pu$&B!n<=#a) GRTu`TDVLp$v`xTg7krh&L4m*0-
2021-09-10 09:33:46 UTC	33	IN	Data Raw: 75 1d 33 7b ec ed cd bf 06 0c 90 49 a2 7f 39 e9 af 4e b1 63 3d 13 f4 b3 46 8d f5 2c 8c 3c 48 97 26 7c c9 31 72 0c 89 8e a8 f1 e3 5c 01 63 b4 0d 1a 40 54 b9 68 f6 77 09 3b c7 cf 50 40 42 d4 a5 3f f2 cf 71 cb 4e ba b4 30 92 b9 49 72 28 6c 0e 57 d3 9c 3c f4 8f 46 c5 8b 00 c4 83 4f c7 5d cd 49 3d 0f f8 82 7f e6 92 48 50 8a 01 f6 b7 cf 5e 22 50 05 34 ad 59 83 b9 a7 23 bf 58 0a 97 37 11 52 5e a0 6a c2 a6 cf b5 da 36 35 2d 0a 0c 3c 73 14 1b 89 ef 29 74 87 7c a0 f3 4d b8 72 1e bf 68 0a 08 3f ef d2 ea 94 95 7f 10 28 f4 16 0f 4a 35 06 42 be 79 43 32 a6 2e 63 85 3b dc 65 fc a9 7a 68 3b b8 f3 e9 a7 1e 49 67 31 e4 3c 47 62 ca af 16 c2 a5 0e ed c6 31 c3 6d 00 15 15 57 5d 2e 08 4a 98 f4 de 9f 8e eb 0f 14 99 72 b7 2d ab d7 bf 93 b4 06 ab 95 34 aa cd 18 73 8e 36 0a 89 23 Data Ascii: u3{l9Nc=F,<H&|1r\c@Thw;P@B?qN0Ir(lW<FO]I=HP^"P4Y#X7R^j65-<s)t|Mrh?(J5ByC2.c;ezh;lg1<Gb1mW].Jr-4s6#
2021-09-10 09:33:46 UTC	34	IN	Data Raw: 59 56 30 ee e3 e1 68 02 6a fa 84 b5 05 24 11 97 87 7a 6b 9f 37 ac 74 a5 52 d5 33 ff 00 8b 8c e9 bf 21 e5 1e b3 19 a4 d5 16 38 8c 52 76 65 c7 77 68 e6 59 13 6e 48 51 b8 10 45 17 f2 14 f2 18 91 f3 d4 27 7f 17 f5 ea 22 12 96 a5 cb 73 46 53 66 35 ef 9e b7 89 dd 32 45 1a a3 77 e1 5b cc c4 7c 37 dc a2 36 67 89 9a 4c 72 77 58 76 d8 0f 21 77 8d a3 c7 41 97 63 cf 9c 4b fc 87 23 f0 39 f4 86 66 99 36 5e 46 3c 6b 13 aa cc 21 0c 14 9d c2 5e cb 8f 9a f6 ed e0 37 20 80 47 1d 12 80 68 04 4d b1 cb 52 5e a5 f2 76 71 dd b5 8b 73 f4 eb 57 66 c6 d2 b2 66 9c 46 31 72 31 64 76 01 7f 4c bd 24 8b bf 93 b4 b5 82 48 16 38 f8 ea 48 58 48 b9 6b 82 f6 f3 df 53 72 d1 5b 35 3f 6f c2 49 34 3c c3 ec 4f 5d 2c 1d e9 17 c7 d3 39 9f 73 83 dc 81 e3 76 4d a8 d1 b9 0f 6a 7d cb 25 03 ed 23 95 f2 Data Ascii: YV0hj$zk7tR3!8RvewhYnHQE'"sFSf52Ew[\|76gLrwXv!wAcK#9f6^F<k!^7 GhMR^vqsWffF1r1dvL$H8HXHkSr[5?oI4<O],9svMj}%#
2021-09-10 09:33:46 UTC	36	IN	Data Raw: fe ac 46 81 82 25 53 18 52 08 e5 63 2a 84 02 eb 67 70 5a 36 38 e3 cf c1 f3 5d 29 3f f9 73 3f 03 2e e8 f1 6b 2d 08 50 66 00 9c dc f5 bb db 5c ef 93 c5 8b f4 66 12 41 a7 20 92 34 72 37 c8 a6 b9 85 95 4b 3e e9 0f 03 75 70 2a b9 0b d0 a6 14 fd b1 6e fb 76 cf d6 1e fb 0d 2c 39 72 de da 81 97 4b 79 43 8b 44 cc c6 78 b4 b9 bb ad 52 c3 2b 64 c6 c1 49 65 db bb 11 81 2a db 8e eb 0d c1 66 1c 59 f0 43 f7 c4 ba b5 b2 be fa 43 72 e4 61 50 66 02 80 86 cb cb bd 62 6f 54 2b 83 d9 48 e4 87 26 1c 8c 68 f3 e3 c6 69 56 28 ca 43 3c 63 2a 14 90 50 52 d0 c8 ec 81 87 05 0f c8 e8 5f ee 0c c5 a8 b3 e8 c0 66 3c ff 00 ac e0 f3 38 50 ee 0b 3f c3 6d 04 d9 f8 b8 43 4a d4 72 f0 24 c7 89 e2 80 12 aa 51 c1 88 c6 5a 00 92 1f 70 b4 da 19 6c ab 39 35 e7 a5 66 ce 98 95 84 a4 1a b3 52 9a f3 d2 Data Ascii: F%SRc*gpZ68])?s?.k-Pf\fA 4r7K>up*nv,9rKyCDxR+dIe*fYCCraPfboT+H&hiV(C<c*PR_f<8P?mCJr$QZpl95fR
2021-09-10 09:33:46 UTC	37	IN	Data Raw: 16 f4 c2 29 0e d3 ff 00 0f a7 a1 69 a5 66 1b b2 33 1c 39 ad 80 74 c7 dc 1b f7 d6 23 31 0e 71 31 77 d5 b2 d3 95 ab 6b 67 14 a7 d7 3a 7e 54 99 3a ee ab 14 3d ed 53 52 9d 95 32 24 88 47 f6 b8 f2 49 24 70 45 13 b2 99 92 35 8d 04 8c 78 8e 49 08 f8 51 4e 4b 9a 90 50 54 41 a2 6f 56 e7 bd 1c e8 6b 48 af 9a 85 ab 13 3f 89 4e d6 7f cb f3 1d 60 0b d0 7f 4a fd 53 97 aa 65 67 69 b1 43 2c 8e f0 c6 af 93 0c 93 20 8d 16 ee 25 57 8e 02 e5 ad 98 49 fb 89 b0 4f 8e ac 26 ce 46 04 aa 94 1a fb 0a 3e fd 5d b2 4c 70 ea 76 29 b9 fe 4f ee da 01 db d6 da fa 7b e8 84 99 46 27 d6 b2 04 b9 4c a4 b1 8f 18 2c 9b b7 0d ca 88 5a 45 48 47 0a 91 00 46 e0 58 d8 3d 22 78 b7 0c 2d 51 4b 77 e4 61 a4 f0 6e 1f 21 70 6b ae dc cf 9c 58 1f 4a fd 3b d0 f4 68 17 16 4c 48 23 c7 95 4a ae 5b c8 17 b1 20 Data Ascii:)if39t#1q1wkg:~T:=SR2GIpE5xIQNKPTAoVkH?N`JSegiC, %WIO&F>]Lpv)O{F'L,ZEHGFX="x-QKwan!pkX J;hLH#J[
2021-09-10 09:33:46 UTC	37	IN	Data Raw: 1e d6 23 69 2b 40 f3 d2 b8 d5 35 d9 4b 20 12 05 ad b5 3d 9e 3b 2f fe 33 85 41 2e 6c f7 b5 ad ea 2a 2a f1 a1 f4 0f ea fe 87 eb 5f 4b 61 7a 8f 07 2a 32 fe a2 d5 b5 cc cc 42 65 86 db 1a 1c e9 61 85 11 51 88 58 9b 15 16 66 63 65 9e 41 cf 3c 31 25 0a 5c b7 96 a5 20 24 5c e7 e7 5a f2 a0 36 8f 4f 9a 12 b0 95 00 b0 a2 28 f4 0f 6a 8d cf 9d 61 df eb 1f ab 3a 67 a6 b0 61 79 35 1c 75 cd ca 30 e0 e0 44 d2 20 99 b2 73 19 62 87 b4 a8 41 0a af 6c ec 17 f6 a9 fc 75 5d 37 8a 58 51 48 05 d3 e1 7d 4f ef 95 c0 6a 43 a9 94 82 00 05 81 0e d4 27 d5 cd b7 f4 8f be 96 f5 f6 26 b1 af 36 3c 19 63 2b fc 0f 18 0c d9 99 dd d1 f5 4c 88 c1 78 42 a0 55 ff 00 86 c7 06 53 bf 73 5c c8 68 58 3d 37 2a 72 95 2c a8 50 d2 ed ae 8d 56 f7 bc 75 52 e5 cb c2 4a 99 ed 4d 0b f2 f2 82 ed 63 59 c3 77 92 Data Ascii: #i+@5K =;/3A.l**_Kaz*2BeaQXfceA<1%\ $\Z6O(ja:gay5u0D sbAlu]7XQH}OjC'&6<c+LxBUSs\hX=7*r,P VuRJMcYw
2021-09-10 09:33:46 UTC	39	IN	Data Raw: a5 fc 40 b2 54 94 b8 34 27 b7 b0 f8 80 a4 2d 8d a9 4d 8a cc 64 c7 c9 46 fb 7c 94 92 35 40 56 59 25 8d 24 5f fa e1 b5 8e 87 35 e0 71 d1 56 4e 17 50 77 b6 5d f3 e5 d1 54 61 42 8a 19 d2 a3 e1 d8 8a 13 7d e8 7d 22 48 e5 48 b9 78 f9 1d c9 0c 43 27 12 75 03 73 73 97 fa 2e 0d 0b 05 5c 7c 55 73 c0 b1 d7 25 aa 59 49 01 2c 75 06 b9 8b 16 a7 cc 79 69 50 38 83 35 9b 63 7e f6 e9 0c 9c 5c c7 c3 c9 c7 ec 48 e9 1a 65 bf 6c b5 6d fb 7c 85 1b ad 47 36 1b 70 36 4f 8b 3f 1d 0d 78 ac ec 08 a8 a5 76 e5 ae b0 4c 60 61 0d 84 93 c8 be 5c f9 fc c5 85 fa 5f ae 2c f3 65 69 59 51 ee 04 49 03 47 b8 c7 14 8b 36 d1 1c c5 cd 31 68 9b de a2 bc f8 3e 3a f4 b7 72 1f 27 1b 1b 77 cd b2 85 26 a0 a8 e2 50 71 5a 35 3b 7e 7d 22 f8 7d 30 f5 06 3e 26 0b e1 fe ac f3 63 42 b0 e4 34 de f2 64 89 f6 ee Data Ascii: @T4'-MdF|5@VY%$_5qVNPw]TaB}}"HHxC'uss.|Us%YI,uyiP85c~\Helm|G6p6O?xvL`a_,eiYQIG61h>:r'w &PqZ5;~}"}0>&cB4d
2021-09-10 09:33:46 UTC	40	IN	Data Raw: a5 b5 61 5b c5 a4 bc 25 2c 54 41 2e df 01 b9 d7 d6 18 43 d7 f8 7a 27 dd c6 ce b1 40 ec 21 02 49 14 45 59 1b 42 db 35 6d de ae 76 dd 1d fe 2a ba 51 69 53 94 91 b3 8d f7 b7 a6 9a b4 58 cb 57 db 97 5f 11 a5 49 ad 41 b0 0c 34 f9 30 09 9d fd 44 7a 7f d2 da 8e 3e 87 93 9f 1a 3a e3 c8 d8 4f 3c dd a1 52 12 b1 c0 ee cc 29 e2 c8 e1 18 5a 85 91 18 1a 6a 30 32 15 3c 84 cb 49 2f e7 76 a6 b6 f3 d0 3c 4c f1 89 4b ae 6a d2 92 2a 00 50 67 a5 df bd 0c 24 7e a8 ff 00 5c 1e 9f c4 f4 ab 27 f8 ac 30 6a ba 7b c9 11 08 ed 24 e5 77 32 4e 90 c3 13 33 ca d8 d2 ad 4d 10 16 51 ac 02 48 1d 58 70 1f 44 e3 27 4d c2 99 65 89 f0 9a bb 6e 05 28 6b d2 29 fe a1 fe a4 e1 38 54 87 98 09 17 18 9d b3 d0 e6 ed f3 15 83 27 ff 00 6a 5b e2 e9 59 da 37 da e7 4f 3b 42 62 8b 22 20 c9 04 d0 04 3d a5 25 Data Ascii: a[%,TA.Cz'@!IEYB5mv*QiSXW_IA40Dz>:O<R)Zj02<I/v<LKj*Pg$~\'0j{$w2N3MQHXpD'Men(k)8T'j[Y7O;Bb" =%
2021-09-10 09:33:46 UTC	41	IN	Data Raw: 8a 8a ee d6 a3 d5 b9 12 3a 67 e5 95 60 f5 d6 9b 91 99 98 9f 66 8d 34 98 12 38 8d d5 54 76 a3 c8 85 a1 c8 db 26 d6 12 49 20 2b b5 ae fb 28 57 cb 74 d4 89 a9 25 9e 81 c0 dc d6 97 f2 8e 2e 52 8a 42 88 04 ef a8 ea fa f2 3e 70 84 d7 3d 0f 97 a8 f6 cb 33 62 45 0e 53 34 c2 ca 3e e5 56 64 62 2c 1a 90 1b 60 37 2b 1a b3 7c 74 e2 54 93 4a ed d9 bd f6 b1 d2 02 bc bc e8 6b 4e 99 5f ce 04 72 7e 9e fa 75 0c 32 65 e2 c5 9b 2a 20 57 ee fb 90 d0 3b 49 05 88 24 b7 34 41 22 f8 af 83 30 a1 24 84 80 03 0a 3e 75 be b9 01 f3 0a 2b f9 2a 99 9a 6d 13 f8 1a 7e 16 99 8a 82 28 a3 c5 8c 01 ba 38 23 45 25 81 f6 01 c7 80 9c 13 e7 f1 d7 66 2c 2c 06 52 a9 46 7d cf 2c a9 e9 ac 78 84 84 38 03 1e 26 e4 29 db fa 5a 05 7d 5d f5 13 40 f4 8e 9f 95 a8 6a 5a 86 2e 14 18 d1 cb 24 f2 49 3c 68 fd b4 Data Ascii: :g`f48Tv&I +(Wt%.RB>p=3bES4>Vdb,`7+|tTJkN_r~u2e* W;I$4A"0$>u+*m~(8#E%f,,RF},x8&)Z}]@jZ.$I<h

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	42	IN	Data Raw: 0a fe 05 74 cc 90 a7 4a 6f a8 fc 6f ae b5 8a b9 cd 55 12 c4 ba 70 e5 e5 7e 64 e6 63 93 df d4 5e 64 72 6b 52 a9 9b 6e e5 46 51 c1 12 1d 83 79 f3 57 ee e5 6b fb 7f 3b 7f a5 4b 4e 00 c5 e8 09 f5 24 5b 22 1b 93 e7 1f 3d fa dc d2 89 c4 0a bd 18 ee 6e 2a 33 2d ef 68 0a f4 f2 41 17 a7 fd 50 d3 76 c4 03 4c d0 74 f6 09 4a fb 32 f5 0e e4 b1 70 3d aa c8 bc 8f 3c 9b be 9a 41 51 e2 81 56 4a 6c ed 51 ae 77 fc c5 47 84 48 29 06 e0 9f 4b 0a 65 5c bc a0 8b e9 5e 30 9b 4a ca f7 01 b7 5c 99 f1 d2 30 c5 c4 4e 88 46 e2 28 7b 54 8a be 38 e7 c1 ba ff 00 ab 4c 22 66 1a 1b b7 e7 2b 7e b5 82 fd 3c 15 5e 82 dc d8 da bc fb 30 f5 81 31 a6 8a 28 25 92 68 0e 4a e4 60 34 8c 8b 22 99 5a f2 71 9d 53 ce f8 5d 08 22 ec ee b1 43 8e aa 25 2b c6 45 19 45 aa 2d 5b 53 2b e4 5e 2c a7 06 41 21 c9 Data Ascii: tJooUp~dc^drkRnFQyWk;KN$["=n*3-hAPvLtJ2p=<AQVJlQwGH)Ke\^0J\0NF({T8L"f+~<^01(%hJ`4"ZqS]"C %+EE-[S+^,A!
2021-09-10 09:33:46 UTC	44	IN	Data Raw: 92 db ea 3c 93 cf a0 69 5a 34 4b b0 66 49 36 74 ac c5 83 08 f0 63 66 8e 30 41 03 99 9d 19 ae bf 60 bb ae b8 95 04 b9 6a b5 f4 20 75 cc bf 2e 91 02 71 2e 8f 71 ff 00 f2 9b 64 d6 ad 28 23 9c 3f 58 b5 8c 4c cc 5d 0f 0a 74 dd 97 87 1e 5e 14 93 1f 70 79 1b 78 70 41 16 2c d1 22 c8 35 c7 15 d2 25 8d 71 d7 91 1c e2 c2 5a 9c e6 06 99 1e 5c b5 e9 14 b7 d5 ef 2c 52 e6 63 e3 17 9a 18 71 62 56 00 0a 8e 54 85 d0 8f c9 5a 22 85 71 76 7c d7 44 42 b1 03 95 c5 41 63 6e 7c ea fe 75 83 10 10 41 48 2e 40 24 dd 9d bd 33 af f4 23 85 8e a3 17 11 56 31 26 4b ca 1b 22 71 ee 08 ab 8f 23 b4 66 35 1f b5 42 ad b0 f0 6b f1 d0 55 72 fd fe b4 86 d1 89 3e 22 71 24 e4 28 6f ce a4 f7 ac 46 66 43 10 4c af b9 94 63 e3 cf 8d 1b f7 99 37 14 8d ec 7b 4f ee 3c 91 c1 20 d0 35 c0 ea 48 77 a7 96 bd Data Ascii: <iZ4KfI6tcf0A`j u.q.qd(#?XL]t^pyxpA,"5%qZ\,RcqbVTZ"qv|DBAcn|uAH.@$3#V1&K"q#f5BkUr>"q$(oFfCLc7{O< 5Hw
2021-09-10 09:33:46 UTC	44	IN	Data Raw: 1a 8f 90 2a ba 12 d2 a4 53 3d 46 44 8f 83 e9 58 b1 97 3d 18 49 29 20 b1 ad 1c 1c 8f 5e 43 90 8a e5 f5 47 eb 36 1e 1e 9f 9b 89 90 f9 58 99 4f 8c c9 26 3c f6 9d e5 8d f7 63 ca 84 80 19 a1 73 b4 ae e5 3d b0 09 ae 8f c3 70 9f 72 72 50 b2 08 50 77 d1 f6 a7 5f 2c e1 4e 3b ea 5f 66 5b e2 62 06 5a b6 af 53 af 31 48 e6 a7 ac 7e ab fa 87 d6 5a 82 c7 93 99 da c4 d3 23 91 60 79 d9 a3 c8 c9 55 20 c7 0c 79 22 42 c5 4b 20 2a 59 b7 10 16 cf c7 5b 5e 0b e8 fc 34 96 74 82 5c 65 f9 d3 31 d6 3e 7f c7 7f a8 78 89 8e cb 52 30 b8 a9 b8 f9 6e f3 22 ba fa 9b d6 12 e4 64 6c 83 26 49 33 c4 ac b3 47 3f eb 92 c0 32 b4 8a ea ad b4 ab 10 5d b9 67 03 9e 6c f5 7d 29 12 b8 60 0a 10 02 85 01 61 41 95 ff 00 1c b4 8c 8f 17 c5 ce e3 16 01 52 aa ac dc 5f 97 cd 35 ac 4e 7a 07 e9 47 d4 ef a9 f9 Data Ascii: *S=FDX=I) ^CG6XO&<cs=prrPPw_,N;_f[bZS1H~Z#`yU y"BK *Y[^4t\e1>xR0n"dl&I3G?2]gl})`aAR_5NzG
2021-09-10 09:33:46 UTC	46	IN	Data Raw: 76 1b a3 6a 0c 48 dc 6c 0f f2 a5 79 1c f0 3a ab 5b a5 c5 c0 ab 5b 77 f6 ee 91 a0 48 c6 90 a2 42 43 7b 51 8e f7 ae f0 a5 d7 a2 15 2c 6a 58 99 d5 8e c9 0d c7 61 81 65 61 c8 be 29 54 f1 6c 47 48 29 6c a1 b1 34 15 f7 f4 a7 2b 56 25 c8 29 04 57 33 a3 e7 a7 bd b6 84 27 a8 71 e2 59 24 94 27 66 28 9d c9 8b ba 3b 52 3e d3 b8 95 fd e4 6f 3f e5 22 aa 80 f9 e9 ee 1e 57 f9 31 63 50 2a 48 d4 fb 6b 98 a4 2b 36 79 48 fb 79 8c e9 67 fe e1 1b ea 2c c6 9a e2 40 46 f5 60 42 da ab 32 55 95 3c d5 02 a0 8b e7 ff 00 2b 04 84 82 ed ef df 77 d4 58 c2 cd 99 85 4d 35 1d 6f 98 7b 9e a2 3a 8e 2c 7a 7e 3b 67 64 3a b0 45 b6 a3 fb 50 c6 2c 6d ff 00 3b 2b 78 3e 7e 4f 8e 87 34 9b 27 cb 31 d8 3e e6 24 03 e6 c0 3e 55 e6 7f bc a2 a7 7d 46 fa c3 97 89 32 e9 3e 94 d3 25 d6 f5 c9 98 c1 a7 e9 f8 Data Ascii: vjHly:[[wHBC{Q,jXaea)TlGH)l4+V%)W3'qY$'f(;R>o?"W1cP*Hk+6yHyg,@F`B2U<+wXM5o{:,z~;gd:EP,m; +x>~O4'1>$>U}F2>%
2021-09-10 09:33:46 UTC	47	IN	Data Raw: 8c 15 90 29 2c 00 a0 47 bb 69 e4 8e 41 af 35 d7 28 2c 37 a0 fc 77 a6 c3 6f b8 94 90 58 56 a4 3b bf 2b 5b 37 e5 14 cf d4 98 f8 f1 4b ac 19 d6 9f 3a 24 86 3f 21 67 79 0c ae 37 28 1c 37 69 80 a6 b5 f1 f2 7a 6a 5a c1 a3 55 db a1 1f 9a 40 e7 58 00 42 99 22 a3 b1 6b e7 eb 14 93 d6 19 27 13 4d d4 70 41 13 3e 8f 9d 99 a7 14 20 a4 81 5e 46 7c 57 76 1e 48 49 0a ad 73 4b d5 a4 84 84 b9 39 d1 f7 d6 b9 45 1f 10 aa 36 8f 6e 57 e9 e7 1c ba fe a1 b7 4f a9 e2 ee a0 15 91 99 d5 6c b1 50 11 8f e3 da 3c d7 e0 93 f1 d6 cb e9 4c 89 45 4a ff 00 ab 8d fc f9 d1 d9 ea f7 8f 9c 7d 79 d5 37 c2 59 a9 5a 5a bf 8e b4 d6 20 1a 5c 5c 2f a7 da d6 62 9f b8 92 6d 43 4a c8 86 38 8d 77 57 0b 1f 67 61 ae 89 1d e2 ae 54 92 4e e0 b7 f1 d3 32 d8 ce 76 77 35 f3 0c 3a 57 9d 69 15 1e 21 2d f1 50 83 Data Ascii:),GiA5(,7woXV;+[7K:$?!gy7(7izjZU@XB"k'MpA> ^F|WvHIsK9E6nWOlP<LEJ}y7YZZ \\vbmCJ8wWgaTN2vw 5:Wi!-P
2021-09-10 09:33:46 UTC	48	IN	Data Raw: 7e 68 7f d9 b9 88 21 36 62 de 6f 4b f3 80 cb 0e a0 fb 3f 5a 1d a3 52 7c 62 b2 a0 45 65 2e 77 00 1a c0 21 7d e4 92 7c 16 3f fc ff 00 1d 55 ab f9 1d 1c e7 be 9b 33 f3 31 64 52 4c b0 46 4c 4f 91 ef da d0 15 a5 e3 ae 57 a8 35 cc f9 44 97 00 87 02 24 71 68 f1 c4 84 c8 45 df ef 92 ec 8f 20 01 66 ba e8 49 67 03 5d a0 49 55 d4 3f c6 e7 4e f6 85 bf aa 66 83 26 5d 61 53 df fe 1d 87 92 23 06 cf 65 9c b3 cb 47 fe 92 88 14 71 77 cd 57 9f 14 29 8d 3d 8e 51 d9 0b 42 e6 33 bb 1b 87 bf cd 5e 39 03 f5 0f 53 12 6b 19 41 dd 66 31 e7 4f 2a a8 92 d0 82 e0 11 e3 f7 12 7f b8 03 92 07 4a 99 49 05 8a 8f 96 54 e9 9b fa 31 bc 5b 25 20 02 47 af e2 9e d1 5e 35 bc f8 a7 97 53 28 84 06 ce 83 1c 90 78 62 d0 ae e2 0d 56 d2 4e d3 f1 62 af cf 5c 57 fc 78 5a 80 de ae ef 47 6b 80 df b8 9a 06 Data Ascii: ~h!6boK?ZR|bEe.w!}|?U31dRLFLOW5D$qhE fIg]IU?Nf&]aS#eGqwW)=QB3^9SkAf1O*JIT1[% G^5S(xbVNb\ WxZGk
2021-09-10 09:33:46 UTC	49	IN	Data Raw: 46 cb f4 d7 af f4 df 44 33 fd 61 ce 6c 2f 51 62 ea be 9f d2 f2 7d 57 8f a9 7d b4 ba 6e 9f 9b f6 e9 3f 77 49 98 cf 8d 02 2b c4 9e e7 1a 6e 1b 8e 3c 22 53 e2 04 e1 29 28 20 b1 05 25 26 cd 77 3c ab 58 ad e2 b8 65 4d f1 29 6c 15 49 6a 03 16 15 12 c1 40 31 4f 85 a8 e2 ec a7 60 41 e8 87 f5 2d 89 ff 00 da e6 7f a5 b5 cd 57 d3 fa 46 9f a8 e8 1e 93 d3 7d 31 93 9f f6 6b 06 4e bf ab 98 43 6a 5a ce b1 a8 4e 9b f2 b3 e6 36 31 fd 91 43 8d 12 88 a3 50 00 eb 3f f5 bf a9 cb 98 b4 26 5b 12 7f f2 80 08 c3 40 0e 55 ad b9 45 87 d1 f8 59 f2 e6 8f 12 b0 da a7 2f 72 2e ff 00 02 00 be 8f ff 00 ec e3 d6 7e ba fd 38 f5 07 ab 7d 29 3a e8 da ff 00 a4 b5 ac 8c 8d 1b 31 21 71 1e 5e 46 32 47 27 62 29 62 36 a5 59 4e d9 17 69 de 03 29 07 ac b7 d4 27 ca c0 25 a2 8a 20 65 b5 5b ba 1c e9 4f Data Ascii: FD3al/Qb}W}n?wl+n<"S)(%&w<XeM)Ilj@1O`A-WF}1kNCjZN61CP?&[@UEY/r.~8}):1!q^F2G'b)b6YNi)'% e[O
2021-09-10 09:33:46 UTC	51	IN	Data Raw: c4 87 27 16 39 9b 04 ba 29 9b 23 73 06 ac c9 69 86 dd ce 90 29 65 57 63 6d d6 d1 2a 29 90 93 38 84 13 85 00 03 77 d0 82 d7 6d 6c c6 3e 4b c6 4c 42 e7 2b ec 25 d2 1d 4a 5d 88 23 63 51 43 6f 9b 52 5f ad 1e 86 ce 83 fa a7 f5 de b3 96 20 8b 17 4f c1 d2 b4 7c 3c 71 ff 00 35 71 9a 34 65 ec 23 03 41 a5 66 dc 54 57 16 79 eb 51 c2 32 38 2c 29 ff 00 20 5e d4 f9 7e be 91 f3 ef a8 85 cc e3 4a d6 a3 99 15 37 d6 ef eb 9c 73 8b fa f6 f4 57 ad f0 72 f1 f5 fc 8d 2f 3b 51 fa 7f fe 1a 98 52 46 cb 2f 63 16 5c a8 44 39 4c 04 43 74 4c a6 8a e4 58 68 de 98 50 be af 78 09 73 04 81 31 28 0a 39 92 ce d7 7a d6 97 cf 36 b4 65 78 d9 c8 33 8c b5 4c 20 bb 25 24 28 8f 2c b9 da dd 26 fe a0 7f ed 23 fe ba 7f af 1d 53 e8 af d3 5f a9 df 50 b0 b5 6f 48 7d 3c d2 fd 0d e8 7d 27 d1 1e 96 f4 3e Data Ascii: '9)#si)eWcm*)8wml>KLB+%J]#cQCoR_ O|<q5q4e#AfTWyQ28,) ^~J7sWr/;QRF/c\D9LCtLXhPxs1(9z6ex3L %$(,&#S_PoH}<}'>
2021-09-10 09:33:46 UTC	52	IN	Data Raw: a4 46 ca ca c0 70 f6 60 7c 7c 89 25 c7 78 a8 f1 ec 90 a3 ab 1e 54 90 47 00 1e b4 09 64 a5 2a 50 60 43 8b 90 06 46 9a f5 6f 36 a7 29 2a 04 0d ae 46 bf af cc 45 fa 97 1e 06 d2 e3 d4 b2 52 0e e6 06 b4 98 19 31 83 52 2e 9f a9 63 98 1e 48 c5 15 0a 99 90 ef 91 c9 da 08 b2 77 57 4e 48 52 b1 50 16 26 80 9a 12 33 6e be 50 8f 13 2d 83 aa 8c 08 f3 cd fc fd 1e 91 59 bd 40 e8 b2 cf 81 34 35 f6 7f 75 84 b3 20 15 2c 41 fb b0 33 9f dc db 5c 90 af c8 0a 7d be d3 d5 da 0b 21 b3 3d 1a e3 30 d6 6a d3 9d 22 8e 69 75 3b 06 0a 70 40 6f 9e af f8 8d bd 2d a1 cf d0 21 87 b7 2b b7 d9 cb 8b da ee 0a 79 71 e5 69 60 97 93 63 62 3b 46 03 51 a0 07 c5 74 ba 88 94 b0 ab 07 72 74 d9 9a ee ed 06 48 fb b2 d4 05 7d 48 e9 7d a9 96 46 26 61 9f b7 8d 13 b2 53 60 e5 26 2c d1 92 c5 c4 2e c8 9e ef Data Ascii: Fp`|%xTGd*P`CFo6)*FER1R.cHwWNHRP&3nP-Y@45u ,A3\}!=0j"iu;p@o-!+yqi`cb;FQtrtH}H}F&aS`&,.

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	53	IN	Data Raw: ae 7c fa 69 00 fe aa c6 c5 c7 d2 d1 90 03 26 51 8e 94 92 15 d4 10 14 86 e0 d9 92 c5 30 a0 0d 73 c0 0e 49 ff 00 c8 8a 8b 82 4e 4c 33 e5 02 e2 4a 08 00 30 55 2b 47 bd 6a c3 ad ef 46 81 ad 4f 04 c9 8d a3 1e e2 f3 89 10 91 03 7b a2 38 d9 06 53 63 8b 0a 09 52 47 8a e9 94 97 9e b2 08 3e 15 00 46 a0 db bb c5 7a 92 2f 6b f5 cc 77 9c 69 68 39 0b 9e 4b 85 b9 23 ca ce 10 db b6 d6 89 5b 78 45 36 0a fe 7e 3e 08 fe 43 c4 02 08 51 17 3c ae 40 e7 bd a0 b2 ac c3 30 3a 53 2f 3f 37 80 9f 57 ee 6c 06 0f b8 89 66 a7 20 fe 65 01 87 35 75 7b 4d ff 00 a0 be ac 78 26 6b 83 fc b9 d6 dd f9 56 2a 78 b7 c4 74 7f c8 fc 47 ed 1f 74 5e 9d 90 cf dc 37 a8 62 fd ba 10 4c 66 28 b0 a6 f6 a1 ab dc 0b 96 70 dc 81 5d 37 39 5e 2d 9d bd 2f ed 01 40 21 38 b2 39 e5 a5 ed 0c ff 00 e9 cf 02 59 fd 5b Data Ascii: |i&Q0sINL3J0U+GjFO{8ScRG>Fz/kwih9K#[xE6~>CQ<@0:S/?7Wlf e5u{Mx&kV*xtGt^7bLf(p]79^-/@!89Y[
2021-09-10 09:33:46 UTC	55	IN	Data Raw: e3 5c a3 5d c7 5d 8d 1b 00 0b b9 8d 83 71 d6 13 ea 9c 34 ce 16 71 28 51 c2 9d 3f cb a0 3a 79 35 ae df 4e e0 44 ce 23 87 96 b9 89 a9 4b 58 b7 56 de a1 c5 45 f3 88 2f 50 7d 34 d4 fe 97 7a a7 51 f4 7e a8 b3 4f a5 cd 22 6a 1e 99 d5 25 06 4e ee 99 94 cc 04 7e e5 2b 23 40 54 2b b2 1e 00 1f 82 7a 0f 07 f5 00 a0 ca ba 73 37 24 d3 bb c0 38 ce 08 e1 24 06 36 b3 3d 28 d6 6b d8 7b 46 5f 48 69 a3 07 d5 31 b1 8e 8c ac 63 67 56 31 ad 29 dc 09 55 a2 49 0a 4b 03 c1 fe dd 31 c4 4c 13 a5 ac 97 7c 22 b6 73 a8 f7 e7 5c a9 53 c3 25 68 9b 84 96 00 e7 4f 42 33 f5 d0 47 48 fe 9a c3 28 8f 18 42 ef 72 48 81 45 20 50 c6 9d 69 54 ee 2a c5 68 fe 2a 89 e6 ba cb cf e1 e6 2e 61 29 34 6c b3 6f 2f 4f 56 8d c7 05 30 09 68 4a 88 ab 73 ae 77 d7 a3 03 1d 16 f4 3b 46 f8 78 d8 d9 72 3b ac 2a 0e Data Ascii: \\]q4q(Q?:y5ND#KXVE/P}4zQ~O"j%N~+#@T+zs7$8$6=(k{F_Hi1cgV1)UIK1L|"s\S%hOB3GH(BrHE PiT*h*. a)4lo/OV0hJsw;Fxr;*
2021-09-10 09:33:46 UTC	56	IN	Data Raw: cb 2b 02 92 84 92 ea 15 09 35 2d 93 5f 9b d3 db ab df d3 4f d0 3c 0f a4 7f 4a b4 dd 33 55 c7 11 6b b9 58 83 52 d7 09 54 0e 99 79 7f f1 59 3b 98 5d a4 6e fb 01 04 d2 af 27 83 54 1f 59 22 6a d6 71 5a 8e fa 13 e4 ed e5 a4 6e 3e 84 89 d2 78 74 24 24 97 59 35 15 16 0c cc fd ed 0b 3f ea 3b d2 f8 9a c6 83 38 8f 08 67 e1 dc aa 1e 23 b1 db 72 15 63 1b d1 56 ad c4 ed ff 00 36 db 06 ba c3 71 1c 5a a4 96 0b 48 62 58 e2 d0 0d 4b 1e e8 2f 1f 4e fa 6f d2 d7 c5 99 6a 99 2c 80 02 4f f1 60 e4 e6 40 a6 7b 88 fe 7e 3e af 7f 4c 7e 8f cd 9b 5e d4 b2 e6 95 35 5c 99 24 96 19 31 a2 65 96 36 43 ff 00 0e 8d b1 18 4b 33 7e d3 6b 7c 53 1b 3d 2d 2b ea f3 81 c5 8c 38 d4 86 6d dc e6 dd 98 d3 cf fa 14 85 4a fb 41 22 c1 94 91 65 73 03 6f 33 15 cb d0 5a 3f d5 5f a4 5a b0 73 a5 65 6a da 2a Data Ascii: +5-_O<J3UkXRTyY;]n'TY"jqZn>xt$$Y5?;8g#rcV6qZHbXK/Noj,O`@{~>L~^5\$1e6CK3~k|S=-+8mJA"eso3Z? _Zsej*
2021-09-10 09:33:46 UTC	57	IN	Data Raw: c9 95 f3 34 cc b2 cc d0 e3 c5 34 59 3b 54 c8 e1 59 ec ed 3f f3 19 0d 21 22 a9 1c 13 75 7d 0f 8b 40 28 71 52 03 78 5c b6 1c b3 eb ef 06 e1 14 53 e1 51 1f c8 b9 ef bb eb 0d 39 65 19 de 9b d2 72 58 dc 91 cd 36 14 ab 61 da 24 95 7b 91 92 7e 23 ee 2a 90 0d 56 e2 3a ad 96 70 ad 21 ae 6c 77 ab b6 de 9c a2 df 88 29 32 80 0a 4d 52 e6 af 56 15 a7 e3 a0 ac 42 68 b2 47 16 3c f8 08 df a1 1e 47 dd aa b8 36 ab 98 ff 00 01 47 21 26 14 df 8b b6 e9 a9 83 3b 37 b7 56 b4 27 28 90 35 cb da 08 83 07 50 0b 14 57 69 23 14 c4 1d ef 1c 81 41 14 7f f8 a8 bc 11 fc 7c f5 09 29 48 c4 71 6f 52 0d bd a8 dc f4 8f 2f 10 20 10 43 dd c1 ab bf 2f 78 34 f4 ba cb 8f ae 02 e1 d6 0c b8 f1 7b 2e 41 da 18 c3 c2 7b 8f 00 ca 8e b7 f0 de 05 f2 61 37 3a 8a b7 a3 3f 3e 9d 4c 46 58 98 66 29 27 f8 eb 95 Data Ascii: 44Y;TY?!"u}@(qRx\SQ9erX6a${~#*V:p!lw)2MRVBhG<G6G!&;7V'(5PWi#A|)HqoR/ C/x4{.A{a7:?>LFXf)'
2021-09-10 09:33:46 UTC	58	IN	Data Raw: ad de a2 fa 45 95 aa 47 92 fa 6a 7d 96 0e e6 7c cc f9 21 5f bb cc 21 88 19 13 49 b7 84 5e 57 1e 05 0a 80 fb b6 9e 0f 5a 2e 12 72 51 c8 d3 5e dd 8d 47 5d 0e 7f 8e 90 b5 3a ec 5b 6a f5 1e 5c a2 95 7a 87 d0 da 9e 83 a8 e7 eb 58 8d 3c 60 e4 11 09 81 5d a6 68 f7 98 a0 12 c9 40 34 d3 84 79 1e 30 c1 16 33 4c e7 8e b4 f2 42 66 23 c5 40 40 3a b0 61 e4 c3 f3 9b 8c e9 c5 29 78 d3 42 0b fe fb b4 31 7e 9a 7d 54 f5 b6 16 74 98 fa 66 06 a1 9b 89 19 c5 1a 84 f9 20 c5 8d 82 53 26 33 1b c7 2e ed 8d 29 48 fb 62 08 99 ca 80 6d 87 8e 83 c4 7d 3e 56 1f b9 2c 56 a5 c5 f5 dd fe 1a 2e 78 4f aa cd 2d 2e 64 bc 49 60 0b e6 1f d6 8f bf 95 7a 2d f4 cf fa d1 3e 8c ca c4 5d 5c 4d c6 4b ae 51 92 6d f8 22 2d a5 0c 5f 6b 33 15 92 45 3b 24 16 56 80 63 f8 ea ba 4c ee 26 51 3f f1 95 25 2a 6e Data Ascii: EGj}!_!I^WZ.rQ^G]:[j\zX<`]h@4y03LBf#@@:a)xB1~}Ttf S&3.)Hbm}>V,V.xO-.dI`z->]\MKQm"-_k3E;$VcL&Q? %*n
2021-09-10 09:33:46 UTC	60	IN	Data Raw: 50 55 64 6b 50 2f ba 4d bf 02 89 35 5d 3f f4 b1 85 db 50 72 d5 9b 48 ab fa bf f1 ee ed f8 cf b1 fb 5e d2 fe f7 56 c7 c1 11 0d b3 ca 49 08 cc c5 02 ae e2 0b 35 80 9b ab c7 c7 90 3a 73 88 f1 29 f5 a6 ae 46 5d 6f e5 78 a8 e1 17 f6 4e 2c 8b 90 2d 6f 4a 77 9c 3c 34 8d 06 1c 0d 22 44 c7 8d 23 ac 45 12 4b 56 43 a6 d6 79 03 dd 58 50 ca a2 bc 9f cf 1d 2c c7 30 60 a6 6a 26 2f 16 86 ff 00 03 ba bd 29 15 d3 eb 9f d0 2f 55 7d 55 f4 6b e3 fa 77 56 8f 46 8d 64 92 56 ff 00 87 12 b4 b3 85 98 40 b9 4c c8 fb 93 6b d2 a2 86 df 34 94 79 02 99 e1 38 55 fd c1 3f 21 57 1a 3b d7 f3 b7 28 b4 fa 67 d6 b8 4e 0a 69 44 f9 60 a4 a9 9c d8 b9 ae be 75 d7 68 a3 d8 df 47 bf a8 8f 4f e7 7a 63 3f 3f d7 0d 26 7f a2 c6 2e 16 8d a9 e6 63 c7 aa ff 00 87 e2 e9 30 4d 0e 36 32 e9 59 30 0c 42 63 c3 Data Ascii: PUdkP/M5]?PrH^VI5:s)F]oxN,-oJw<4"D#EKVCyXP,0`j&/)/U}UkwVFdV@Lk4y8U?!W;(gNiD`uhGOzc??&.c0 M62Y0Bc
2021-09-10 09:33:46 UTC	61	IN	Data Raw: 4e 5c c4 ad 58 47 f9 17 a5 b4 7c a2 13 52 94 87 51 0f 97 2d 7f 51 cd 7f ac 5a 67 73 54 c4 c9 da 15 5d 5d dd a3 b0 cc 92 a2 c2 cf 20 22 97 77 b7 8f cd b7 5a 8e 0e 66 19 69 46 da 0d 87 ad fb 68 c7 7d 49 02 72 8e 1c cb 13 47 b0 6c fd df dc 47 30 3e b0 cc 99 1e b3 83 11 62 07 17 4a c7 66 30 c9 c8 28 87 cb 71 cb 92 a1 54 9f 03 e2 cd 75 b2 e0 15 82 4b 1b 90 3d dc 7b b5 af 68 f9 bf d5 e5 7d a9 a7 27 72 05 72 77 6e c7 e1 05 aa 63 43 95 e9 2c cc e9 5c c7 36 56 ad a4 c3 02 bd 09 0e cc 9c 83 2a 0f 80 36 b2 02 4d 58 20 79 ea ef 84 5d e8 c2 e4 10 4d 98 eb a3 3b 46 52 7b 12 5f 3c 40 f9 67 bb 75 b1 d2 0a be 97 44 d0 69 ba 63 2a 31 31 e6 93 29 3b 95 18 97 9e 35 49 7c 01 51 92 0b 1b bb 1f 8e 2b be a8 9f ba b2 3a 52 dd 3d 06 67 d6 2c 7e 90 bc 08 c0 ec c0 6f cf e6 d4 bb 51 Data Ascii: N\XG|RQ-QZgsT]] "wZfiFh}lrGlG0>bJf0(qTuK={h}'rrwncC,\6V*6MX y]M;FR{_<@guDic*11);5I|Q+:R=g,~oQ
2021-09-10 09:33:46 UTC	62	IN	Data Raw: b8 96 be ef 32 75 8c 0b 0d fb 99 15 14 12 08 1b 45 9e 2e b9 f3 cf 41 c4 53 51 d5 ed ca cc 5e 3a e0 d8 8a b9 a7 9d 85 5f d7 94 20 f5 c6 4c af 54 7a ce 6c dc 86 88 68 ba 3f d8 60 ec 6d cb 0e 56 62 96 90 8d d4 a6 4e 46 d1 f0 14 93 76 07 51 12 ca 8e 32 70 82 ff 00 3e fc 8e 6c 05 a3 92 9c 92 1c 9e bb 1e cc 72 17 ea 00 8f 27 d4 5a ba 15 66 68 b3 73 9b 7b 06 53 49 29 2b 23 38 1d bd ce 08 62 b7 f3 e3 cf 4a af fe 32 0a 0b d4 f6 3a eb d2 ad 0f f0 a9 c2 80 14 c4 80 ce dd f5 bf 4c c1 b3 75 38 f5 1d 23 4a d3 c7 fc a1 ad 4f be bf cf b5 b1 d5 e3 dc 29 8e e6 5b 20 55 f3 d0 80 ff 00 35 0a 97 2e d5 19 b3 ed a0 87 92 3f e0 02 ed 30 8e 6c f5 f3 ee d1 31 eb 79 23 cd c8 f4 d4 31 a8 5c 79 72 b1 7d d1 a9 20 26 34 4f 0f 69 95 49 a0 b2 02 4f e3 75 f1 d2 c0 ba d5 47 a6 96 2e 1f f1 Data Ascii: 2uE.ASQ^:_ LTzlh?`mVbNFvQ2p>lr'Zfhs{SI)+#8bJ2:Lu8#JO)[U5.?0l1y#1\yr} &4OiIOuG.
2021-09-10 09:33:46 UTC	63	IN	Data Raw: e6 7a 9f ee 1c 91 68 91 e8 1a 83 ea 92 eb 9a 96 a7 a9 69 3a dc 72 e9 b8 58 b9 3e df f0 dc 88 0c 79 38 33 e3 c4 9b a7 87 71 25 22 ca 91 d3 7f bd 40 23 84 66 2d 2d 88 a4 33 69 d5 c9 6e ef ac 5a 4a 50 6c 18 12 1e 9f c4 6f 6a 66 cd b5 a1 99 0e 4e a5 3c d9 11 31 db 16 5c 8f 20 c7 75 8e 36 44 0a c5 12 59 25 a5 8c 2d 8d cc 82 d8 d0 5e 07 55 d3 d6 97 18 56 5b 9f e0 fb 0f 28 6a 4a 14 01 70 fa 16 ad db a1 a3 36 90 d7 f4 be a7 93 8d 85 30 85 57 21 d2 2e dc eb 14 44 a2 4a ab 58 e5 25 90 d2 c7 13 a8 2f 43 73 1f db e7 9f 7d dc 08 04 80 74 04 76 32 ec 42 fc 47 0d fe e5 dc e1 23 37 6b e8 dd e9 12 5f fb f1 9f 95 8d d8 32 c7 2c 98 c4 83 03 4f b1 7e e7 80 de ef 71 da cc 96 77 02 54 00 07 e7 a8 ff 00 b9 fb c9 34 21 bc 36 60 dd da 2a 26 fd 38 48 50 25 78 89 f1 13 4f 32 45 cf Data Ascii: zhi:rX>y83q%"@#f--3inZJPlojfN<1\ u6DY%-^UV[(jJp60W!.DJX%/Cs}tv2BG#7k_2,O~qwT4!6`*&8HP%xO2E

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	65	IN	Data Raw: 98 fb 61 85 1d 83 c6 9b 25 24 d2 3a 96 b6 f3 d4 f1 27 51 12 1f 4e e1 d1 5c 78 8e 4e 5e b5 1c b3 e7 05 9a 87 d0 3f 51 7a 86 2f 53 64 60 be 3e 1e ab 99 8f 9f a9 c3 9f 8b 0e 4c 1d ad 45 74 6c 8c 3c 4c 95 69 54 a6 c0 1d bb d1 24 7e e7 62 e1 ee fa 89 32 d1 e3 2a 04 96 a1 a8 a0 f7 fc 5e 91 c3 c3 c9 a8 0b ad 5e a3 a3 31 cf 2b 7e 0a b4 2f a0 d9 be a2 d3 7d 2b ae 3b 4b 1e af a4 e8 d0 69 8b c3 17 c7 2d 84 b8 79 fa 74 e8 77 77 95 de 31 34 52 4b c8 75 0c 2b 75 74 a4 ce 2c 89 a0 e2 38 42 58 00 68 7f 17 6b 0b 47 0c 8e 1a 58 c2 b5 39 25 ea 49 ca f4 e6 df 9c 88 34 0f e9 d2 1d 26 4c 53 8d 8b 8f a7 26 03 76 96 15 5d b1 36 39 6e e9 0b 44 85 3d e6 67 61 c8 24 d0 00 1a e9 6e 23 ea 49 6c 2e c4 5e b9 52 8d db 98 6a 54 99 6a 4b 4b 4d e8 f9 1c a8 ed ef a6 90 6b a8 fd 25 d2 26 cb Data Ascii: a%$:'QN\xN^?Qz/Sd`>LEtl<LiT$~b2*^^1+~/}+;Ki-ytww14RKu+ut,8BXhkGX9%l4&LS&v]69nD=ga$n#ll.^ RjTjKKMk%&
2021-09-10 09:33:46 UTC	66	IN	Data Raw: 5b f9 d1 9a 0f 3d 29 99 0e 3e 6e 9c 64 75 db 0c 9f 63 31 6b e6 39 ef b5 1b 51 05 00 f7 21 b0 6d 80 1f 3d 57 71 41 4a 2a 67 a1 2e da 3d ba f4 ce 2c b8 64 60 52 01 2f e1 38 9c bb 9a 58 1d 32 b7 c4 6f ea d0 c5 8f 97 36 3e 38 8c b6 14 9f a4 56 e5 1d b8 dc ce 8c c2 bd aa f0 bb 27 3c d7 1f 07 a1 48 5a ad 95 45 ff 00 2c fc b7 7d e3 87 f9 af 98 83 ed 10 61 4d 89 f6 a6 c0 64 89 9a 52 08 b5 91 19 c1 e4 d1 8c 58 db 47 83 40 f8 eb d3 89 05 2c 48 a6 54 ce 25 25 d8 e9 df ee 27 f4 12 fa 6e 3e 36 9c f4 91 77 b2 d1 e6 72 a0 97 92 57 78 6b ff 00 09 4e 17 f3 c8 1d 13 10 28 d4 f7 5a ed 57 88 94 9c 65 89 6f 9d 1a bd 3e 32 30 5d 55 b0 e5 83 69 66 6f b2 58 64 45 1f e6 8d c6 d7 20 95 e4 a9 ae 07 3f 3f 1d 04 07 48 7f 83 ca e0 e5 04 05 4a b1 cb 56 07 ca 3f a2 c0 2d 15 01 a6 16 48 Data Ascii: [=)>nduc1k9Q!m=WqAJ*g.=,d`R/8X2o6>8V'<HZE,}aMdRXG@,HT%%'n>6wrWxkN(ZWeo>20]UifoXdE ??HJV? -H
2021-09-10 09:33:46 UTC	67	IN	Data Raw: 89 26 f8 00 94 f6 8a ad c3 83 cf e7 a7 ca 92 c9 b1 b6 6d 40 73 d3 53 08 aa 51 73 42 0e 7b f4 be f5 d2 04 b5 ed 28 9c 57 c7 24 47 42 dc 3b 10 e6 55 b2 a1 ca a9 5d b2 13 bb 60 15 63 c7 8e b8 27 12 ac 25 5e 1d 3b b3 fc c7 55 c3 3a 01 20 d7 d7 d7 7e b9 42 3f 51 d1 86 0e 46 ec ac 46 81 1c d8 77 b9 04 92 07 f6 32 4a a1 42 82 09 a5 70 28 72 47 8e 8e 9e 21 61 86 27 16 a3 50 79 1b 65 fb 85 07 0a 84 a9 f0 87 1b 96 1e 77 d7 93 b5 c4 7e c5 ca c7 42 21 2c 06 2c 7f f2 61 ed d0 de ff 00 be 40 08 d9 23 1a 20 32 9d c3 c7 c9 eb 8b 5e 21 9e 96 66 f2 e4 cd 06 96 82 09 60 ce 45 9b f7 4b 66 d5 39 c3 53 d3 1a be 99 16 21 44 ee 03 03 16 58 24 52 a5 4e d3 b9 b6 ed da a0 79 f7 7e eb e3 a4 b8 82 53 2c e1 24 6f 52 69 5c fb ce 1f 91 2b c5 54 b8 2c a2 0b df 3b 5d fa f9 46 1c 6c bc 09 Data Ascii: &m@sSQsB{(W$GB;U]`c'%^;U: ~B?QFFw2JBp(rG!a'Pyew~B!,,a@# 2^!f`EKf9S!DX$RNy~S,$oRi\+T,;]Fl
2021-09-10 09:33:46 UTC	68	IN	Data Raw: 64 14 24 95 a9 03 15 37 44 59 a0 3a 57 88 92 95 a9 d2 18 d8 eb b5 4e 96 8d 27 09 3b 02 46 13 6b d8 b9 2c ec e3 96 7c a1 1d eb 5f a5 d9 39 e9 2e 4e 9f 23 c3 38 63 30 c8 64 00 a8 ee ed 89 46 d0 aa cd ee 54 29 b6 dc 9f 1c 72 8a f8 72 9a a0 9c 55 fc 8d 7d 39 d2 2f 24 f1 72 d2 30 ce 01 40 b6 80 b7 3d fa 5a a6 15 63 48 d7 34 1c f3 2e a5 0a e6 c9 8d 85 1c 70 a4 10 47 23 93 bb 71 22 23 b5 45 00 0b 6d e7 92 1f a0 31 96 95 50 85 13 7f 13 da b4 d9 b7 fc 49 42 54 c3 ff 00 18 01 26 ac ee 5a c4 64 ed db b4 10 69 fe a9 9d 97 11 0a f7 30 71 73 5a 67 89 20 59 15 3b bc 08 a4 86 42 1d 24 8e 42 5d 64 53 4a 79 b2 2b a9 f0 fc 54 c4 bd 08 01 dc 7a 9e b7 0f 7f 78 07 13 c1 49 58 01 14 59 cd dc 77 7a dd f3 25 e1 8f a4 7a 87 44 7c d8 e4 93 06 68 e0 8b 16 10 0b 23 c6 23 68 25 76 5d Data Ascii: d$7DY:WN';Fk,\|_9.N#8c0dFT)rrU}9/$r0@=ZcH4.pG#q"#Em1PIBT&Zdi0qsZg Y;B$B]dSJy+TzxIXYwz%zD| h##h%v]
2021-09-10 09:33:46 UTC	69	IN	Data Raw: 41 3b 09 15 47 23 7d bd 5f 93 e0 75 bd fa 34 f2 25 39 2e c1 a8 05 1f 97 ce ce c1 e3 e6 9f ea 19 00 b6 11 87 1b b9 2f 95 5c 03 d6 da 88 ab 90 e1 c7 8d e9 64 c6 9d 0b f7 55 f2 51 29 8d 83 2e ed e7 f1 b5 15 54 37 f0 0f c7 57 9f 7b 18 cd ec 1d af db 7b 46 28 cb fb 4e 86 70 ee 1f 5f 2c bb 6a 88 29 f4 8c 42 6c 7d 36 38 d9 99 a4 19 27 bd b8 a8 89 23 8a 67 42 7f cc de db 4f fc 40 8e 6b a4 e7 ff 00 c6 bf 11 07 96 b5 eb cf 5c eb 06 92 84 a9 15 0e bd 41 f6 02 bc ed 4e b0 7d 95 8b 00 9b d1 b9 28 5e 4c 7c ad 17 57 81 62 89 ad 62 c9 d3 a4 68 a4 8c 92 3f 7b c3 28 90 12 6e 91 4f 40 33 ca 78 72 6c 92 b3 46 dd ad e6 79 3e 90 69 92 90 05 aa 13 77 37 73 b8 71 d3 6d e1 7f ea 9c c6 d5 30 1c 3b ab 4d 95 87 3e 1f dc 15 db 23 64 e1 2a 94 91 88 e1 8c d8 c5 28 79 dd 13 93 60 f0 7e Data Ascii: A;G#}_u4%9./\dUQ).T7W{{F(Np_,j)Bl}68'#gBO@k\AN}(^L|Wbbh?{(nO@3xrlFy>iw7sqm0;M>#d*(y`~
2021-09-10 09:33:46 UTC	70	IN	Data Raw: 64 78 d4 51 3d b0 40 b2 a4 58 21 9c 92 49 f9 23 a5 d0 91 ff 00 22 08 b3 b0 34 14 76 f4 d1 fd 23 ab 00 ae 52 ae 14 52 f9 38 b6 94 80 cd 61 db 07 59 8d 32 ed b4 dc ec 68 32 19 54 17 31 4b b8 c3 24 c8 d4 08 78 d9 6d ea fd bc 35 8e 98 96 94 19 60 a0 78 92 9c cd d8 36 b9 3d 5b ca 94 2a 8a 65 f1 06 5f f8 1a 00 7a 75 7e da 27 91 67 39 82 39 25 56 8d 62 86 5c 57 8e 99 84 98 81 56 26 a3 fb 5a 7c 7d 8c d5 c3 d1 04 90 3a 09 0a 28 2b 3f cd c8 b3 30 16 71 ae 40 fc 40 a5 90 89 a4 37 84 17 cf ab 7c f3 89 c8 f2 e7 8f 51 10 3c 6d ff 00 19 72 b9 42 14 89 11 d6 68 18 01 60 10 54 fc 78 fc df 4b 2c 03 2e 60 48 65 80 c5 f3 7f 2d fa 52 2d 11 31 49 98 0e 20 05 40 05 9f 22 45 6b 5d 72 f4 86 4b c1 3e 4e 56 3e 62 05 6f f1 1c 58 8d b3 14 08 f1 dc 6f b8 79 34 97 cf 3c f1 e3 9e 92 94 Data Ascii: dxQ=@X!I#"4v#RR8aY2h2T1K$xm5`x6=[*e_zu~'g99%Vb\WV&Z]}:(+?0q@@7|Q<mrBh`TxK,.`He-R-1I @"Ek]rK>NV>boXoy4<
2021-09-10 09:33:46 UTC	71	IN	Data Raw: 6f da 48 ed 86 1e 08 2c d6 79 22 c7 03 cf 5f 30 fa cc d0 66 4d ab 90 a3 f3 7e 7b 36 5c c7 d8 3f d3 d2 01 91 24 1b de d9 16 07 76 0d dd e3 ac 9f 4e a0 43 06 2e d9 26 95 15 62 54 54 04 b3 b7 01 90 80 ab 40 55 ee 3c f1 e4 df 58 75 a0 95 3a a8 1c 90 c6 bd f4 8f a3 c8 70 80 86 f0 a6 8f 99 a6 7e 4d a7 ab d8 9d 26 19 50 cb 70 30 ef 2b c5 dc 91 94 10 24 db db 72 39 f6 80 84 2d 0b 2c 28 5d f5 39 69 c4 a0 1d a8 4b e7 4e fa 41 57 25 d3 40 4d 68 da 77 ab d9 a8 44 12 c1 82 41 56 30 b3 0d bd c1 2e ed aa 14 91 4a 54 15 dc f6 a4 80 79 f7 74 6c 66 c4 30 4e 79 16 d7 bf 88 04 ce 10 86 c3 57 fe 47 26 ef 68 f2 fe 97 c7 9f 21 27 64 0a 02 6f ec fb 94 a5 82 ec d9 32 d9 ad 84 91 b7 e3 72 8a 3c 74 03 35 49 98 4e 59 39 3e 6d 4b b7 3a c4 ff 00 da 85 06 72 cd a0 20 51 ef f9 67 ce 30 Data Ascii: oH,y"_0fM~{6\?$vNC.&bTT@U<Xu:p~M&Pp0+$r9-,(]9iKNAW%@MhwDAV0.JTytlf0NyWG&h!'do2r<t5INY9>m K:r Qg0
2021-09-10 09:33:46 UTC	72	IN	Data Raw: 87 91 7d 1e 4b 04 d5 54 dd bf 39 57 48 47 89 e1 0c d7 29 14 15 04 7c 3d fd 68 f9 98 64 61 e5 45 90 a1 5e f6 48 11 68 ae fd d1 9e 37 29 00 01 b6 ec 92 45 f1 fd ba 6e 52 86 34 9a 1a bb 96 cd bb d9 cc 66 f8 ae 18 a5 25 ae 29 b3 8a 0a f6 cd e5 e2 6d 21 b1 cb 30 2d 24 31 ac a2 13 ca b1 0e e1 89 2c 2c 0d a4 00 b2 72 02 f1 f3 d6 82 4b 19 63 24 e1 a3 72 fc ea 7a e6 69 84 bf 19 fb 81 87 e9 fc ed d4 f5 81 8d 43 4c 6c 66 69 65 87 6c 13 b2 87 48 5c 95 27 6d aa ef 5b 08 a3 f7 31 35 b8 9f 3f 3d 01 88 51 63 89 26 e6 cc 69 97 bd a1 d9 45 12 e9 88 9c ec d7 61 e5 be b5 a4 6a 64 69 67 27 1e 44 48 59 8a c2 1a 39 41 60 87 6a ef 60 81 af b8 63 5a 36 a1 4f 1b 87 e7 ae 14 54 ac 17 6b 83 61 76 fd 3e bc a1 e4 4e 0a 21 21 8e a4 3b 86 1f 3d 3a da 07 33 3d 1d a7 6a bf ab f6 e2 29 55 Data Ascii: }KT9WHG)|=hdaE^Hh7)EnR4f%)m!0-$1,,rKc$rziCLlfielH\'m[15?=Qc&iEajdig'DHY9A`j`cZ6OTkav>N!!;=:3=j)U
2021-09-10 09:33:46 UTC	74	IN	Data Raw: 35 0a 2e 4a 9c 3d 18 33 53 4b 41 f6 04 ef 9f a4 e6 63 bf 72 45 43 2c 61 a4 6f 70 ed 12 40 20 92 5a 86 d6 05 05 14 3c 7f 10 12 c2 4a 66 25 4a 2a 24 24 a4 8b 03 ca bd 39 bc 7a 74 dc 00 a4 24 10 69 9f b0 6b 73 fd ad 30 94 63 e7 be 14 fb c4 72 c3 24 84 25 95 57 53 dd 08 3c 79 1c a9 e7 db 7c 8e ac 98 94 62 cc 10 e2 dc c9 6f 6f 4b 88 a6 5b a1 64 ff 00 d9 ef e8 68 d9 55 a3 f4 50 4b f6 79 a0 6c 20 e5 a3 ab d5 38 1c ba 95 3c 57 20 a1 f9 36 01 ea 20 9c c5 03 55 dc fa 0b c4 42 71 0c 59 9f 4a e7 7f d6 f0 c5 d3 bb a7 05 73 82 b6 fc 27 52 a2 c3 6e 2a 23 ee 2b 22 8b 0a 50 92 41 03 dc 01 e0 8e 95 98 b5 22 72 b0 80 42 c5 5d d8 0a 9d 2a 41 b0 a5 c5 58 c1 d2 92 64 a4 a8 80 51 50 33 38 73 35 2d 7a d3 2b 46 a7 af f0 63 9f 07 49 d4 71 c7 e8 89 25 c6 70 a4 8a 87 20 2b 02 5a 80 Data Ascii: 5.J=3SKAcrEC,aop@ Z<Jf%J*$$9zt$iks0cr$%WS<y|booK[dhUPKyl 8<W 6 UBqYJs'Rn*#+"PA"rB]*AXdQP 38s5-z+FcIq%p +Z

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	75	IN	Data Raw: f9 1b f7 51 9d f6 19 40 a6 b9 21 93 5d c6 d5 63 2b db d5 30 b1 f3 64 65 3c 19 66 0b 1e 52 f1 74 44 88 49 1f cf f2 47 4e 01 e1 6a 57 3e 7c db bb c2 53 31 05 b8 0a 6c fd 2e fa b7 91 bc 0d 6b 15 2c 3a 82 aa 02 93 77 40 5b 1b 6d 65 5f cd 83 ba 89 23 cf f6 f3 d4 d0 a0 08 35 6d 8e 87 6e 59 1f c4 75 52 8a 8c c5 a8 30 21 80 ce d9 d3 bf 79 ff 00 4d c6 b9 5a 36 9b 86 9b c4 ff 00 7f a7 40 ec 0b 05 0a f9 ec 59 36 81 c9 08 a0 93 c8 ae a1 c4 cc 64 cc 98 5d b0 9a 3b de bc ac 72 14 a9 d8 77 81 4f 89 08 16 0a 19 9b 39 d4 ef b1 a9 8e e5 7d 13 c5 fb 7c 0d 2d 25 57 de b0 62 c4 36 fb 4d f6 d0 57 22 b6 f3 64 ad 91 5e 6f af 95 7d 45 62 6c d9 a5 8f f2 25 ef 47 f8 6d 23 ee 1f 46 94 25 ca 92 68 d8 52 40 1a 91 b9 fd 3b 56 3a 59 e8 84 78 a2 c0 68 5b 6b 40 8a ce a7 da a4 15 da 45 b1 Data Ascii: Q@!]c+0de<fRtDIGNjW>|S1l.k,:w@[me_#5mnYuR0!yMZ6@Y6d];rwO9}|-%Wb6MW"d^o}Ebl%Gm# F%hR@;V:Yxh[k@E
2021-09-10 09:33:46 UTC	76	IN	Data Raw: 2a c0 21 a8 43 69 b5 79 30 3e f0 bd c3 c2 87 1e 62 62 61 1d 10 a0 c8 18 8b 03 70 1b c8 dc 28 7c 0e 2c ff 00 1d 47 0d 30 ff 00 95 f6 d1 b5 df ac 5a 4c 9a a6 09 52 81 17 f0 fe db fb 6b c4 9c b1 85 4e e4 c5 40 1b d5 9d 09 db f8 06 bc ff 00 3c 7c ff 00 b7 4b ce 50 15 c8 38 c8 59 81 f5 10 24 90 b2 13 ae b6 d6 3d 41 91 16 ee 57 70 1e 00 1b 77 11 b4 86 56 22 ac f2 5b 75 0f 1e 7a 8a 4a b0 b8 b7 b6 76 eb dd 22 4b 42 d3 47 4b 5b 3b 75 ad 99 a9 57 3a 43 17 44 d5 b7 29 8e d5 36 7b 03 b2 f7 16 ab 90 68 90 be 7c 81 e7 8f c0 e9 a9 53 12 06 02 4e 26 60 45 41 3f 9c f6 de b1 5b c4 f0 67 11 74 8c 35 20 66 1e df 34 a7 41 0e 0d 0b 2b 1e 68 fe df 2a 9e 11 1d 2f 75 94 46 09 3b bc ad 59 e6 95 49 3e 7a ba e1 27 d0 21 64 33 00 f4 2f 93 8f 63 19 4f a9 70 ca 4a 89 40 a1 38 ad 7f 2c Data Ascii: *!Ciy0>bbap(|,G0ZLRkN@<|KP8Y$=AWpwV"[uzJv"KBGK[;uW:CD)6{h|SN&`EA?[gt5 f4A+h*/uF;YI>z'!d3 /cOpJ@8,
2021-09-10 09:33:46 UTC	77	IN	Data Raw: 09 14 35 d2 85 8f 99 e6 d0 8a d7 70 e6 9f 15 a2 08 e7 b7 95 36 46 30 3e 5d b1 e0 05 d1 79 a2 1d 77 1f c1 db e2 ef a7 38 42 71 e1 36 cb a8 f9 27 4e b6 8a ee 2d 00 a5 45 2c d4 ef fa d3 94 22 f5 18 0e 9d ab e9 7a cc 91 ad 6a 0f 3e 3c e0 8b 56 59 17 f4 8d 9e 6f c2 80 7c 11 67 e3 ad 0c 8a cb 58 4d 4b e7 4b 0c 9b 95 de b7 11 9d 9c 0c a5 09 80 8c 20 e1 23 32 4d 05 87 36 e9 1e 30 33 65 d3 63 9e 27 2c 85 64 b0 a4 f3 52 48 0a 12 e4 11 b4 c2 cc 8c c6 c7 b4 5d 10 3a 92 42 41 c2 45 72 34 a9 cb 76 dd 87 9d 20 f3 43 c9 c7 46 fe 4d fe 54 af 7a c0 de bd 2b 61 ea 98 b9 d0 91 53 a0 db 4c 55 01 0c ca d4 cd cb 6e 47 a3 f1 5c 7f 1d 3d 21 9d 69 51 34 01 c8 1b d0 72 e6 33 76 8a 99 cd e1 55 81 2d 5c b9 ed 48 d9 92 7f b2 9d 1b 61 7c 7c 89 22 8d de c1 57 89 b6 b2 4b 57 56 b6 ea db Data Ascii: 5p6F0>]yw8Bq6'N-E,"zj><VYo|gXMKK #2M603ec',dRH]:BAEr4v CFMTz+aSLUnG\=!iQ4r3vU-\Ha|"WKWV
2021-09-10 09:33:46 UTC	79	IN	Data Raw: 95 1b 28 02 30 3b 91 b0 a2 14 fb a8 b5 8a 07 dd c8 1c 11 d0 a6 90 95 38 72 cc c4 3e a6 b5 d1 bf a7 87 50 71 4b 75 11 88 d3 9d c3 1f 7f 88 ae ff 00 58 70 18 eb 39 f2 12 ef 24 f2 62 e5 a2 ee 2a 04 33 c9 bc 10 a4 9a 8c c8 5b 80 0d 5f 1d 5e f0 2b 0b 92 b7 20 94 8a 37 f4 db f6 d1 43 c5 a0 49 52 94 b1 87 30 08 70 77 07 7a 53 95 20 09 93 7e 9f 1a 11 b2 4d 27 25 ae 4b 25 5a 0c b5 69 16 32 2b 8d 92 8e 0f 80 5b e4 1e 9e 0a 00 33 d4 52 de 94 dd a9 5c f4 84 ca 8a 92 0b 32 6e fe 7b 93 bd b6 88 49 cf fc 3e 4c bd be ec 62 26 73 b8 f0 ae c4 95 63 f0 6c 9f db c5 f1 f9 be ba 9f 08 01 40 bd 69 a5 db 97 cf 46 22 5c e2 b9 64 61 29 22 84 db 91 a5 fd be 4f 7e 9e c7 1c 99 fe 9a 57 4a 59 f5 6c 20 22 11 ff 00 cc 0b 31 49 1b f9 55 a3 b9 bf ca 4d 0b f3 d2 bc 61 c3 26 60 36 2f 86 a4 Data Ascii: (0;8r>PqKuXp9$b*3[_^+ 7CIR0pwzS ~M'%K%Zi2+[3R\2n{I>Lb&scl@iF"\da)"O~WJYl "1IUMa&`6/
2021-09-10 09:33:46 UTC	80	IN	Data Raw: bc 9b 7a 47 11 33 1a 54 0d 33 1b bd 7d f9 5e 0b df ed f3 31 a3 65 c4 98 3a 28 62 c6 46 24 1e 4c 67 61 23 dd e4 83 55 f0 2c 74 a2 81 62 12 1c 81 95 ea de ce 2d f3 1c 41 62 10 aa 07 2c ad 9f f0 cf f1 48 11 cf d4 d5 52 78 b2 d5 9a 50 fb 54 9f 04 03 b5 79 fd a7 90 2c 13 fb 8d 7c d1 41 73 16 84 cc 70 c4 11 f3 4a 12 d6 e7 d6 2c e4 70 a8 24 14 ab 11 ff 00 26 a5 dd 85 75 cb 91 31 13 89 95 8b 9a 80 ce b1 96 40 ca e3 79 53 6b 6b 7b 81 e2 55 f9 5f 27 c7 45 90 b0 a4 95 28 b9 27 7f 6b f6 f6 82 cf 94 b9 65 c0 27 c4 2e c7 23 f8 b7 2e 51 9b 22 38 a6 45 4f f9 68 54 3d f2 cc 40 7b 00 2f ff 00 f5 75 40 f5 09 b8 55 72 e0 bb 91 a3 de 23 2c 16 2a 01 c8 c9 f9 52 9d f2 8f 4d 04 68 2e e2 65 00 f9 bd c8 18 5a b5 2f 1c 79 a6 35 fe c7 ae 91 85 1e 0f 15 0b 11 ca fb e5 d3 3a 3c 4c 3b Data Ascii: zG3T3}^1e:(bF$Lga#U,tb-Ab,HRxPTy,\|AspJ,p$&u1@ySkk{U_'E('ke'.#.Q"8EOhT=@{/u@Ur#,*RMh.eZ/y5:<L;
2021-09-10 09:33:46 UTC	81	IN	Data Raw: 4d 9e e7 b1 0c df 4e 96 92 23 87 2c 82 35 d4 30 a1 88 30 28 ca b9 18 88 25 8a e5 27 8d e6 09 36 91 ee a7 db c0 e0 d7 f1 47 02 88 45 53 e5 7a bd 79 57 ce 90 6e 1a 63 b3 8b 57 e3 6f 6b 5b 28 9a d7 33 ff 00 c6 74 14 89 64 79 32 b2 74 59 7b 53 24 54 25 cf d3 f2 81 50 ce a0 90 c8 21 75 6f 06 9e f8 07 aa d4 21 08 59 51 55 49 24 06 d4 3f c8 34 34 ac 3e a9 c2 64 b5 24 86 22 da e8 e0 e4 d9 d3 70 61 65 ab 08 57 ed 1e 46 6d d1 34 33 a1 90 ba ac 91 ce a0 4a 06 f3 b0 30 0e e0 8f e3 9e ac a4 25 4a 20 a4 39 a7 56 a6 7b 57 6e b1 49 36 ea 49 77 05 db 40 f7 d2 11 7e a8 c0 c8 9b 01 f1 41 90 4f a4 66 b4 c5 4f 2a 62 86 5b 0c a7 85 00 a1 56 24 1a fe c3 8e af f8 65 00 40 3f fe c6 ec 48 a3 f4 04 d3 48 a2 e3 90 f2 95 84 78 81 f1 35 ff 00 15 f2 d6 21 74 98 e5 cf c3 ce 76 89 f2 0c Data Ascii: MN#,500(%'6GESzyWncWok[(3tdy2tY{S$T%P!uo!YQUI$?44>d$"paeWFm43J0%J 9V{WnI6Iw@~A OfO*b[V$e@?HHx5!tv
2021-09-10 09:33:46 UTC	83	IN	Data Raw: b1 d7 bf cf ff 00 db d5 ff 00 3e 90 dc a5 f8 1a b4 4b e8 ed 91 ec ef 1b 7e 8c c2 81 97 07 28 3c b9 13 c7 1e a7 91 32 d3 2a c1 24 89 2c 11 a9 bf f9 88 61 60 17 f0 7c 7c 75 c9 ca 22 81 9d c3 1f 52 47 95 20 92 13 8d 44 9d c5 5e a6 ef 4f 31 ca d1 01 22 47 8d 3b 07 51 37 f8 ab 34 32 47 18 41 1c 43 1c 7b e4 f3 41 94 d0 36 3c d7 9e 7a ea 0b e1 ea 7c c5 7d 47 9b c4 a7 4b 09 a8 1b 93 52 f9 1e 55 be ef 10 98 b0 ac fa 1c 51 9c cb 30 fa 83 37 f4 1d c0 63 1a 08 e6 11 be d6 24 04 57 dc 80 50 e2 cf 52 59 09 25 ff 00 ea d9 dc fe 1f b1 11 96 a7 48 0d 40 ac af 4b f3 bf c5 61 0b f5 59 65 71 16 44 a1 94 49 78 cb 35 da 91 89 98 3b 4a 00 b3 c2 10 79 ff 00 b0 e7 ab 5f a5 82 c4 e5 43 cc 3e 9a 1a 65 eb 15 7f 56 19 91 46 bb b0 b0 bf eb 27 d0 c2 d7 13 32 18 f2 b5 2c 1c 89 6f 1a 4c Data Ascii: >K~(<2*$,a`\|\|u"RG D^O1"G;Q742GAC{A6<z\|}GKRUQ07c$WPRY%H@KaYeqDIx5;Jy_C>eVF'2,oL
2021-09-10 09:33:46 UTC	84	IN	Data Raw: 7b 3a 94 ad 89 1c ab f3 f3 58 b6 e1 d2 b0 19 f9 8f 4a 6a f9 36 43 76 8b 89 e8 f6 ca cd 8c 3c 4e 98 d1 27 75 d2 51 1f 73 b3 04 82 c7 70 3d 0b 96 75 de c4 10 76 d5 93 d4 50 cb 18 d2 c0 b7 7e a2 f4 e7 05 9b e0 21 01 c0 e5 9e 75 e4 2b 67 d1 a1 b3 a7 e0 e4 e5 cb 80 88 a8 4e 44 63 74 b9 0a 63 52 80 c8 64 c9 57 06 bb 6e 42 ed 23 75 15 15 c1 e0 13 25 a9 4e a7 05 ea 47 bf 41 e9 10 fb b8 68 0b ed 9e d6 30 45 a8 e1 c5 81 8a d2 42 ff 00 ae 22 8c 2b 85 b5 98 12 44 8a 4f 14 ea 2f 6f 9e 00 b2 3a 55 7e 14 bb fc b6 76 1b 0a 53 d5 e0 b2 14 a9 b3 18 83 7f 26 6e d8 e6 7a 42 db 5d c5 8a 4c 53 19 08 45 99 03 a5 06 2c e4 33 f2 c4 9f 69 aa f8 07 9f c7 49 2d 01 49 24 b0 c5 e2 63 42 33 62 6a e7 d8 1d 62 f6 5a d5 24 38 7a b6 ce cf a0 ab 3e 57 78 5e 29 93 4f c9 30 29 69 93 76 e7 50 Data Ascii: {:XJj6Cv<N'uQsp=uvP~!u+gNDctcRdWnB#u%NGAh0EB"+DO/o:U~vS&nzB]LSE,3iI-I$cB3bjbZ$8z>Wx^)O0) ivP
2021-09-10 09:33:46 UTC	85	IN	Data Raw: 17 ba 6d bb 65 76 e7 a0 8e 5f 7f 54 ca f2 7a 4b 5f 2c ac 4c 78 12 64 22 a9 14 8b 1e 49 da 54 f0 38 53 bb 68 e4 9f 06 a8 75 ad fa 45 66 cb 00 ff 00 91 bd 08 a1 cc fc 97 a4 7c ff 00 fd 42 96 93 3b 97 a3 8d b5 14 e7 a9 8e 47 6b 9a b1 fb 9d 3b 15 ce e5 85 9a 17 b1 fa 67 23 52 74 99 8a 81 cb 11 b7 6d 78 0e 6f 9e 3a fa 07 0b c3 29 48 2a 36 67 a9 c8 77 5d e3 e2 5c 74 cc 1c 42 c3 d0 13 43 76 ef 9c 1d e0 4f 94 d8 9e 9f c9 8f 96 95 57 b9 8d 90 19 5d 64 c1 c8 1d c4 d9 5f f3 36 b4 a8 5b 8b 04 f5 57 f5 04 61 05 3f a2 33 7b 5d 81 03 48 37 0e 71 82 13 4d 2a dd 32 d3 9d 2d 07 da de 59 d2 74 4e e4 58 64 c5 8f 92 f9 51 b4 65 6a 1c 7d 45 7b 13 26 e1 e0 45 90 88 f2 1a dd fa b4 05 df 55 dc 32 3e f2 8e 2a 61 24 73 cd ea c4 0b 3e ba c3 7c 47 fc 29 05 9d d2 2d 5a ab df d0 42 bb Data Ascii: mev_TzK_,Lxd"IT8ShuEf|B;Gk;g#Rtmxo:)H*6gw]\tBCvOW]d_6[Wa?3{]H7qM*2-YtNXdQej}E{&EU2>*a$s>|G)- ZB

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	86	IN	Data Raw: 3f 92 fe 91 5e f5 56 2f a7 e2 64 a4 c6 59 23 ca db db 71 b5 96 c9 04 31 6b ab 36 7f b7 f7 eb c1 0a d0 0e bf 88 61 0b 0d 7a 65 4b 54 f5 8d 4d 6b 55 0f 82 d1 a0 45 95 b0 f0 61 5b 51 fb c3 bd af 37 64 92 05 71 e2 fa 90 46 b6 ad 35 a7 3f dc 16 0a bd 07 3b c3 85 a9 cf f6 95 24 3a 63 18 a5 36 23 76 10 90 18 59 34 56 d8 90 2f dc 2c fc f4 39 f2 c9 53 11 57 14 cf 4d 3d 8d b5 86 e5 28 03 34 6c 2d 52 ec 1f bd e0 4b 1f 10 49 26 89 31 3b d6 5c cd 4d 26 76 dc 01 c9 9a 78 e4 0a c4 1e 43 28 92 8f 8e 07 cf 5d aa 15 25 29 34 62 ef 77 71 7f 78 94 af f9 10 4d 5d 21 58 8b 75 35 f2 ee f1 3e 9e d3 e4 59 fd 4d de ff 00 88 86 2d 76 2c cc 70 90 ef 30 c6 00 c5 9e 03 c0 04 50 00 0b b2 0f 9e 3a 3c ec 2b 09 09 3e 20 52 4b 64 c1 cd f5 2f 95 8f 48 5a 48 61 34 3d 94 f4 cd 81 71 d0 f6 21 Data Ascii: ?^V/dY#q1k6azeKTMkUEa[Q7dqF5?;$:c6#vY4V/,9SWM=(4l-RKI&1;\M&vxC(]%)4bwqxM]!Xu5>YM-v,p0P:<+>RKd/HZHa4=q!
2021-09-10 09:33:46 UTC	88	IN	Data Raw: 7a c1 26 91 00 7c b9 a2 2e 28 c9 bc 17 f7 28 8d 19 bb 8c 1a 85 3e ea db c7 b1 4d 1b 3c f4 29 89 0a 25 f2 7f cf 3b 88 97 06 86 0b 56 97 ad ad 6d 68 47 ad 21 fb f4 f6 73 1e 3c b8 e3 14 9d ee 63 fb 92 f4 b2 e3 d9 65 51 dc 0c 55 49 b2 a5 00 61 e0 9e 91 9c 54 41 4a 32 d3 96 9d e6 2c ed a2 92 87 4a 14 d5 70 68 72 1e ee 6b 6f 37 8b 79 e9 26 82 1c 49 1d 12 79 69 6e 57 0c d1 a4 a4 a0 20 2c 6e 48 75 8f 85 be 01 3e 47 3d 2a 99 93 11 2e bb 7e c9 af 3e cc 38 25 63 5b 2d 86 ae 91 4e ac 6f 5b 7c 43 6f 48 d5 d5 42 a7 71 e4 99 31 e1 c7 5d cd 6f 0e 38 05 86 3c 69 fb 51 5d db 73 57 24 00 2f 8e 17 54 ec 42 b4 cc fe cb f7 bc 48 70 08 0a 2a 20 54 f8 9b bd 6b bd 35 11 27 95 a8 5a ce 72 7b 91 62 1e d3 31 61 51 c9 b8 1d fb 02 92 43 ab f0 42 9e 47 91 5d 2c a5 2d 4a 2c 29 4a 81 4d Data Ascii: z&|.((>M<)%;VmhG!s<ceQUlaTAJ2,Jphrko7y&IyinW ,nHu>G=*.~>8%c[-No[|CoHBq1]o8<iQ]sW$/TBHp*Tk5'Zr{b1aQCBG],-J,)JM
2021-09-10 09:33:46 UTC	89	IN	Data Raw: f4 31 5b 3e a6 a4 2d 0b cf 1c 8a d5 99 1d 30 0c 03 89 ad 9c b3 0b f7 0a 3e db a2 47 23 e7 ab 2e 1a 64 c7 47 3d 0b 38 0e 5a bc dc 6b 94 52 71 32 98 39 b3 dd b6 7e b4 ee 82 39 a3 fd 52 4d 8f ff 00 ba 3a e4 83 76 d9 70 9b 0d 0a 8d b4 ea 43 5b 6e f2 de dd db 7e 48 af 06 fa d3 7d 1c 28 f1 04 ff 00 ec 31 75 23 5f 5b fb 18 c0 ff 00 a8 52 d2 27 91 a1 16 17 7b de 38 a3 ac b2 3e 66 5e 46 a3 26 c8 17 2f 05 db c8 9b 1d 91 3b 69 90 07 00 0e eb 47 6a 0f 25 b8 eb ea 7c 1f fe 01 c8 7b 6d f8 7a f2 8f 83 7d 4c 7f f9 2b ff 00 d8 b7 b7 6e e4 0b 9b 18 78 fa 47 2e 4d 70 62 18 25 8a 29 65 c9 97 38 b4 a5 14 2c 72 a8 59 a2 8b 70 20 d4 80 b5 82 36 86 16 3c f5 51 c7 4b 25 58 cb 80 69 d6 9e bf 8a de 19 e0 70 0f f8 f5 e5 73 cf f1 ca 1a de a3 d3 31 f1 74 0c ad 33 25 ae 71 3c b1 24 72 Data Ascii: 1[>-0>G#.dG=8ZkRq29~9RM:vpC[n~H}(1u#_[R'{8>f^F&/;iGj%|{mz}L+nxG.Mpb%)e8,rYp 6<QK%Xips1t3%q<$r
2021-09-10 09:33:46 UTC	90	IN	Data Raw: 16 1b 37 97 3d c7 50 d4 1c 03 64 8a f3 63 e7 a5 26 91 85 46 d4 38 72 3e 95 e6 7c e1 be 1c 35 4d 85 e8 ee 0b 54 eb d1 fd 1a 39 55 ea dc ec c7 8f 20 81 db 96 0c 77 0b 90 ac 41 91 9c d1 0a ab e4 b8 f0 09 a1 c8 1f 8e 96 40 04 92 76 af 53 5f 7e 70 f6 10 a1 40 08 be 80 75 3a 79 c2 47 39 b5 36 83 4b c4 fb 72 c8 f3 19 5b de 37 92 c4 3a 96 b1 7b 48 b2 41 f8 e4 0f cb 38 51 ff 00 6f 51 6e f2 f5 88 a1 24 52 e4 e5 a7 79 e5 eb 1a 19 03 74 b8 a5 20 63 f7 59 cf 1c c9 b8 38 0d 8e 0c 81 b7 0f 70 45 f1 63 e7 a1 90 c4 88 72 5a 01 b9 39 0b db f5 dd 21 af e9 3d 99 58 19 d8 b8 bb 22 92 3d 03 52 c8 9d e5 6a 8c 49 b6 40 89 1f 20 31 09 1b 3a d9 f2 4a 8a 3c 74 15 93 89 de b4 cc bd a1 85 27 09 a6 62 bb ed 93 f7 94 2e 3d 31 38 97 44 c5 70 64 90 60 6a 53 e6 8f 6b d3 bf dc 4b ec 1b 8d Data Ascii: 7=Pdc&F8r>|5MT9U wA@vS_~p@u:yG96Kr[7:{HA8QoQn$Ryt cY8pEcrZ9!=X"=RjI@ 1:J<t'b.=18Dpd`jSkK
2021-09-10 09:33:46 UTC	91	IN	Data Raw: 24 82 01 36 60 49 ce fe df 3a c5 62 f5 26 58 95 4a 11 1c aa 52 54 70 58 92 e0 31 dc 79 34 49 00 a9 be 6f e3 8a ea c2 51 25 40 3d 01 1d 0b 8f 88 cf 71 48 20 e2 2c 41 06 9b df d9 b9 42 83 ee 71 de 3e c6 2e 69 85 e1 49 0f 6a e4 13 39 3e e8 63 45 a2 37 2b 01 b5 89 da f4 40 6a be ae 10 82 12 93 71 6f 4a 36 6f ae b6 ca 29 e7 28 36 01 46 2e 58 33 fa 55 b9 fb 41 6e 8b 92 b2 3f 7e 4f f9 9d 95 09 23 1a 66 66 a1 91 be 20 6f 79 72 6d 54 55 03 bb c0 e8 53 95 85 9f 3b 83 9b 38 eb b4 39 c2 0f 05 9d c6 83 51 e7 4f d4 58 3f 47 66 0c 65 c5 80 6e 57 99 6a 10 48 3b 42 8d 8e e1 0f 04 3d 58 04 58 ab fe 3a 49 4b 42 42 88 00 12 0d 43 27 2e 4f ee ef e7 a9 e0 65 a9 69 49 c0 3c 21 ed 98 af 3b 31 ac 5b 0f 4f 66 ce d8 eb 0c 72 45 24 51 20 b7 25 95 a4 3b 40 b0 14 59 27 f0 38 3b 7e 7c Data Ascii: $6`I:b&XJRTpX1y4IoQ%@=qH ,ABq>.iIj9>cE7+@jqoJ6o)(6F.X3UAn?~O#ff oyrmTUS;89QOX?GfenWjH;B=XX:IKBBC'.OeiI<!;1[OfrE$Q %;@Y'8;~|
2021-09-10 09:33:46 UTC	93	IN	Data Raw: 40 e7 34 47 7b 4e c1 48 f6 b1 57 1b 36 8a 31 1e 39 dc 36 80 08 bb 62 07 4a 97 b1 cb 28 3a 52 5e b6 19 1b 1e 50 bb d5 0c 84 cc a6 6d d0 ce ed 3c 72 95 02 bc 95 42 c4 d0 2c 3c 8a ff 00 b7 9e a4 87 0e 03 74 ef f0 1e 38 bc 26 98 43 8d 45 b3 ef da 15 da 94 84 ef 62 c2 46 21 a9 fc 6f d8 a7 86 af e2 c0 51 5b 88 e4 d1 ea 4b a2 69 4a 8d 87 c7 37 db 5a 42 cb 48 00 02 c6 ec 76 f2 a7 9e 7e 55 df ea 13 40 34 f9 dd 51 da 08 a6 8c 3a 23 52 99 d4 35 6d 0c 2c b0 06 f8 6b ab af 07 a7 b8 47 52 a5 87 37 60 e5 da 9d 62 87 8c ff 00 21 90 c4 c3 2b 65 5d c9 8e 5d 7f 53 d2 98 7d 07 9f 34 80 48 cd a9 48 c1 64 f6 c7 1a cb be 08 c0 a3 64 96 75 2b c9 24 82 39 f1 d6 bf e9 28 3f ee 33 62 a1 41 a3 d0 fc 01 af 28 f9 d7 fa 8e 60 1c 3c f7 ff 00 a9 a9 ad 41 0c d6 d1 8f f6 dc 53 f5 9c 1d dd Data Ascii: @4G{NHW6196bJ(:R^Pm<rB,<t8&CEbF!oQ[KiJ7ZBHv~U@4Q:#R5m,kGR7`b!+e]]S}4HHddu+$9(?3bA(`<AS
2021-09-10 09:33:46 UTC	94	IN	Data Raw: d1 10 08 aa aa 0b 1a 5f 7f 8f cc 2e 52 18 e2 1e 2f 11 bb 6b 97 6d 18 61 2e b2 b3 cb 4a 03 10 89 f0 cb f8 26 bc f1 c0 f6 f4 45 10 4b 8c ff 00 af 88 e4 a5 2c 5b 53 56 f4 bb 59 a9 5e b1 f7 29 a2 40 d9 4f 68 12 2b 23 77 00 f8 1b 79 f2 7f f5 f3 d2 cb 3e 36 26 c2 83 c8 fb 8a 69 58 2b 82 f4 25 44 e4 69 5d b3 ad b9 73 80 3d 52 53 ab 66 61 98 e3 63 89 0b 96 99 de c0 7a 4b 0a a7 81 ed 24 9b 1c 1a 15 d0 97 6e bf 06 0b 2d 2a 49 c5 4a 86 eb 7a 9b 7a d1 b4 8a c7 f5 8f 52 4c 6f 47 ea b8 21 81 4c 9c b9 e0 8b 77 20 3a ca c6 5b 1f e6 e3 81 c0 b3 5c 5f 4b cc 4a 48 ad ce 5d db bd dd c9 04 e1 23 2e fe 47 a7 38 e5 b6 b9 31 9b 51 d4 a3 57 a8 a1 88 aa ef dc 17 79 7f 71 16 76 f0 00 fe c7 a0 e1 01 db 3d cf a5 cf 74 10 e2 09 09 1b d0 8b e7 01 92 05 86 6c 52 e5 5d a3 82 49 05 fc 30 Data Ascii: _.R/kma.J&EK,[SVY^)@Oh+#wy>6&iX+%Di]s=RSfaczK$n-*IJzzRLoG!Lw :[_KJH]#.G81QWyqv=tlR]I0
2021-09-10 09:33:46 UTC	95	IN	Data Raw: ca 76 b0 7e 08 03 6d ef 55 b2 39 a2 c0 0b a1 d7 42 c6 77 f7 1d fe a1 29 a5 4c 49 b3 1b 0a 9a 73 71 ef 4c e0 3f 58 d3 a5 0b 27 69 54 ac 9b ed a3 91 23 2b 64 09 00 04 1b 61 c9 57 6b f8 5e a7 a7 e7 b7 ee 9a 04 4f 49 1e 2c 45 54 00 9a fb 79 36 50 88 f5 9e 24 58 f8 45 60 6b 40 b3 86 90 2e d7 ef 48 ac 63 72 00 36 e1 ff 00 e6 a9 e1 89 2e b5 75 d7 bb 1d 8f 2f ce 6a 4c 23 c5 7b 68 5f bb 76 5a 28 ef ad 75 4c 8d 38 49 87 39 51 95 1b 49 2f ed b4 9d a4 2c e2 44 71 41 6c 5e e0 dc 03 fd fa b0 e0 c0 5b e3 16 29 a8 a0 0c 32 19 f9 3e ae 2d 9e e3 66 a8 a9 94 28 02 98 8d 3e 5b 9c 28 b4 2c 8c 8c cc 89 32 de 19 c8 57 68 d9 22 a7 65 40 6d 64 26 41 4c 43 0e 08 26 b9 db 55 d5 f2 0a 68 12 2c 28 69 ca ef 14 0a 1e 35 17 d6 9d 61 a7 e9 f5 77 3d f8 dd c4 4c f2 15 45 0b ec 75 93 6b b2 Data Ascii: v~mU9Bw)LIsqL?X'iT#+daWk^OI,ETy6P$XE`k@.Hcr6.u/jL#{h_vZ(uL8I9QI/,DqAl^[)2>-f(>[(,2Wh"e@m d&ALC&Uh,(i5aw=LEuk
2021-09-10 09:33:46 UTC	96	IN	Data Raw: 11 46 0c f1 64 12 a7 73 6d a6 22 ac 28 37 5e 47 49 cd 94 92 97 c4 c4 b5 ed d0 3b 3f 9f b0 8b b9 53 57 84 02 9c 44 e4 cc 4b 1c f4 0f e7 58 5e 6a 78 d2 36 f7 dc 7b ce 4c 92 28 3b 98 a1 e1 77 29 e6 81 2a 41 aa 00 93 e7 aa ce 26 5a 81 18 66 a5 89 62 96 0f fa d3 dc 18 b3 e1 54 a5 38 54 b2 18 53 50 db f4 7c b3 80 dc a6 96 23 2c 53 a4 7b 51 95 48 f2 0a 3a 6d 0e a4 f0 2c 9a a0 78 e4 f9 ae 97 52 51 87 09 d2 8c 58 9e da 9d 77 77 d0 01 2e 9a 38 b9 d9 af d4 0b 7a e6 27 92 a0 46 16 18 fb 81 98 c5 24 6c e1 b6 98 cd ef 5b 1f e5 17 fe a3 fd 7a 50 dc b5 b2 83 c2 e7 5c 78 e1 12 42 23 68 f7 6f a6 0c 64 b5 56 fd ea bc 95 00 5d 81 cf 37 e0 74 44 a4 10 ee 5c ef d2 06 ba a8 93 73 c8 39 67 3e e3 d7 68 51 ea 84 77 66 88 b0 25 a3 32 0b 6d aa 80 29 a2 fb 79 6b 04 5e ce 0d 1e 7e 7a Data Ascii: Fdsm"(7^GI;?SWDKX^jx6{L(;w)*A&ZfbT8TSP|#,S{QH:m,xRQXww.8z'F$l[zP\xB#hodV]7tD\s9g>hQwf%2m)yk^~z

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	98	IN	Data Raw: c1 1d 70 09 80 30 a7 91 f9 f9 8e 94 83 71 ea 63 fa 37 42 77 04 bd aa 48 e4 1f 1b 97 77 06 85 73 5f ef fd ba d3 23 f9 0a bd ed c8 f3 8c 19 9a 40 70 9a 8d ff 00 51 95 98 ed dd be c2 95 b1 cf b8 1f c5 5f cd 78 e0 d8 e7 9a e8 aa 0e c7 fe ae 79 c7 90 4d 54 d6 49 24 75 cc df e6 3f 40 8e d2 f7 37 28 b6 06 bc 2e d3 c7 02 f8 3f 9f e7 c0 eb c9 38 83 b0 1e ba 66 c3 db 4d 23 a2 67 fe b9 6a 74 e5 d7 4e 91 35 1c a5 57 dc 96 c7 da 0f 36 07 9b ae 6f f8 23 e2 bf d3 a9 0c 4b 92 a7 2e c7 2d a9 02 23 ee 95 17 c3 85 e8 ce ed d4 77 a4 7a 60 d2 15 50 2f c9 1c f0 6f 81 63 e0 7c 9b 3f 1c f5 35 65 46 a7 c9 fe fa c7 91 72 15 60 d5 19 d0 5f e5 9e 91 0f a8 b9 c8 49 20 56 51 12 b6 d6 ab f7 39 ad c9 63 e0 d1 a3 c0 15 d2 93 47 8b 16 8d 4f 28 20 9a 92 e0 00 5a 97 88 ec c5 45 c3 8a 38 e9 Data Ascii: p0qc7BwHws_#@pQ_xyMTI$u?@7(.?8fM#gjtN5W6o#K.-#wz`P/oc|?5eFr`_I VQ9cGO(ZE8
2021-09-10 09:33:46 UTC	99	IN	Data Raw: 63 20 6d 61 cd f9 be 83 30 21 40 24 cc 63 71 40 4d f6 3e 8c 6e d0 e4 8f ba 80 71 4b 7b 97 a8 03 2a 33 39 06 d6 f3 82 9d 06 7c 98 a5 94 34 9f 70 ae c1 62 8d cc 71 85 45 45 42 a8 47 b5 85 02 41 35 f3 67 a2 01 84 21 2c ed 99 19 73 b3 8e f2 85 a7 f8 b1 39 09 ab d6 c1 c5 bd 62 7b 23 37 11 27 89 e4 a5 93 ff 00 86 01 b7 57 3c 16 da 01 03 9f 68 b3 64 7b 88 ae 87 88 99 89 05 2e 01 35 cc b5 47 b7 bb 08 12 10 a1 2c 84 9d 3c 54 73 5d 01 6a f3 de 91 ed 32 d9 d6 4e d6 d8 94 39 55 12 c6 1a c5 d3 30 7b e0 31 fd b7 76 2f 9a f2 55 f8 87 fd 5b 21 9b 6b df 47 85 94 a5 12 52 a7 24 58 59 cd bf 11 f9 65 73 24 72 b1 0c f1 36 e0 61 60 4a f9 1d be cb 50 fd c0 d9 5f 77 fd 35 d0 08 f0 b8 53 1d 1b 36 72 33 e4 f4 e7 11 9b 34 94 7d b2 9c 0e 2e 4f 6e ef eb 61 03 ba a3 c7 90 b2 b3 64 2a Data Ascii: c ma0!@$cq@M>nqK{*39\|4pbqEEBGA5g!,s9b{#7'W<hd{.5G,<Ts]j2N9U0{1v/U[!kGR$XYes$r6a`JP_w5S6r 34}.Onad*
2021-09-10 09:33:46 UTC	100	IN	Data Raw: 3e da 42 ef 47 d8 7e a9 58 64 2c 84 85 29 90 a2 ef 9f 46 a7 99 a7 94 63 c5 9a 6c 89 5c e5 05 06 48 d5 02 88 f7 c4 ac 28 85 06 c5 90 39 b1 44 ee 17 57 5d 72 52 14 a9 95 14 26 80 7c ed bf bc 06 62 d0 89 67 c4 c3 56 ce fd 1c f6 f5 89 49 e3 ed 46 69 23 66 48 e1 32 a4 92 84 2a 93 10 a1 16 02 41 91 6b de 42 ee a7 1c d0 3d 3f 32 4a 80 2a 49 21 39 0a 5a c5 8d 0f e2 d0 ac ae 21 25 40 e3 24 a8 ef f2 3d 4e 47 78 85 97 36 48 e3 9e 18 b7 47 91 0b 87 70 5d d9 65 8f 71 11 ee 83 85 8d 92 22 52 ff 00 cc a4 11 ee 17 d2 62 63 a1 52 c0 75 62 24 07 ca d6 e7 e5 ce 2c b0 25 53 10 bc 59 0a 1f 62 dc fe 2b 9a cb d4 cd 2a be 6f 6d a3 94 84 53 1a 4e 80 18 3b 81 59 a3 32 2b 37 7a d8 dc 4c eb c0 25 49 07 aa 89 df e5 e2 65 02 49 4b 58 12 d4 3c cd 4e 54 d8 46 a3 81 0a 02 58 48 a5 89 0f Data Ascii: >BG~Xd,)Fcl\H(9DW]rR&|bgVIFi#fH2*AkB=?2J*I!9Z!%@$=NGx6HGp]eq"RbcRub$,%SYb+*omSN;Y2+7zL%I eIKX<NTFXH
2021-09-10 09:33:46 UTC	101	IN	Data Raw: 59 52 61 65 6b 98 fa 4c 59 27 ed 26 c3 75 99 92 30 44 91 e4 ca f9 78 73 94 70 18 95 79 05 91 44 6c a2 02 b1 00 f3 52 52 82 6f d3 fb e5 41 43 15 7c 39 51 5b 3b 9a 90 18 97 6a ea 7e 32 88 39 64 c9 c0 68 0a 83 23 e3 e4 4f 8f db 60 50 3c 0c 40 74 6f 6f cb 0b 89 9b ca 92 a3 8e 7a e8 48 28 07 0b 9e 9d 58 7e 39 da 27 31 53 25 ad d5 40 48 0c 77 cd f5 77 89 0c a8 76 98 e0 da d1 ae 66 d7 fc 76 1d ff 00 e4 cd 18 e0 af 69 ff 00 d3 6d df f1 0c b0 bb 9a 83 7c fc f9 56 3c 3f f2 38 27 57 1e a1 fa b7 93 41 a6 9d 1c 5a 9e 9c 74 ac 89 63 94 77 02 62 97 66 2d 0e 7a 21 12 44 d7 b5 06 3e 6a 8d 80 1a 0a e1 4a d9 34 11 58 5c a5 9f fa 92 ed 97 7f d6 91 67 20 fd d0 65 a9 56 34 a5 73 b5 5b 97 c5 1f 1e 04 27 4e d2 1b 47 c9 c7 96 0c 9d 3e 47 98 63 be d6 7e d8 c9 44 55 50 3f 6e d0 cd Data Ascii: YRaekLY'&u0DxspyDlRRoAC|9Q[;j~29dh#O`P<@toozH(X~9'1S%@Hwwvfvim|V<?8'WAZtcwbf-z!D>jJ4X\g eV4s['NG>Gc~DUP?n
2021-09-10 09:33:46 UTC	103	IN	Data Raw: ba 21 92 ab fc df cf 46 c6 92 68 ee 48 6b 00 35 cf 5b 6d 11 12 92 e4 90 1f 5d a9 df ad eb 1a bf 54 a0 33 65 69 ba 9b ec ec f6 64 79 a4 1b 79 4c a4 a9 09 0b c5 ac d1 ed 2b b4 15 3e 6a f8 7f 82 99 87 ee 24 bf 88 96 02 a6 ed 4b d3 42 f9 6c f1 5b f5 07 0a 49 23 30 01 1a 1a 01 b7 79 45 a7 fe 96 b5 c7 3e 9a 8f 14 fb a4 c2 cc 65 50 94 de d7 bb 34 6b 6b d8 06 cd 70 28 13 c7 59 5f f5 24 9c 33 71 a5 25 94 90 41 e4 59 89 a9 fe a9 1b 1f f4 8c e6 46 17 66 52 9c 9b fe bd 4e 71 d2 9f 49 eb f1 a4 4b 34 c0 bc 52 04 86 58 98 03 4d da 05 de 44 20 5f 14 ab 63 e3 e4 75 8c 9b 2d 80 16 55 4b f3 1f 14 fd 47 d7 be 9b 3c a9 29 c4 a7 d8 b5 6b bd 9d b4 b5 9a d1 60 fd 2e c8 25 c6 78 a2 56 89 55 a4 04 37 ba a4 5b f7 c5 54 cd 43 8e 08 06 85 8e 7a 48 a0 80 49 a9 bd 34 f9 3d ed 1a 74 4c Data Ascii: !FhHk5[m]T3eidyyL+>j$KBl[I#0yE>eP4kkp(Y_$3q%AYFfRNqIK4RXMD _cu-UKG<)k`.%xVU7[TCzHI4=tL
2021-09-10 09:33:46 UTC	104	IN	Data Raw: db 20 28 b1 35 15 cf a8 2f e6 47 95 da 05 75 fc 2f 7c 99 2a 3f e1 e5 01 9e 56 91 99 bd a0 d2 c7 7b 77 10 cb 64 01 f2 7c 9e 83 f6 c2 c0 5a ea df c4 00 f6 eb d1 9d e1 a0 52 40 15 f0 e4 1b 3f e9 f9 56 d5 85 57 a9 60 9d e2 cc a7 ee 23 c4 24 5f 1b e3 05 29 64 5e 78 b2 2f 68 fc 59 ae 99 03 12 53 86 ce 28 69 fa ac 4b c2 1d 81 2e 0d 36 76 e7 4e b0 a5 8f 15 f1 75 4c 44 0b 1b 2a 4b 1c 72 c8 c0 06 91 b2 55 ce ea ff 00 c0 40 b6 e3 9f 8e 8c 83 46 cc bb 69 68 56 68 a1 2c f9 be 6f 61 df 3b b5 0a f1 b1 b7 ca 23 8a 16 21 77 21 95 c7 b4 06 2e 77 8b 5b 60 cd e3 9a ff 00 b5 47 ee 1c 45 39 d7 2f 9e ff 00 25 97 2d 78 01 35 61 99 a8 cb 96 c2 ba da b1 bb 8a d1 e9 39 11 4d 3e e9 4b 4e 51 d7 f5 15 49 24 00 cc 14 f8 1e d5 51 44 73 c8 3e 7a 10 01 4a 77 a5 1e ef ed d7 3b 47 27 48 c4 Data Ascii: (5/Gu/|*?V{wd|ZR@?VW`#$_)d^x/hYS(iK.6vNuLD*KrU@FihVh,oa;#!w!.w[`GE9/%-x5a9M>KNQI$QDs>zJ w;G'H
2021-09-10 09:33:46 UTC	105	IN	Data Raw: 12 01 a5 5e 99 1e 54 7e ad 1f 19 98 13 8a 76 37 aa d4 cd ce 8f 4a e5 6a 7b 42 cf d5 d8 8e b2 ea 3b 54 56 9f 85 0a a4 ca 76 95 8f 1b 86 75 1b 85 13 b9 f7 7c b1 0a 48 1d 5b 48 29 99 28 38 f0 86 35 6a 5d d8 97 a1 eb d6 f1 43 38 09 7c 45 49 bb 38 d7 cf cf 9b 5c 45 e4 fa 0d ea ff 00 b9 f4 bc 31 66 17 c9 9d b1 60 c2 27 b8 8c 11 55 0a e2 ce cb 25 01 de 8c 24 67 e5 58 75 89 fa c7 0e b1 39 4a 42 0b 63 2a 06 b6 7a 52 96 ae 47 36 ac 6f 3e 8b c4 20 c8 28 5a 9c 94 b5 1a bc c6 6d 5b e5 10 1e b3 c0 8f 42 f5 14 b9 5d e0 b8 f9 98 8b 93 01 8b 97 c6 d4 22 95 16 44 dc 08 52 b2 0d a4 d8 f1 f8 e2 c5 22 61 5c b0 8c 2a 0a 4d dc 30 cf 78 84 f9 48 97 34 a8 58 9e 5d d2 9f 11 0d af e5 e3 6f df 8e f2 49 79 65 90 4b 1e c0 d0 ea 58 cb 33 07 3c d0 19 0b 20 e0 d5 a8 af c0 3c b2 ea c3 50 Data Ascii: ^T~v7Jj{B;TVvu|H[H)(85j]C8|El8\E1f`'U%$gXu9JBc*zRG6o> (Zm[B]"DR"a*M0xH4X]oIyeKX3< <P
2021-09-10 09:33:46 UTC	106	IN	Data Raw: fd bb 5f 2c a1 19 85 46 78 a5 1d f9 8a b6 86 9f bd 21 83 3a 43 85 a4 ac d1 7f f8 b7 58 62 f7 12 91 ed 92 30 cf b4 21 b3 b9 59 94 fc 6e e7 a4 d3 45 a9 2f e2 39 38 7c f7 b5 61 e5 02 50 95 b1 c2 12 1c e4 0e 8f 9d f9 e5 06 ff 00 4a f0 96 38 b5 e7 c9 41 2a 04 79 21 5b fd aa e8 c1 63 0a 6f 75 11 63 cf f6 3f 00 e2 8b a4 01 53 8b 2b fc f5 f7 a8 76 38 70 ac 81 70 f9 5d eb b7 79 bd e5 f1 71 a2 8a 75 ce 89 92 45 33 41 a6 6a 30 9b 0d 0c 13 c8 dd 9d a4 91 61 40 04 2d 56 d0 4f 04 73 e1 44 82 69 40 f4 6f cc 15 ea 75 b9 eb fd 40 fe a9 89 91 89 84 d9 78 6d ee c3 2b 7b 89 01 93 be c8 1c 0f fc 29 7c 78 35 d7 99 2a 15 53 0b 82 5a ed 6f ee b1 12 40 29 19 bf eb e5 ba c0 fc f8 c3 23 40 c9 cb ee 26 ff 00 f8 90 ea 8a a1 55 83 89 eb b7 47 dc c8 ce 49 22 8d 8e b8 95 11 31 08 48 70 Data Ascii: _,Fx!:CXb0!YnE/98|aPJ8A*y![couc?S+v8pp]yquE3Aj0a@-VOsDi@ou@xm+{)|x5*SZo@)#@&UGl"1Hp
2021-09-10 09:33:46 UTC	108	IN	Data Raw: 15 40 18 ab 79 6b 25 81 73 fb 89 00 0a eb 37 c4 4c 23 16 65 d8 6b 7b 59 86 5e 51 b4 fa 5a 41 52 d5 7b 33 0a 13 e5 a3 db 20 6b 94 5c df a6 68 34 f8 7f 5b 19 19 a7 c8 86 18 e5 2a d2 3e 34 2c c1 1c d5 13 db da cd ee a3 5b 89 eb d2 8b b0 5d 1d af bd df ce a2 be 91 6f 3a 50 5c b5 29 26 a9 49 55 ea 30 82 6b 51 7b 73 3a 52 2e 66 8f e9 f8 a4 ce d3 22 8d d6 55 c9 c7 c6 7e cc 7f a2 44 50 52 18 e3 69 02 b2 f6 d5 77 8e e2 2f 70 29 20 f3 d5 ac 9e 05 0a 9a 06 27 4e b9 56 83 4d de 8c 3c 9f 1d 3f 8d 9b 2a 5c d5 b2 92 e0 80 75 ea 7b cd cd 89 96 bf e9 4c 28 97 1f 0f 1d c3 4e 76 e7 b6 4c 52 07 5c c8 32 01 8b 19 25 8f 73 08 e6 0c 26 33 ae e2 0a 88 de 86 ee 9b e2 7e 9f 2d b0 ca 62 a6 1f c7 7d 7e 2d ed 15 3f 4d e3 e6 2a 7a a6 cd 74 a5 3f f6 76 0d bb 3e ec da d4 d6 17 d9 de 97 Data Ascii: @yk%s7L#ek{Y^QZAR{3 k\h4[*>4,[]o:P\)&IU0kQ{s:R.f"U~DPRiw/p) 'NVM<?*\u{L(NvLR\2%s&3~-b}~-?M*zt?v>

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	109	IN	Data Raw: 0f 76 7b c7 26 55 b0 d4 0c c6 cc 21 59 a8 ea 11 bc 39 0f b4 ed 59 a7 23 76 eb 05 47 bc 2f c4 6b 28 06 db dc 4d 90 39 3d 4d 0e c6 fb 7e be 7d 63 d8 88 f0 b5 b0 f3 b5 f4 a3 fe e1 37 ae 32 16 76 1e dc 61 bd 88 76 3b 56 36 e0 90 f7 65 03 10 68 0b f2 4f 37 d4 50 19 75 a3 9c f4 66 7f 38 4b 8b 25 48 21 bc 4d 60 e0 dc 77 5f 76 8a d9 f5 15 95 a0 7c 84 31 84 2b 34 25 46 e6 df 21 0b c9 b3 4a 3c ed 6f 26 fe 7a bc e1 70 85 a1 49 20 b1 18 88 36 1a 9c f6 8c 97 d4 54 91 29 89 09 38 8f 87 47 1d d6 db 0c f9 f5 f5 e7 19 8f a4 f5 1b 45 58 d3 48 c8 b5 b3 68 ee fe d5 53 44 37 b7 9b e0 0b 1f 23 ad 47 d3 14 7f dc eb 76 ad c0 d8 5d be 74 8f 9b 7d 58 ff 00 c1 c4 56 e9 b5 72 50 d3 cb b6 3c c0 c9 c4 84 e0 e1 5d c1 b5 b3 4b 12 ab 4e eb be 52 8d 64 0d ee a9 18 56 f0 dc 7e 3a de 25 6f Data Ascii: v{&U!Y9Y#vG/k(M9=M~}c72vav;V6ehO7Puf8K%H!M`w_v|1+4%F!J<o&zpI 6T)8GEXHhSD7#Gv]t}XVrP<]KNR dV~:%o
2021-09-10 09:33:46 UTC	110	IN	Data Raw: 81 24 f9 16 6a b8 bf 3c 73 d4 14 aa 01 60 1b d3 f5 f2 60 ba 1e 46 bb d6 35 70 59 a5 79 f2 b6 85 57 99 d9 08 02 ff 00 cb b0 91 cd 1a e0 ff 00 a8 eb d2 d3 f7 0b 5a 84 d7 6f 9a 65 1e 8d eb db 25 b0 dc 1d d1 98 dd 5d 9e 47 f6 e3 e0 5f 34 3a 8c ea 10 06 49 20 f5 e5 e7 eb 10 98 3c 20 ff 00 ed f0 7b ae 91 5b be aa 6b 43 57 d7 f1 f0 50 ed d3 f4 59 97 23 33 6d fe a4 c0 16 8a 28 d4 7e 18 29 90 7f 6a e9 39 b8 52 92 48 bb 8b 16 d7 2f d5 0c 33 20 38 03 61 ec 28 d5 db 98 3b 47 37 fe b0 ce 32 b5 8c 68 65 a4 ff 00 8e 97 2d db 7d 00 11 cc 81 0a 9a 3f f8 6c 8e 0d 02 39 be ab d2 a2 e4 d7 0b 97 ce 95 66 15 d0 16 1c e2 ee 52 65 e0 20 8f 19 2e 0b 58 5f d7 6b f3 84 96 b9 30 9b 35 24 dc 49 1a 76 4e 64 8b 64 06 2e 15 51 c1 f1 61 00 03 f3 57 5d 11 2b 4e 20 1e ea 02 c7 51 b7 af ac Data Ascii: $j<s``F5pYyWZoe%]G_4:I < {[kCWPY#3m(~)j9RH/3 8a(;G72he-}?l9fRe .X_k05$IvNdd.QaW]+N Q
2021-09-10 09:33:46 UTC	111	IN	Data Raw: df 9c 46 74 b3 2c 8c 3f c4 9c b4 b9 a5 fe 5e 06 75 4d 48 ae e6 19 0a 4a 90 24 75 90 c6 ad 49 b9 59 9d 8a 93 cf 91 76 78 fc 75 d8 82 d4 9c 0e de 5a 54 5f 3c bf 70 8b f5 4e bb 3b 43 2a 45 91 df 32 34 8c ce 17 7f 24 82 b0 21 21 85 f1 b9 a4 71 5f 1c fc 88 cc 77 6e 4f ca 9d f4 ea 24 20 04 bb 3e 7b dd ed e4 18 d7 72 2d 44 fe af ea 12 a4 39 8c 32 25 ed ef 92 42 59 54 3c 72 6c 62 09 61 61 d6 32 2c 00 15 41 f8 be ad be 9f 29 38 92 f7 72 72 b6 84 8a d4 b5 3c e9 58 a2 fa ac c2 9e 1e 78 e7 4d 43 1a 72 ec 5a 13 fe 83 f5 e4 19 38 a0 b4 91 bb 18 62 c6 62 cf 61 df 1d 3b 92 52 79 46 26 da ff 00 ea a3 5d 6b d1 28 14 25 fe 5f e3 ca 3e 65 c4 4f 29 cf 5d 88 a9 7e c0 df 57 9a 83 d5 b8 d1 6a 4e 7b 88 0b b1 9e 26 2c 83 70 2c 09 5d c0 ed a6 ba 29 41 c1 e8 13 b8 51 81 c5 5a f4 6d Data Ascii: Ft,?^uMHJ$uIYvxuZT_<pN;C*E24$!!q_wnO$ >{r-D92%BYT<rlbaa2,A)8rr<XxMCrZ8bba;RyF&]k(%_>eO)] ~WjN{&,p,])AQZm
2021-09-10 09:33:46 UTC	113	IN	Data Raw: e5 76 33 7b 3d db a9 a9 68 df e0 11 f1 c0 d5 34 cc ae 45 bb ae fe bb 45 af 0e 84 f0 c7 08 0e a2 c4 1e 7e 4c cd 9e 81 a0 63 55 cb d8 50 87 4f d9 b1 d2 20 de e2 a4 85 91 2c 82 b5 fe 60 49 b3 e7 cf 2b aa 8e c7 f9 3b f7 d6 2c d0 83 30 a5 4a e9 fa ae 96 66 ce 02 f2 f3 62 69 63 56 99 04 bc 86 b7 0b 60 30 07 db 60 d8 55 fd a3 70 fc f4 03 33 0d 45 19 eb 7d bb f7 8b 64 4b 00 87 a8 19 10 4b d3 26 e6 2f ac 08 6b 19 69 36 44 0f 27 ea c7 04 ad ee 0c a7 60 1b 98 38 51 55 40 00 2c 92 0f 8e 90 98 b2 b5 87 c9 40 8b e6 d4 7c c6 d9 08 b2 92 e1 34 17 77 bb 30 cb 4b 64 cd 99 80 1f 50 ea 50 cb 9b 8e f1 ce 56 c3 44 9b 8d 6e 67 6d d5 ff 00 ee 78 35 f1 5f 3d 29 35 43 19 35 a9 ed fb f3 b9 64 21 91 b8 03 cb fa af a4 0b 7a ab 22 61 00 92 04 b3 71 28 db ee 23 f4 cd 1b a2 3d c4 15 5b Data Ascii: v3{=h4EE~LcUPO ,`I+;,0JfbicV`0`Up3E}dKK&/ki6D``8QU@,@|4w0KdPPVDngmx5_=)5C5d!z"aq(#=[
2021-09-10 09:33:46 UTC	114	IN	Data Raw: e6 14 92 01 49 02 ac d5 27 b0 6b ec 1f 5e 8f c8 9b fc 37 b6 8d 8b 90 af 26 3c 65 72 b7 2c cd 8f 9b 03 c4 0a a8 0b ba 32 e3 b7 22 12 40 6d a4 fc 1e 96 ef b2 7d 3d a1 b4 2c 09 63 ee 17 a5 f6 ef ca 26 f3 f4 bf f1 0c 74 9a 6c b8 d1 13 22 48 92 29 d9 97 69 40 dc c4 42 82 63 03 81 77 56 05 f5 e4 ad 28 24 53 bf 3e bb c0 d4 42 83 02 e5 dc e5 ea 6f 1d d7 91 42 b1 52 05 fb 5c 50 17 fc dd df fe 5d 6a e5 24 02 76 f7 3f d4 7c f9 0c ca 7b 38 7a 91 61 e4 df 2f ca 30 6d 7a f9 f2 cc a0 9e 0f bb c2 9a fc 79 15 e4 d7 3d 1a 3b 86 59 71 4a 8f fb 47 d4 df 66 85 a9 b0 2e 88 b1 44 81 f8 5f 91 60 7f a7 17 09 9f c7 af c1 80 94 21 a8 7d 15 fb cf 2c fd 23 dc d9 05 e3 29 18 23 6d a8 35 c3 12 01 f1 f9 3d 07 a7 7f a8 64 58 72 be a1 9a 26 34 94 66 83 f6 a9 60 4e e0 6e c1 07 87 ab e0 79 Data Ascii: I'k^7&<er,2"@m}=,c&tl"H)i@BcwV($S>BoBR\P]j$v?|{8za/0mzy=;YqJGf.D_`!},#)#m5=dXr&4f`Nny
2021-09-10 09:33:46 UTC	115	IN	Data Raw: 7f 76 c3 44 a8 2c 38 4b a0 d4 08 be 90 9a 95 03 51 5f 53 a6 f9 1e 8d d2 d8 2e 5a 8e 30 58 9a 83 fb 34 1f 36 a4 36 74 bd 6c 34 52 21 8d 92 29 d8 c6 a8 cd fa 6f db 24 05 0a 2f 69 f6 96 7a f1 c7 f1 d4 56 84 e1 05 aa d4 36 26 ad e7 9d 7f 30 57 4b ba 4b 8f f2 ad cf 57 73 57 af 4b 3c 14 60 65 8b 9f b4 0b c6 ea 0a db ee 2a d5 5e c8 81 2b 22 1f fa 4d 72 3f 8e 94 05 69 51 a5 3d ab d8 eb 43 0c 2a 63 25 3e 26 be 43 bb f9 7a 44 92 66 80 f1 a0 55 66 05 2c 30 3d 82 c4 12 18 be e0 21 db b4 0d b5 f1 67 8e 7a 20 29 50 62 6b 72 c2 b4 f3 cb bc a2 20 b3 11 fd c7 a9 75 09 7b 45 9f 74 b0 5b 8b c7 6d e1 59 89 2d bd 83 06 11 86 be 6c df e3 a1 a8 35 de 95 f2 ad f3 de 3b f7 2f 54 f4 3f b8 0c d4 f3 a4 64 66 02 43 b4 ab 46 de 14 50 d9 27 6d 09 d8 d5 bb 89 1c 10 2f 85 be 3a 86 31 a1 Data Ascii: vD,8KQ_S.Z0X466tl4R!)o$/izV6&0WKKWsWK<`e*^+"Mr?iQ=C*c%>&CzDfUf,0=!gz)Pbkr u{Et[mY-l5;/T? dfCFP'm/:1
2021-09-10 09:33:46 UTC	116	IN	Data Raw: 49 b9 1f f3 07 34 a3 fc bf b1 8f 07 93 5d 15 3c 48 49 6a 51 ed 71 d9 b1 1b 73 82 a4 e3 2c 0b e7 5d 05 cf 47 f7 cc 46 08 35 69 92 6d 8a e5 1e 30 64 59 9c 90 ac 07 b4 00 28 a2 ab 12 4a a9 36 7e 01 be 98 13 82 92 6a 4b 8f 7b 67 eb 0c 21 36 19 5c e9 f9 db 58 3a c2 d6 27 78 18 c8 60 b9 63 45 27 f6 b1 92 32 1e d5 43 18 ed ea 9b c5 df fa 74 7f f0 eb f9 df bf 58 02 92 53 31 d0 d5 f5 dc 5e 8d 97 e9 89 70 7d 5b 8a f0 ac 6a f3 7e 82 82 e3 22 22 51 17 7e d6 2a 2f 71 f7 58 55 56 14 45 92 07 47 0b 45 98 7f fc b6 84 26 f0 a7 ee 0b 97 2e 58 ea f4 d3 98 ad 33 66 89 26 d7 20 96 14 31 ac 85 a3 21 cb 31 24 10 18 a9 14 6f 6e f3 c6 df 9f 8b 03 a0 a9 7e 22 cc ce f9 e9 cf b3 11 ff 00 6f 70 f6 ca 83 95 f6 f2 dd e3 53 2f 2e 57 8e a0 54 c7 bb 73 1b 1b bf 95 04 70 b7 47 8a be 2b e7 Data Ascii: I4]<HIjQqs,]GF5im0dY(J6~jK{g!6\X:'x`cE'2CtXS1^p}[j~""Q~*/qXUVEGE&.X3f& 1!1$on~"opS/.WTspG+
2021-09-10 09:33:46 UTC	118	IN	Data Raw: 16 05 fa 3e 79 5f 91 e7 10 02 38 b1 f2 a3 19 0e 5f 1f 32 44 81 d5 63 21 b7 c8 19 5a 8e eb 0c 18 ab ed 34 01 52 cb 67 cc 93 30 f8 ca a8 49 61 9b b5 ef 6c af fb 15 f2 d2 a9 8c 05 00 bf 37 ee f4 7d ac 5f a1 6f 9f 0a 04 ee 15 c8 c1 6c bc 6c a3 21 36 42 6e fb 72 e4 8a 56 76 0e 94 78 25 ba ae 9a 30 cc 2a 1f e5 96 df 37 f4 8b 34 80 90 12 92 69 fc bd ed e7 78 8e c9 87 1f ee e3 c3 a7 12 1c e0 98 d3 a2 8b c6 9e 54 57 c7 2a c7 dc 11 df 74 52 a9 24 02 77 0a 23 a9 8f 10 e9 50 29 6b f7 d6 39 89 42 60 76 6f 2d 9b 99 cf 96 b0 d6 cc 56 cb d4 f4 5f 52 64 41 1a f7 c4 78 9a 9a c6 9b 12 2d 5b 0e 38 a0 ca 52 09 62 61 99 04 33 03 c0 62 cf 43 8e 14 0a 20 2d 3a b9 ea 46 5c b2 2d be 90 e2 c5 12 aa 96 15 f8 ed ee 61 87 e9 fd 67 0f 4c d6 4c 79 b0 c9 3e 14 78 59 6d 0c 30 d2 19 a6 0e Data Ascii: >y_8_2Dc!Z4Rg0Ial7}_oll!6BnrVvx%0*74ixTW*tR$w#P)k9B`vo-V_RdAx-[8Rba3bC -:F\-agLLy>xYm0
2021-09-10 09:33:46 UTC	119	IN	Data Raw: 14 d2 a2 9a 21 c4 23 ed 2d 2a 72 f8 81 c4 79 f7 96 b9 45 f9 f4 66 ab 2a 61 68 f3 98 99 e1 c9 c3 c2 3d e4 a9 0c 6c 51 15 c9 1e 43 6e 1b 77 af 1f 3c 8e b1 bc 5c bc 3c 4c c3 5b d3 26 e5 af 57 8f a1 7d 36 6b f0 92 88 bb 57 d1 ad ca cd 16 1f 40 d5 23 9b 3b 34 4f 36 c7 6e c1 8e 55 e3 7a 2e d0 19 df fc 92 82 29 d7 80 cb e3 cd 74 8c d9 52 c8 2a c2 ea b0 56 6f 5b 9e cf 47 8b ce 1d 6a 52 80 2a 25 25 25 83 e6 1b 4c c4 59 9f 47 ea 0e 54 02 d0 cc 23 01 15 b7 5b 46 0d f2 f7 ee 56 6e 76 f0 0d 5d d0 27 aa 75 82 ea 49 2e 0d d3 95 6e f7 e5 1a be 0a 6a 7e dd 17 95 00 3a 8d 2f 73 ee 74 8b 1f e9 9d 4f 68 85 9c 99 d6 70 19 ce fa d8 91 ed 0a c8 a4 d5 f1 44 f8 24 5d fc 94 a6 c9 48 a8 4d 36 7b 79 e5 1a 2e 17 88 08 40 a9 07 98 3b 0f 50 0b 16 73 46 87 4e 91 aa 45 90 a4 df b5 18 10 Data Ascii: !#-*ryEf*ah=lQCnw<\<L[&W}6kW@#;4O6nUz.)tR*Vo[GjR*%%%LYGT#[FVnv]'uI.nj~:/stOhpD$]HM6{y.@; PsFNE

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	120	IN	Data Raw: 8f 2e 2e 9e da 4c d9 99 91 48 59 60 50 b1 84 8d 94 33 fc 6d 76 8d a9 49 b3 19 36 41 ae 7a a9 9b c5 09 c1 7f f2 12 e0 b0 77 ab 8e ce 91 73 27 83 9a 56 00 05 29 34 2d 6d 2c de b1 6a be 99 7f 4b fe b0 f5 40 c4 c2 d3 60 c8 f4 de 04 e6 1f b8 d5 24 0e 72 12 12 db 1b ed 92 39 1b 19 a5 68 e8 83 2c 61 01 a6 23 cf 49 2d 72 82 43 b1 34 ad 1d cd eb bf 56 8b ee 13 82 4c a7 33 70 a8 33 a4 2a 95 77 63 5d 74 ab 5a 91 d8 cf e9 f7 fa 75 f4 d7 d2 4d 1e 28 52 79 f5 6d 42 65 66 c9 d5 f5 44 85 75 09 64 2a b6 bb e3 89 50 45 ee b0 a8 80 50 e7 a4 38 89 c9 4a 99 80 4d f4 f5 ef f0 ac f9 bc 54 e5 30 43 07 2d 42 13 96 55 bb 53 f2 62 e1 62 c5 8e ca b0 08 c3 70 a3 bb 65 82 ad 6d 50 82 95 41 bb 24 d6 e3 63 c5 5f 49 2d 61 56 cf a3 7a 57 b3 03 08 98 81 fc 94 14 2e 01 b1 ea 0f 2f 5a 88 92 Data Ascii: ..LHY`P3mvI6Azws'V)4-m,jK@`$r9h,a#I-rC4VL3p3*wc]tZuM(RymBefDud*PEP8JMT0C-BUSbbpemPA$c_I-aVzW./Z
2021-09-10 09:33:46 UTC	122	IN	Data Raw: 79 24 a1 80 c7 22 c9 89 3c 6c ac 2d e2 c8 91 1c 87 14 a8 59 97 cf 55 0b 42 a6 4b 52 4b 95 02 a7 71 93 96 f4 2c db 69 58 d1 49 9a 94 2d 24 1a 61 41 d5 e8 03 03 7b 57 66 ad e1 f1 36 3c fe a8 f4 7c da 5e 46 39 93 23 32 29 f2 71 64 28 01 59 f0 58 a4 5b 4b 59 1b fb 7b b7 0a 05 4f 92 0f 59 e9 0b 1c 3f 16 54 a6 01 c8 d0 39 39 8e 76 39 0a de 2d e7 a3 ef 4a d4 10 fd 8a 5f f5 15 c3 5e c2 19 ba 5b cc 17 60 8c af 7d 2c 83 8f 34 28 52 78 14 d5 da 94 de 9c 8e 3c 1e b4 bc 1c cc 20 13 50 a5 05 02 74 b5 34 0e d6 1f bc e7 12 87 4a a5 9b 8f 40 39 da fc bc a1 5b a4 2e 4e 2c f3 45 94 56 4c 4c f9 1e 17 94 2d b9 87 24 32 63 b4 a5 ff 00 69 dc 36 97 fd c1 40 af 3c 5c ad 45 d0 45 28 68 f9 d4 00 fa fb c5 30 97 84 4d 25 4e ce 0b ec 45 3d 59 ff 00 b8 c5 a8 60 47 93 88 91 43 9c 5f 53 Data Ascii: y$"<l-YUBKRKq,iXI-$aA{Wf6<|^F9#2)qd(YX[KY{OY?T99v9-J_^[`},4(Rx< Pt4J@9[.N,EVLL-$2ci6@<\E E(h0M%NE=Y`GC_S
2021-09-10 09:33:46 UTC	123	IN	Data Raw: c7 c5 f4 76 98 99 32 22 3f f8 6e 6e 54 44 9a 2c d2 87 0b da 65 0a 03 29 65 04 9f 9b 00 93 d5 72 e5 63 98 e9 2c ed 99 a7 b0 bf b9 8b 14 a8 04 8e be ff 00 b8 5e c4 f1 67 fa 62 3d 33 24 40 27 7d 3c b8 69 3e 64 91 0c 5e 58 d7 70 a8 8e 44 bb 2e 40 5f 8e 48 94 19 6b 4d 5e f4 77 14 f2 88 4c c1 84 8d 7b 66 df 96 74 b4 06 fa 36 2c d6 d3 3d 41 83 8f 0a a4 a6 1e cb ee 65 b6 31 c6 32 95 c2 9a f7 b2 2d c7 f1 40 fc 74 c4 c3 e0 04 b5 c3 f9 f7 d4 40 24 a0 85 9a 9c 00 1a 51 f2 67 c8 77 a4 44 6a b9 39 9a 6e bd e9 0c 9e fb 49 89 a8 e7 39 95 97 6a 85 9a 34 1b 15 f6 fe 37 95 04 7c 71 cf 9e 88 80 85 4b 51 f1 52 bf 3a 75 c8 56 b0 39 8e 66 04 7f 8a bf 91 37 19 bb d0 65 a6 d4 88 4d 67 14 03 34 92 22 a2 ca f9 71 4a de 18 33 b1 45 6d dc 92 4b b2 92 09 04 71 d4 e5 ac 05 a6 60 ba 68 Data Ascii: v2"?nnTD,e)erc,^gb=3$@'}<i>d^XpD.@_HkM^wL{ft6,=Ae12-@t@$QgwDj9nI9j47|qKQR:uV9f7eMg4"qJ3E mKq`h
2021-09-10 09:33:46 UTC	124	IN	Data Raw: 34 26 63 7d 63 d3 19 d1 ea 9a 26 63 e0 e7 2b 15 2d 1c 87 84 52 7f 49 62 27 b4 eb fe 53 1d 05 ab 36 09 e9 e3 31 13 53 84 b1 4d 9d be 6b d6 2a 4c 8e 23 86 56 29 78 83 1d f9 e4 1f e6 d5 20 43 77 48 fa c2 f9 4a b1 6b f0 cb 0e 5c 5d b4 39 78 a0 98 66 35 c3 98 41 dd 18 b3 ef 20 fe e3 c7 02 8a 93 78 34 d9 fc cf 5e 94 b0 ad 05 af 16 bc 2f d5 56 7f f2 93 b1 ab f7 b1 19 c3 5f 4a fa 95 a1 c2 85 e6 d4 a4 42 8c 94 b1 23 77 77 55 a8 93 f1 ee ab 26 eb cf f3 d5 6c ce 0c 02 79 de 8f 56 ef ce 2f 13 c7 ac 80 50 a2 c5 ef 7e e9 b4 1c 60 6b af f5 0a 5c 18 73 fb 9f e0 d8 cc 04 50 09 7b 72 19 a3 62 7b 8c 9f b1 c4 96 0d b9 dc c3 fc b7 7d 08 e0 90 96 70 f9 db 3b 79 dc f4 b4 31 28 4c e2 96 9c 45 4c 74 a1 a7 21 a5 e2 f0 7d 2d f4 46 97 90 71 95 21 06 08 92 38 fb 6d 1a 13 22 b0 3d a1 Data Ascii: 4&c}c&c+-RIb'S61SMk*L#V)x CwHJk\]9xf5A x4^/V_JB#wwU&lyV/P~`k\sP{rb{}p;y1(LELt!}-Fq!8m"=
2021-09-10 09:33:46 UTC	125	IN	Data Raw: 26 cf 02 19 b1 f7 3f e6 0d ea 84 08 d5 d7 b6 24 60 08 60 f5 c9 6e 6e ec 81 60 03 c5 74 e2 70 e5 72 c6 f6 c9 bc fb ac 66 e7 82 a5 62 04 ea c6 a1 bc f6 63 ca 2a d7 d6 42 d1 fa 7b 58 85 41 de d0 3c 11 05 3b 64 de 64 a1 5b 87 ba af 9f 1b 80 35 7e 3a bc fa 6b 85 05 0d 5a b9 52 f4 cb 2f 7c db 2b f5 49 81 12 d5 ad 45 b5 7b c7 17 3e ad eb 69 a6 ea 99 71 cf 16 c9 a2 7e c0 32 a2 b2 b3 b4 2a 5a 48 ff 00 ea 06 3e 28 fe d6 66 fe 3a fa 3f d3 a5 95 4a 0a ae 66 9c 9c 39 3c ab 6f 98 f9 0f d5 a7 21 33 56 01 a1 51 37 e4 d6 b6 d5 fd 43 69 fa 6c 9a d7 a5 7d 64 a1 56 55 97 4b d2 5b 1e 2a 01 a3 ed b4 bb d9 87 21 41 04 11 5f 80 6c 74 61 39 32 a7 90 ec 74 6a bb 50 8c b9 0d b3 8a dc 06 64 92 a6 a1 a1 6e 8c 5d de 94 ac 0b 7a 33 0c cd a0 6a 8c b6 cb a6 6b 5a 7e 30 a5 1c 63 a4 4f 8a Data Ascii: &?$``nn`tprfbc*B{XA<;dd[5~:kZR/|+IE{>iq~2*ZH>(f:?Jf9<o!3VQ7Cil}dVUK[*!A_lta92tjPdn]z3jkZ~0cO
2021-09-10 09:33:46 UTC	127	IN	Data Raw: 05 8e 7f f5 fc 75 e0 9c 00 e7 4e 56 8e 8a 3a 1a ea a9 de 83 fb 0f eb 1c d9 fe a0 75 b9 e5 ce c9 8d c8 78 e5 79 26 dc 77 16 10 a5 a4 62 87 e4 01 4a de 2c d0 3c 74 a7 10 7f 8e 58 94 de 75 87 e4 80 0a 2b 40 c7 d6 80 f9 f5 f4 8a 9d e8 c8 22 93 51 d5 35 57 9c f6 e0 31 00 36 10 54 72 58 d9 14 76 d7 c1 bf f6 00 d7 f1 09 b2 0d 42 bd 1a b5 1a e9 af 28 b4 92 42 54 b5 82 f8 88 e4 05 ba be 8d 08 7f a9 92 24 99 39 53 2c 8e 4c b9 19 0f dd 2c 4e d1 e2 3d aa b7 7c 1f 34 3e 45 7c f4 e7 02 e9 f0 a4 b3 67 d2 dc bd 77 84 b8 d1 52 41 1e ee 3b f6 a6 50 0f e9 15 10 e6 e0 c1 24 8a 5e 6c 85 9d 50 b6 c6 03 b8 a1 5c 11 61 59 b9 1b 6b cf f7 e9 ae 21 d8 a8 d5 c1 77 77 d4 d7 2c bb 68 e7 04 a6 71 9d 2a fd 6d 5e e8 61 cb ad 8f b8 d6 74 dc 48 d4 01 91 24 05 19 80 12 99 27 90 42 58 91 c1 Data Ascii: uNV:uxy&wbJ,<tXu+@"Q5W16TrXvB(BT$9S,L,N=\|4>E\|gwRA;P$^lP\aYk!ww,hq*m^atH$'BX
2021-09-10 09:33:46 UTC	128	IN	Data Raw: 27 42 f4 7c e1 87 a3 e3 9c 86 8d e7 3d b8 e2 6b 54 51 fb c0 21 63 0c 14 fb a4 52 6c 9a 36 3f b1 e8 c8 95 87 27 f4 f2 a3 81 d8 80 4c 9a b2 ac 41 4d 5b 3f 3b bb 79 d1 fc a1 81 87 84 00 91 1a 37 ef 2a 99 54 33 59 17 ca aa a0 2b 5f f5 1d c0 80 3e 47 47 42 42 85 3c 26 bb ea 2f 7b c7 84 f5 1b 92 75 1e f6 f2 d7 6b 46 5c ad 2e 37 82 55 09 b8 40 49 74 2c 2c 32 94 74 62 49 ab 52 7f 6d 9f 1e 3a 34 b2 30 00 a4 b9 0e e4 d3 33 96 de f6 30 05 61 52 ca ad 8b ab 5a f5 1c df 2b 55 a0 17 57 f4 d4 79 6d b8 c0 aa 63 6d d0 b6 c0 cf 1c 8c 09 dc 08 00 7e a0 62 0f 8a 07 8a e3 a9 a2 6a 9c 10 e9 02 87 57 70 75 3d 6a 79 dc 08 ae 5a 48 ad 6e c7 4b 79 fa 5a 13 9e a2 fa 7f f7 07 fe 45 f7 03 38 b0 54 83 64 32 11 7c a9 a2 6e f7 10 2a b9 ea c6 5f 13 87 0b d8 d4 10 5e a3 30 33 bd 0d b5 06 Data Ascii: 'B|=kTQ!cRl6?'LAM[?;y7*T3Y+_>GGBB<&/{ukF\.7U@It,,2tbIRm:4030aRZ+UWymcm~bjWpu=jyZHnKyZE8T d2|n*_^03
2021-09-10 09:33:46 UTC	129	IN	Data Raw: ea ef 47 b0 16 cf d4 d9 9e 57 ec c8 d0 22 77 3b fd ef d4 62 80 6c 8f 95 00 82 49 f2 2f e7 9e ba a2 50 58 54 db d2 0e 85 b3 82 7a bb 7c 39 6d 2d f2 37 9f a9 1e c7 70 b8 fd 76 40 25 4f f9 88 1c 85 3d df 1c 77 18 2b b0 17 4a 2f 8e 3a 19 40 0c 49 04 9a 12 df c5 f3 27 41 f3 13 2b c4 d5 b5 68 74 eb ae 8d a3 c0 0e a2 92 2c dd dc 89 e3 09 1c 72 17 de ff 00 a6 cf bb 6d 85 52 4f 37 63 dc 01 aa a3 d0 e6 49 35 28 2f f3 5a d0 9f 9b c7 3e f8 52 b0 81 cc bb f3 19 7a 1e ba 2d f5 dd 49 4c 72 e3 c0 76 03 b3 bb 38 76 89 5e 48 e4 16 54 af b9 41 1e d5 00 7b 8d 03 43 9e 86 99 44 e6 1e b6 14 fd 47 8a 9a e1 f7 39 57 95 6e ed b6 cd 10 d3 4e 5f 73 28 12 6d 09 ee b2 ce ac e2 98 1f c2 9a 04 d9 e4 fc 81 5d 31 2e 5e 07 ab 93 b7 f7 f1 9e b0 bc c9 a0 39 1e 59 35 72 dd c5 32 6b d6 21 93 Data Ascii: GW"w;bII/PXTz|9m-7pv@%O=w+J/:@I'A+ht,rmRO7cI5(/Z>Rz-ILrv8v^HTA{CDG9WnN_s(m]1.^9Y5r2k!
2021-09-10 09:33:46 UTC	130	IN	Data Raw: 29 8d 70 b1 49 df 13 46 3f 78 d9 26 ca 65 25 85 10 dc 72 35 55 38 95 5c 9a da f9 f7 58 60 0a b2 7c 2d d7 d3 5a ea 79 44 a6 36 4c 53 ea 5d dc 6c 87 4e f6 14 93 4d 0a 30 42 92 3c f0 d5 6d 04 34 6a 01 0b 74 56 c0 37 7d 1a 4a 18 3a 48 0e 05 83 df 73 09 71 2b 0e 19 35 14 bf eb 6f 9c e3 fa 13 c7 20 7f 9b dd 5b 80 02 c8 1c 8f fc ef fb 1e b4 25 4a 29 6a 3d 3d fb b4 62 14 09 04 0b ef 4e 91 95 99 9b da f4 55 c3 00 6e 8d 8e 6e c5 78 36 7c f5 c4 96 3a 39 01 43 98 b6 f7 6a 5e 01 67 d4 7b f7 a4 7b 88 49 dc 02 23 c2 a8 f7 73 ee 04 d7 20 9a e3 f3 d4 a7 29 92 c2 e7 cb 46 eb f1 05 42 b1 0d 4e bb 7e bb d8 6b d4 82 4c cc dc 3d 13 71 11 a4 91 6a 59 cd 5e c3 00 b3 8f 01 16 46 e9 76 6e b3 f0 28 0e 97 90 a5 32 b2 38 88 e5 af ae 7c a3 cb 03 0b e6 19 b9 3b 37 7f 30 71 0b 2a e2 81 Data Ascii:)pIF?x&e%r5U8\X`|-ZyD6LS]lNM0B<m4jtV7}J:Hsq+5o [%J)j==bNUnnx6|:9Cj^g{{!#s)FBN~kL=qjY^Fv n(28|;70q*

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	132	IN	Data Raw: 46 71 bb 8d 24 4a e8 55 76 b1 0f 16 fe 77 4b 56 ac 8e 38 25 8d 01 7f 3d 53 f1 4b fb 8e 84 7f 81 6a e7 ad de 35 5c 1c c0 97 c6 59 ea 39 87 b9 15 be ef a5 21 8d 83 37 dd ad 34 aa 64 55 59 04 b2 1f f9 6e 38 01 96 3e 19 18 80 bc 92 39 da 79 ea a6 62 08 20 f8 6b be 75 8b 9e 1e 65 c9 2e 09 a5 f6 f2 f6 17 82 3c dd 52 3c 4d 36 42 64 98 e5 24 68 23 18 f1 b7 eb b3 46 a3 68 1b 4e c8 f7 96 ed 8e 38 3c f3 d2 4a 07 10 09 b3 db 36 a1 d3 bc e2 d3 ee 27 08 c8 81 d1 c3 0b 5b 2e a6 fa 46 a7 a5 fd 07 9b aa 30 d6 f5 7b 0a e5 a5 c7 c5 63 bd e4 89 b6 9a 94 15 bd ca 40 3b 45 1d de 3a e4 d4 e1 4f 87 3b ef ad 77 a7 74 80 89 ab 36 a9 e4 1b 77 7f 4e 9c 83 43 17 1a 14 90 e2 b2 04 ed a8 dd 5b 55 85 da 82 6e b6 f1 e4 79 a0 2b cd f4 35 25 04 05 24 57 f9 17 19 06 7a 1f ed a0 2b 9a b0 d5 Data Ascii: Fq$JUvwKV8%=SKj5\Y9!74dUYn8>9yb kue.<R<M6Bd$h#FhN8<J6'[.F0{c@;E:O;wt6wNC[Uny+5%$Wz+
2021-09-10 09:33:46 UTC	133	IN	Data Raw: dd 23 5f ee 6e 2f 68 e4 2f 82 78 f2 6c 2d 39 2e 40 34 e5 95 b9 eb 05 93 34 a5 40 a5 44 a7 fa df ca b7 84 be a8 23 89 9a 06 70 d2 45 5b 48 50 15 01 15 db 62 fb 4d 23 12 a5 41 2d f2 01 1c f5 14 12 92 30 b9 d8 eb d5 fc ce 51 67 26 79 2b 0e aa 67 7d 5f a5 bc a0 33 21 5a 09 48 8e 18 e6 6e d9 21 43 92 1e 2d ff 00 aa 17 fc c1 d8 05 b6 f2 a1 78 ae 7a 3a 15 e2 2e f5 a3 8a 87 bf e7 21 90 d2 2c 14 b1 30 32 4d ec f4 0c d5 af 3f 4b bd 1b d1 d4 15 51 6e 65 63 0a 48 a3 1b 90 b2 46 58 95 ab a0 7b 7c ee dc 43 37 9f 15 d1 aa ed 46 6b bd 7c bb e7 1e 96 85 84 90 5a aa 39 e5 6a b5 2f cc 83 e9 ee 2d 4c c8 b2 15 db b1 00 0f 0c 6a 58 ab 2d 16 2a ca c4 fb d2 c7 e0 58 be 14 f4 44 a9 c8 72 28 0d 4f 4e df f3 02 9d 89 93 84 66 6e 6b 96 6d db ef 1a b9 bf f1 d0 4d 24 69 97 8d 0c 45 65 Data Ascii: #_n/h/xl-9.@44@D#pE[HPbM#A-0Qg&y+g}_3!ZHn!C-xz:.!,02M?KQnecHFX{|C7Fk|Z9j/-LjX-*XDr(ONfnk mM$iEe
2021-09-10 09:33:46 UTC	133	IN	Data Raw: 41 49 00 10 48 a8 7e 7c bd 7a d2 02 8e 20 33 87 7a 65 4c a8 6b 5d da 01 f5 34 8e 44 30 ac 6a 65 67 72 cc 11 96 81 52 58 ee e7 73 5d 1a 02 cf 8f e3 af 09 64 3b 80 2b 56 73 fb ec c3 42 70 12 88 52 bc 45 d8 8b 87 66 f2 39 13 7a e4 f1 07 14 39 6a 02 01 ba 47 40 0b c4 85 ad c1 04 17 55 ba 35 cd b7 83 e4 0f 1d 45 45 23 3a 75 d2 2b d7 36 85 2e ec ef e7 4f 37 67 89 3c 4f bd 9a 29 4c 50 ef 38 87 b4 cf 33 04 0e eb 61 e3 da 85 77 2e d2 58 8b 20 30 51 f9 e8 13 16 2f 5d 2d dd 3b 3b 05 94 73 0c 79 d1 fb f7 d4 c4 06 b5 8d 1a 45 39 52 b4 56 20 aa bf b9 91 b9 20 93 c8 65 36 a6 bf 82 3a 83 92 c5 36 7a 9b 30 63 ed e5 4c e1 49 a8 18 80 17 24 bd a8 00 34 07 90 a7 2b 08 a1 7f d4 0e 20 97 46 cf c6 ee 8c 68 e5 8b 26 36 99 94 ba dc 91 ec 45 65 fe 6d b9 1c 8f 9e 38 eb 57 f4 7a a9 Data Ascii: AIH~|z 3zeLk]4D0jegrRXs]d;+VsBpREf9z9jG@U5EE#:u+6.O7g<O)LP83aw.X 0Q/]-:;syE9RV e6:6z0cLI$4+ Fh&6Eem8Wz
2021-09-10 09:33:46 UTC	135	IN	Data Raw: 35 92 47 1e 7e 08 f3 d0 67 0e 66 82 da b9 ed a3 8e 51 56 6b 5e 9c b9 73 81 ac 65 9b 27 5f d7 f2 c6 d9 a2 49 63 85 a2 00 b3 2f da 42 63 17 f8 16 6d 45 f8 b0 7c df 5e 32 c2 00 c3 50 a4 82 5b 2a 7a 17 26 08 16 3f 8a 88 0f 67 2c ef b5 99 9b 0a c4 f0 9a 4e c0 44 3e e6 ff 00 21 04 5f 04 16 1f e9 f8 fe 3a e0 21 05 99 c0 6a e5 7c 8b d2 ba c7 00 f1 d0 51 a8 72 cb ba 7b 42 83 ea 77 a8 13 4c c2 78 da 40 b2 ae 3c 8a df 2c 86 50 15 3d b7 65 99 81 aa 1f c9 e3 ae a9 49 2c 5c 3e 84 f9 1f 58 32 0a 7e e0 49 04 95 02 47 af 9e 47 4a e7 1c 9c fa 8f ac 2e 66 ab 3c 50 49 dc b9 18 10 58 92 8c cc 01 63 c5 d2 d9 26 fc 9f f5 e9 29 ca 2a 74 e9 57 1e 59 13 ef f1 16 52 70 a5 78 08 67 4d 29 bf a4 49 ea 0a f8 5e 8b c8 ee 10 42 e1 81 02 b8 74 dc 0a fb 8a 93 bb f7 1a a2 17 9f 35 c7 55 Data Ascii: 5G~gfQVk^se'_Ic/BcmE|^2P[*z&?g,ND>!_:|j|Qr{BwLx@<,P=eI,\>X2~IGGJ.f<PIXc&)*tWYRpxgM)I^Bt5U
2021-09-10 09:33:46 UTC	136	IN	Data Raw: 12 38 7b 4a 8f 14 6a 76 04 03 da 56 af da a4 78 a2 58 d5 80 2f 83 a4 a5 49 25 4c e0 0a 16 7a fe 36 a3 f9 40 cc e6 0c 2a a7 7a 57 a5 e9 60 f9 fa 42 e3 54 d7 b1 f0 27 76 99 e3 5d b6 a5 81 b7 0c 1c 90 43 72 0d 03 67 71 2d 5d 49 32 44 c7 c2 6f 92 4f 6d ca 9f 9a e9 fc 43 3b aa ce 72 d2 99 65 6d 6b bc 66 d0 bd 6b 85 3c 82 31 34 66 31 71 9f 78 f7 12 c7 6d bb 5e e5 6b e0 28 b1 cf 81 7d 32 9e 17 0d 4a 54 1f 57 76 17 cf ab f2 84 47 d4 31 16 00 13 b7 7e 50 d0 d3 3d 41 18 9f 6e 35 b0 58 cb d0 7b e1 86 de dc 64 10 0d b7 20 fc 79 aa 04 08 af 86 24 38 73 76 a3 00 29 5d fc ff 00 31 69 22 78 29 75 29 8b 3b 13 6a 1e 94 b5 ad 94 30 71 32 b1 63 47 26 58 e2 9e 60 65 78 da 42 c0 86 40 6a c5 47 bb 95 e4 7b 4d 11 64 91 d2 8b 93 91 bd 2b f8 a3 c5 8c 99 a2 60 0c 45 77 f9 27 3f 30 Data Ascii: 8{JjvVxX/I%Lz6@*zW`BT'v]Crgq-]I2DoOmC;remkfk<14f1qxm^k(}2JTWvG1~P=An5X{d y$8sv)]1i"x)u); j0q2cG&X`exB@jG{Md+`Ew'?0
2021-09-10 09:33:46 UTC	137	IN	Data Raw: c4 c1 27 10 d1 81 35 bb 12 1f 6a fb 58 a3 4d c0 46 21 a5 57 97 11 24 de 27 86 4e d4 89 db 16 c9 32 b2 ee 96 30 48 01 ae b6 f0 7c f5 cc 49 d4 74 af b4 30 a4 78 46 24 dc 9a 90 c4 58 7b 07 e7 9e b8 f2 17 50 4c 85 58 c0 38 59 66 4f 76 da 65 8e d9 12 32 ad e7 b9 65 ad 68 01 e3 93 d7 84 c0 3c 40 12 35 6a 68 7c bd e9 03 99 21 0a 41 0e 1e 87 f9 7c 3b eb ef 9b 44 44 d0 e0 ab 14 9b 16 6d b8 c8 7f 52 45 db 53 90 41 2a 2e 99 54 80 00 da 5b e7 c1 e9 84 28 29 49 74 e6 3d c7 51 f1 15 ab 42 d2 54 14 f8 43 d4 9a 6d d4 8d 21 79 ae c6 df 79 1f 62 67 6c 72 bf a8 e0 ae d0 8c bb 54 07 22 d4 a9 fd c3 f0 45 71 d3 35 0b c4 d4 6e 8e ff 00 af 48 09 2d 44 8a e8 c4 d3 a4 03 ea 6a 5a 61 09 31 b3 92 84 32 92 0b d0 a6 65 1f 81 cd dd 37 04 78 ae 88 b0 91 57 03 50 e3 da 05 89 4e 41 2c 5c Data Ascii: '5jXMF!W$'N20H\|It0xF$X{PLX8YfOve2eh<@5jh|!A|;DDmRESA*.T[()It=QBTCm!yybglrT"Eq5nH-DjZa12e 7xWPNA,\
2021-09-10 09:33:46 UTC	138	IN	Data Raw: e3 49 21 68 34 a5 85 c2 b1 45 7c 89 2e 36 76 02 83 48 b0 48 c3 6d 36 d5 b3 c5 f4 29 98 48 c2 e1 9b 5b e4 36 ec f5 64 a9 86 2f f2 2e ed a0 b3 8a e4 29 67 3c e2 32 2c bc e5 47 cd 7e 37 f6 71 fb 8a e0 ab 94 13 30 a5 04 15 3b 04 7b 89 02 c8 f9 f3 d1 d3 82 c5 40 5b 30 3f 5d 3f 10 a2 d2 a3 52 7c ed ed e8 7d 23 fa 58 00 05 dc d6 50 01 40 58 6a f8 3c 5d 28 ff 00 b0 fc df 37 f1 90 20 1a 77 ae bd f9 c7 86 f1 b8 f2 84 de d1 cd 0f c0 fc d9 e7 93 f1 f3 d7 a3 98 53 76 b5 4d 74 e7 fb f8 8d d8 99 21 1d cd c2 95 0c 9f 34 9b 6f 8f cf c5 d0 f0 7f 8e 94 52 de 66 17 39 fb e4 fd 07 75 e1 46 33 42 c7 5d bd bb 61 11 9a 11 77 c1 9b 31 42 2c 99 b9 19 33 e4 6e 03 7c 8c ce 76 31 23 e7 b7 b4 0a f8 a1 40 8e 8a 54 e0 0b 00 03 ee dd bf 58 87 db c6 e4 d7 09 d2 ed ae d9 f7 5c f3 e5 fb 63 Data Ascii: !h4E|.6vHHm6)H[6d/.)g<2,G~7q0;{@[0?]?R|}#XP@Xj<](7 wSvMt!4oRf9uF3B]aw1B,3n|v1#@TX\c
2021-09-10 09:33:46 UTC	140	IN	Data Raw: 60 3a 80 7d c7 7d 88 b0 18 38 19 87 15 64 6c 65 12 05 89 52 67 61 b0 1d c5 e4 31 82 76 d3 5f 1e ef fa 47 8e a8 c2 dd 4a 07 fe cc 1b 2f 32 7c e2 f5 32 98 5a b9 1b d7 6d 32 6b df 5b 6c 63 cc 22 d6 99 8c 06 31 8f 0c 48 a2 32 84 17 31 95 de cb 74 64 34 68 b0 e0 b7 f1 d7 94 ac 00 94 d3 15 09 6b 01 b3 7f 7c 8b c7 2d 7f d8 2f 96 86 97 d3 ca 34 3d 57 ea f2 30 a6 88 05 89 e3 62 ac ac e1 0b 14 52 36 c8 a2 80 3e ed c3 60 22 eb 71 3d 12 40 c7 bf 3e 9f bf dc 2b 30 b6 22 2e 09 eb 5f 9d ba 47 39 be b0 7d 6b 87 40 c8 c8 8b 27 35 61 6d c4 b1 12 12 a6 f7 02 9e d0 2c 86 1e 48 b0 0d df 15 d6 a3 e9 9c 08 98 6c 6a df df 6c f7 7d 32 df 51 e2 16 87 20 9b 12 d6 b3 97 2f cb 21 d2 b0 17 f4 8b eb ae 2f a9 33 fb 31 ea 02 5a c8 d8 15 5a ca b0 f6 b0 23 f7 02 13 94 23 c9 e4 75 77 c4 fd Data Ascii: `:}}8dleRga1v_GJ/2|2Zm2k[lc"1H21td4hk|-/4=W0bR6>`"q=@>+0"._G9}k@'5am,Hljl}2Q /!/31ZZ##uw
2021-09-10 09:33:46 UTC	141	IN	Data Raw: ae e8 23 8a 5a 23 91 d1 84 a7 20 8b 3d 9a c3 e7 be a1 5a 70 b3 d5 35 23 a1 af 5d f4 6e 50 bd 97 fa 88 c6 c3 cb 5d 2e 79 e1 82 51 20 8a 45 47 b6 df e1 4d 29 f0 d4 0f 3c 1e 2b a2 61 98 09 08 b3 7a 64 7a 79 5e f9 2e a9 32 c8 13 0d 6a f7 2e fe 97 e6 fe 70 d8 d0 7e a5 62 6a b1 42 6e 37 79 b8 07 63 b2 bd 9f 6b 31 e5 96 bc 9e 2f 8b be 83 39 68 6d 35 f6 23 97 cd f2 80 7f b6 58 aa 1c 7a ea f6 e9 fd d4 96 eb 58 b8 1e a0 c1 92 27 95 24 7d 84 21 8d 2c ee 07 95 70 d4 78 f2 ad f3 fc f1 d2 13 26 a0 57 f5 af bd 9a d0 c4 89 53 02 aa 5c 8b f4 77 15 b3 b7 f5 92 b3 d3 38 52 a6 54 f8 93 c1 25 c1 23 08 e4 23 da ca ae c3 6e d6 b0 ad 54 05 8e 7c 5f 4b fd e1 35 d2 f4 d2 f5 f4 b6 ba 0a de 2f b8 64 cc 06 94 25 47 3c a9 4c bc fa c3 8b 4b d2 a1 e1 9c 18 db 73 c6 cb 26 cf b7 94 4a bb Data Ascii: #Z# =Zp5#]nP].yQ EGM)<+azdzy^.2j.p~bjBn7yck1/9hm5#XzX'$}!,px&WS\w8RT%##nT|_K5/d%G<LKs&J

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	142	IN	Data Raw: 61 c2 54 7f f6 57 90 af be 5d 60 a0 e4 ed a8 f2 ca c7 7e 9a c6 1c 39 5b 03 31 32 e3 0c 19 54 e3 39 60 a6 36 8a 51 b5 e3 64 aa 20 90 6f e7 c1 bb 1d 0a aa 7a db 2b 53 32 3f 3d 32 86 e5 86 7a 33 90 db b6 9c bd e1 b1 e9 7d 45 f1 f2 92 7c 59 a6 1e e1 1a 32 b6 de dc b2 46 16 e7 e0 19 31 a6 a0 18 1b 50 a4 93 e0 1e 90 e2 12 18 9c c1 0f cb 2f 71 bd 2f a5 b7 0e 58 97 b1 04 1e ad 04 f3 07 87 50 46 64 4d b9 2e 32 77 2d 14 8d 9f 74 6f 18 db 40 15 16 bf 1c 51 1e 3a 49 44 a9 26 b4 4f 2c b6 ed b9 43 26 5e 15 24 ea 41 1d 8d 7b 16 82 ec 0f 51 64 ae 95 93 1c c5 a6 d3 e4 ce 8e 21 1a 92 19 8e 04 59 11 26 41 6a 3c 87 9b 68 f2 29 7f bf 49 af f9 1e 9e c2 1b 42 73 cc b3 0d bf 27 db 3c a2 37 54 91 f0 13 03 0a 22 21 46 c7 7c 85 73 ef 13 a1 64 45 72 40 fd ca 4b 0a 23 da 2f f3 5d 4e Data Ascii: aTW]`~9[12T9`6Qd oz+S2?=2z3}E|Y2F1P/q/XPFdM.2w-to@Q:ID&O,C&^$A{Qd!Y&Aj<h)IBs'<7T"!F|sdEr @K#/]N
2021-09-10 09:33:46 UTC	143	IN	Data Raw: 19 e4 74 ae 90 d0 fa 5b ac 8c 6c 0c dd 3b be 55 b4 cd 55 a7 83 74 9b 77 61 ea 0f df 54 8f 75 b3 c6 85 9d 7d bc 2d 15 f8 e9 7f aa 20 2c cb 50 01 b0 e4 36 d4 66 43 50 ed 06 fa 54 df b6 a5 a4 9f f2 b1 a1 02 f4 e4 0b 01 43 17 3b d2 7a bf dc c0 89 2d 48 1a 35 04 31 e3 da 49 55 27 fc 94 3d c3 fe a1 5f 9e b2 f3 e5 94 aa da 86 b3 f4 b7 9d 87 23 1b 39 53 3c 09 6d b3 34 6b 87 df d3 23 0c 04 96 67 9f 18 4d bd 71 8c 5d 83 2c 66 ca 2b 31 d8 18 58 ae cb 20 bb af 22 fc f4 1c 2a bb 7c 7e e2 45 45 47 37 34 6f cf 7e 90 65 a0 4a b8 d9 51 f7 e4 8a 44 c7 32 a9 db 1b 47 21 70 d6 93 29 2c 02 77 23 a2 49 b5 03 cf 00 74 25 ff 00 05 72 3a 35 db 9f cd 2a c5 dd d9 5e 09 81 cd 19 e8 f5 b5 3a 1f cc 3f bd 0f aa e3 89 7e e2 64 60 df 72 e9 18 82 6e 24 46 a2 ac ca a5 81 1b 01 dc 2a 89 e6 Data Ascii: t[l;UUtwaTu}- ,P6fCPTC;z-H51IU'=_#9S<m4k#gMq],f+1X '"*|~EEG74o~eJQD2G!p),w#It%r:5*^:?~d`rn$F*
2021-09-10 09:33:46 UTC	145	IN	Data Raw: 41 06 30 73 96 36 7d c6 31 ca 94 2b 47 b5 e2 ef 63 ca 8a c1 76 b4 91 b2 ac ac 4f 26 ca f2 47 5c 3c 32 00 70 ee 05 36 e5 13 1c 48 b7 8a bb 8a 0f 7d 5c 00 3e 22 05 fd 6f 95 88 21 2a f3 e2 be 01 ee c2 ee ec 62 3b 4d 18 55 51 8c aa 4b 0e e6 f7 35 ca 8d a0 5f 42 57 08 a5 58 16 d6 a6 fa 1f 87 3e 90 65 4c 94 53 e3 52 4b 35 d8 e7 d7 d7 9b 52 24 13 eb 4e b1 7b c6 b2 a1 1e b6 c5 3c e4 89 11 88 69 46 e7 3b 46 d7 40 a2 ff 00 b8 17 e3 9f ed 66 ab f9 06 ae 6e 4f b7 b3 96 85 54 8e 02 65 54 90 29 5a 37 6c ed 93 f2 8c 52 7f 52 39 18 ab 22 cf 98 a9 24 56 85 c6 5b 39 08 c7 70 50 09 0a ac 14 7e eb 66 3e 3a 8a b8 75 82 52 05 2a ce 1b 6a 6a e7 4e 46 b7 5c f0 32 16 a3 80 f8 47 f1 b5 bd 6b af f5 03 ad fd 54 64 63 39 9a 49 da 48 11 64 a5 ee 06 24 93 b2 83 33 82 6d 7d c4 9a af 8f Data Ascii: A0s6}1+GcvO&G\<2p6H}\>"o!*b;MUQK5_BWX>eLSRK5R$N{<iF;F@fnOTeT)Z7lRR9"$V[9pP~f>:uR*jjNF\2G kTdc9IHd$3m}
2021-09-10 09:33:46 UTC	146	IN	Data Raw: fc 2a b9 67 06 fa 34 23 3d a5 f1 94 2e 55 57 6a ea c2 95 a9 cf f1 06 72 6a 5b f4 2f 54 e1 3c 5b da 4c 22 1a 2f 24 b4 30 a6 44 64 0f 21 f6 1a 20 0e 48 1f 23 84 8a 49 9f 2c 87 b8 b7 97 f5 a4 31 c3 a8 60 9a 82 18 b1 24 e8 e0 65 c9 ac d7 61 0b 5c 78 e2 38 7a 33 47 8b 32 33 89 71 e7 90 98 d9 15 1e d6 12 c1 05 82 ac e4 7b e8 a9 23 82 3c 5a 29 6c 54 33 f0 d2 bb b9 bd 4e af 9f aa f3 03 a1 25 85 45 4d bf c8 dc d7 3d 73 e7 03 11 c9 93 a3 6b d0 6a 1a 7b f6 33 71 d6 1c 93 b2 d4 49 da 98 a4 8c c4 7f 21 58 a8 3c 80 07 82 47 45 52 c9 90 7d 3c 9d c9 c9 ac 75 85 a4 86 9c 5e c4 16 22 81 dc 30 05 df 77 eb ac 58 cd 6f 51 83 4d d2 34 1c ec 6c 6e e6 3b cf 36 a5 91 11 60 87 21 35 96 df 9d 8d 20 5a 56 8e 39 7b f1 ae ee 10 32 72 68 11 49 8d 4d 30 b5 47 f9 58 8a fb 9d b2 a5 a2 da Data Ascii: *g4#=.UWjrj[/T<[L"/$0Dd! H#I,1`$ea\x8z3G23q{#<Z)lT3N%EM=skj{3qI!X<GER}<u^"'0wXoQM4ln;6`!5 ZV9{2rhIM0GX
2021-09-10 09:33:46 UTC	147	IN	Data Raw: 99 0d ef 42 d3 88 d5 98 03 ca d2 79 3f db c9 e8 2a 94 92 a4 12 cc a2 c6 b9 0a 36 d7 a7 20 21 81 30 b2 f0 b0 c2 80 68 01 62 d5 b8 ce ef 12 b8 52 1c dc 1d 27 52 90 40 e9 ad e1 cb a4 64 64 72 3b 39 11 3f dc c3 63 ff 00 82 64 48 80 51 f2 d7 e7 9e b8 a4 fd 99 8b 09 a0 24 61 b5 00 77 6e 67 da c2 38 92 26 26 5a d8 85 07 c7 d4 8a 96 d9 ed 96 a2 17 7e a1 df 0f ac f5 0c 68 16 46 c7 d4 34 b5 9b 10 16 26 d9 01 23 80 08 52 ac 24 42 df 2a 41 3e 3a 9b 29 52 ca c9 24 e2 0d b7 6d 4c dc b7 2e 10 cb c4 2c 5c 1a e4 68 28 7f b8 14 d0 e6 39 23 d5 78 14 c1 71 5b 1f 2c 4b 93 c4 8a 4b 76 e4 1b 7e 14 35 15 fd c3 68 fe 7a 3c d2 d2 a4 80 c9 52 c8 04 9e 7b de dd e4 8c a3 8a 7c e4 2a a9 09 27 0f a6 94 cf 96 5b 95 7a 4b 5a 3a d6 a5 27 a7 b5 39 76 6a 58 d8 f9 11 e0 6a 08 09 69 52 38 d4 Data Ascii: By?*6 !0hbR'R@ddr;9?cdHQ$awng8&&Z~hF4&#R$B*A>:)R$mL.,\h(9#xq[,KKv~5hz<R{|*'[zKZ:'9vjXjiR8
2021-09-10 09:33:46 UTC	149	IN	Data Raw: e9 1f 5c 70 34 dc a4 fb 9d 43 2b ed c4 06 09 53 23 10 23 76 f6 b3 02 32 55 55 9e da d0 b4 c1 98 2d 73 7d 2d 33 e9 a5 41 c2 12 08 76 a9 ad 0d 0b 28 fc 43 29 fa 99 92 13 f7 65 4c 96 ec 31 81 72 01 70 46 87 b7 b4 32 f4 6f ae 2b 90 af f6 ba c4 39 8e f3 a4 d8 2d de c8 49 31 22 3d be e6 3a c4 d3 f6 18 15 0e ac cd 1e e3 64 f9 ae ab e6 7d 3a 60 a1 94 30 b1 73 56 6a 68 7c bc f4 8b be 1b ea 5c 2c ec 03 ef a9 2e 18 bd 2b 87 37 0d 56 61 78 70 69 9f 57 b0 f2 27 95 b3 71 b2 82 cc 71 d2 31 c4 d1 c2 ce 2e 42 8c 7f 7e 31 24 d9 04 6c 3e 41 a3 d2 8a e1 14 82 70 a5 b0 82 73 ae 1c af eb 48 b8 e1 17 33 1a 95 29 78 c0 f1 0c 4c 08 cf 41 6a 7b 43 c7 d3 df 50 b4 2c 29 5b b2 c8 e3 bf 8e f8 f9 1d d0 b3 62 3c 4c 5b fe 18 73 71 ad ed 72 c7 90 4f c0 be 96 29 52 ff 00 92 48 26 a7 6c af Data Ascii: \p4C+S##v2UU-s}-3Av(C)eL1rpF2o+9-I1"=:d}:`0sVjh|\,.+7VaxpiW'qq1.B~1$l>ApsH3)xLAj{CP,)[b<L[sqrO)RH&l
2021-09-10 09:33:46 UTC	150	IN	Data Raw: 69 70 7b ef 78 0d d6 da 14 b8 e6 90 2d 30 55 ee 30 46 62 cb 4b fc 51 e2 89 1e 40 e3 a9 23 f9 56 b4 2d ce 1e 96 5d 2c 0f 37 da a3 ba 42 e3 50 0b dd 20 c2 12 48 cb f7 99 64 f6 31 51 b1 40 e0 02 a5 6c c8 47 05 a8 fe 6d e9 69 2c 4a ec 05 19 9e dd 8a e9 9c 27 3b 88 01 45 09 0e e5 b7 ad 2b 6b 65 01 19 b1 15 69 20 52 84 7f cc 8c 90 00 e7 9a dc c4 59 00 df 1c 10 2c 78 e9 84 2c 61 c2 94 b1 ad ab a5 7b b9 78 09 00 a7 15 ce b5 d6 b0 23 24 69 1c bb a7 2a 94 cd 2b 4a ad ed 60 41 a2 ab c7 22 bd c0 f0 79 fe 7a 31 2c 2b 5f 98 e2 49 70 1e 9f 02 23 9e 58 e3 08 c6 55 20 04 a5 91 76 aa ed 61 ef 45 65 fd c0 5f 86 da 07 f2 3a af 9a 17 8d 45 2c c7 47 1f e3 cb f2 cf b4 10 97 a5 88 6a ea e7 3e c1 e6 20 2f d4 da 93 41 13 03 2a ba bb 05 d8 8a 19 ab dc ff 00 bb c9 53 fd 80 fe 7a f2 Data Ascii: ip{x-0U0FbKQ@#V-],7BP Hd1Q@lGmi,J';E+kei RY,x,a{x#$i*+J`A"yz1,+_Ip#XU vaEe_:E,Gj> /A*Sz
2021-09-10 09:33:46 UTC	151	IN	Data Raw: e4 f8 85 95 15 09 1f b8 a8 92 94 9f 80 6a c7 47 13 d2 2c 4f 94 06 5c b5 61 7c 89 cc f6 dc b4 68 fe 8f a1 b4 b6 21 4d 02 a0 8b 15 c5 a9 56 bf 9e 2b fb d0 1f 1d 5f 2c 31 e7 53 de 91 87 50 c4 96 76 07 43 5e fd 39 b4 6b a9 69 58 b1 dc 09 04 8e 39 00 02 2a 8d 2d d8 e1 ae fc 9a eb a8 0e ee 4e 56 a7 ef 2d 60 7f 69 2c 7c 4a 7d cf 7e d1 87 21 19 7b 43 9d cb 20 7a aa dc a5 48 20 30 fc 7c 5f fe 67 ae ac d5 bf b8 f0 0a 03 0e 12 40 d8 9f 51 df 48 f1 99 2a c3 1e e2 48 3c 70 3e 0f 14 49 f2 07 e7 f9 37 d2 f3 1d a9 b9 af 63 78 ea 12 e4 9c d2 c7 d7 7f 68 43 7d 4a d5 65 5d 27 51 06 4d aa 61 90 00 08 e6 89 f7 46 49 f2 47 07 8b 00 9f e7 a0 25 6a 25 ad e8 46 df 91 d7 28 3e 00 b4 82 49 7a 91 5d fc ff 00 19 67 1c c2 f5 46 40 d4 3d 45 8d 86 63 67 fd 5d e3 da 8c 69 25 b2 39 ab f1 Data Ascii: jG,O\a|h!MV+_,1SPvC^9kiX9*-NV-`i,|J}~!{C zH 0|_g@QH*H<p>I7cxhC}Je]'QMaFIG%j%F(>Iz]gF@=Ecg]i%9
2021-09-10 09:33:46 UTC	152	IN	Data Raw: 06 b3 f2 89 cd 2e 6e ce 54 f1 c1 3f be 39 92 74 b1 47 70 55 5d 89 c5 35 2b 55 b6 ea 5a 37 7d 27 c4 24 94 30 ae 43 2f 3f 3c a1 be 16 6a 65 94 90 6d ab 83 ed 6c ff 00 b8 b4 3f 4d b5 f6 81 d7 b6 5b 1b 2d d5 90 b3 11 3a a9 5b 2a cc 58 9a 7d d6 37 da ed 56 a0 41 03 ac b7 1f 21 c3 d4 10 36 6a 74 03 a0 e7 1b 7f a6 f1 08 50 48 26 fa 52 e1 ed fb 06 94 a8 8e 80 7d 39 d7 e1 c9 d1 f1 96 67 7d f3 d6 f2 87 72 97 fd ac c1 ec d0 b5 1e 38 af e4 f5 9c 5c a7 c5 8a 8c e5 bf 2f 4b 67 58 d0 95 82 d8 4d ae 3b eb 0c 76 8b 18 c3 34 e1 a4 70 96 06 d0 ab 23 bf 25 59 1c d6 e5 03 8b ba 17 e2 f9 2b 94 24 02 58 16 27 20 d7 6c a1 94 28 b8 49 a8 39 9b b3 1e 7e c4 e9 10 d9 b9 0d 24 56 44 6e a3 1d ea 3f da cb 22 30 02 26 e6 d8 95 f7 3b f9 63 c7 e7 a3 4a 5a 92 52 58 33 8b 3b 80 f7 02 db be Data Ascii: .nT?9tGpU]5+UZ7}'$0C/?<jeml?M[-:[*X}7VA!6jtPH&R}9g}r8\VkgXM;v4p#%Y+$X' l(I9~$\VDn?"0&;cJZRX3;
2021-09-10 09:33:46 UTC	154	IN	Data Raw: 36 a6 62 0b 3f fd 3f 30 ad 25 69 2d 89 c3 e9 bf 91 a0 14 30 e8 f4 a7 d0 9d 03 05 f0 f2 71 f4 6c 5c 59 5c 05 0c b1 46 dc 84 a8 cc 91 80 0c 6d 0d 5a 35 92 c2 83 12 47 40 4f 19 3e 61 20 a8 91 cc f3 6e 87 df 94 75 7f 48 97 2c 02 65 80 90 ce 7b 7e 56 ce 2c 96 8d f4 ff 00 4f f4 fe 34 59 b2 2a 16 78 a5 10 ef 80 31 62 e3 64 86 d8 b1 1e d2 36 0b a5 f2 39 ae a1 32 72 80 20 97 3a 1a 6a 48 f6 7e 7c e1 15 25 24 aa 5a 7c 29 4d d8 07 ad 81 f7 03 2f 23 0d ef 47 68 92 ea 79 d1 4b 8c 86 0c 00 d1 46 55 68 cb d9 58 e8 a4 c6 c0 00 4a 3e 07 2a 7f 8e a9 b8 89 ca 2e c7 3e c6 fa d1 b5 72 62 ab 8b 9a 8e 1d 2a 18 89 05 5a bd 2b ed 17 1f d2 b8 5f e1 58 c2 28 17 d8 ea 02 2c 9e 19 af 69 16 b4 1d 8d 7b 45 78 f3 75 5d 57 ae 60 2e 0a bc 59 69 a0 0c 47 b1 ca f1 85 fa 8c c1 31 65 92 92 2b Data Ascii: 6b??0%i-0q|\Y\FmZ5G@O>a nuH,e{~V,O4Y*x1bd692r :jH~|%$Z|)M/#GhyKFUhXJ>*.>rb*Z+_X(,i{Exu]W `.YiG1e+

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	155	IN	Data Raw: 10 65 30 79 14 93 b9 43 23 ec 61 57 44 83 d7 26 84 cb 9d 88 12 eb 35 d3 98 b5 da c4 88 60 f8 f8 72 90 5f 12 59 c5 dc 04 9e cf 9b 31 8c 9f 4c f5 07 93 ff 00 79 7d 2b 96 e8 a9 ac 34 7f 6f 22 c8 ad f6 92 5f db 48 db 6c 6d 90 07 89 c7 ca 84 35 c3 11 d7 b8 84 31 4c e6 25 49 ca 8c 1d b5 ab 8c bc a2 32 16 58 a0 b1 0c 45 6e db 1f 3f 27 d2 16 f9 7a 7c 9a 4e ab 3e 1e 52 3a cf 0c d9 5a 7c c4 90 94 f1 4a 55 78 00 12 ae 81 5d 48 fd ca d7 e3 a6 50 bc 72 f1 1a 12 f4 16 b5 5f 93 bf 90 bc 56 ae 5f d8 5e 12 28 68 fe b7 b0 ef 68 f5 94 87 ed f5 6b 50 d2 41 81 08 47 f1 cb cb 18 4d cb c0 6a 5b ba e6 e8 f9 1d 4a 53 78 56 e6 e0 d3 2f eb a3 8a 51 e2 13 93 88 03 5f 0d 07 23 ad 7b d8 3c 06 e1 61 41 06 7a 98 de 9a 59 62 d9 bc 1d 81 c3 2c a5 57 fe a0 42 1a 20 8a 24 ff 00 62 ec e9 f8 Data Ascii: e0yC#aWD&S`r_Y1Ly}+4o"_Hlm51L%I2XEn?'z|N>R:Z|JUx]HPr_V_^(hhkPAGMj[JSxV/Q_#{<aAzYb,WB $b
2021-09-10 09:33:46 UTC	156	IN	Data Raw: 01 96 d4 7e de 7f 1d 31 c3 a8 14 00 43 1b 56 bb 33 b7 3a 65 10 9e 96 99 88 57 93 f4 16 fc 52 37 70 75 61 26 8f a9 b4 03 63 e1 e7 60 1c c5 48 fd 9d f6 42 24 90 fb 82 a8 98 8b 01 47 2c 2f fc c7 a1 4e 96 ea 0d 42 5f cb 21 f3 9f bc 76 54 c0 10 cd 91 17 b7 cf 4e c6 86 a6 13 31 31 71 32 42 8c 2d 4a 04 74 61 49 d9 9c 02 57 21 2e a9 92 f6 92 09 16 68 9e 86 81 e2 99 93 12 5d af 7f 7c bc c6 b0 72 5d 28 3a a7 3e 91 a9 ea fc d9 63 83 40 99 91 4c 49 0c b8 93 ca 52 ed 36 ae 3b 34 dc 92 77 29 13 2b 31 3c 92 7e 3a 2f 08 a2 16 41 27 0e 22 28 45 59 86 74 62 7a fb 42 dc 6a 71 4a 76 f1 00 0d bd 35 d6 17 de 8f c8 71 1e 6e 36 51 91 c6 99 97 24 31 cf 20 26 31 b9 98 a3 c7 76 18 48 00 ba 3f 35 d3 bc 54 a0 90 99 89 2d 89 dc 1b d1 cb 1e 87 3f c4 23 c2 95 29 2b 4a 8b b6 16 a0 a5 df Data Ascii: ~1CV3:eWR7pua&c`HB$G,/NB_!vTN11q2B-JtaIW!.h]|r](:>c@LIR6;4w)+1<~:/A'"(EYtbzBjqJv5qn6Q$1 &1vH? 5T-?#)+J
2021-09-10 09:33:46 UTC	157	IN	Data Raw: e3 c7 52 1c 52 c2 1b 06 b4 39 55 ef 1d 33 e5 92 e8 98 80 12 6c 48 04 f2 e7 de 6f ad 07 a4 b0 35 4c e4 d3 f1 60 b6 66 58 8c 52 c6 23 8e 50 cc 19 1d cb 2d a3 6c 1b 96 8f 24 11 d0 bf de a2 98 c9 49 25 83 5b e3 5f 7c a2 6b 51 fb 61 68 00 e1 0e a0 08 71 41 98 2d 56 36 a9 87 66 8d fd 29 7a 9f 5e cb d4 32 74 ac 4d 06 18 34 dc 49 72 e7 9f 51 99 a0 c2 9c 43 14 32 b6 10 15 b0 e5 49 04 c2 48 94 c8 15 96 ac 80 c0 8b 9e 13 e9 dc 5f 18 8f b8 94 94 ca c3 88 2d 45 d2 76 0d 72 44 61 3e b3 fe ba e0 7e 96 85 48 75 2b 89 2a c0 50 0a 41 09 2e 09 63 93 b3 d3 f2 67 f3 bf a5 3d 09 9f d4 d0 e7 eb 99 d8 59 5e 9d d1 e0 d4 e4 c2 d3 a3 83 22 12 b9 58 d8 99 53 17 8e 7c c8 17 0d 34 a6 cc 48 e4 09 1c e3 21 09 54 2e fc 99 9e 0f ed a5 78 c8 18 53 53 4a 6a 59 f6 62 6e 69 94 57 f0 ff 00 eb Data Ascii: RR9U3lHo5L`fXR#P-l$I%[_|kQahqA-V6f)z^2tM4IrQC2IH_-EvrDa>~Hu+*PA.cg=Y^"XS|4H!T.xSSJjYbniW
2021-09-10 09:33:46 UTC	159	IN	Data Raw: 4a ca d8 91 ca 86 59 25 2a 40 21 c9 6d 88 56 eb 8b e7 9d e7 fa 7f e9 9f 76 72 66 90 30 20 05 33 12 09 70 18 1d 6a 3a 16 b0 2d f2 ff 00 f5 97 d6 53 25 1f ed 92 4a 94 a2 5d 49 21 83 a5 ab 9e 84 e6 f1 c7 9f 52 42 de a1 f5 e6 5c d1 63 93 10 de f1 e3 d9 fd 28 e2 6e dc 92 36 ee 55 9c a9 7b ba e2 87 8e be a2 17 f6 b8 75 04 90 92 43 50 d4 38 cb 6b da ee d1 f2 12 94 cd 98 92 b6 27 11 2f 4f c6 4f 53 0c 4d 0f 53 c3 79 f5 33 05 28 86 68 e2 89 58 92 18 96 31 10 16 eb dc 14 1f e0 5f f3 d5 2c f1 ff 00 19 06 a4 97 70 1b b7 e7 47 8b 9e 11 49 13 31 50 84 8b 5d fa b1 66 67 21 b6 86 e7 d3 fd 57 ec b4 0d 4e 79 63 56 dd fe 26 92 9f 69 5f d4 28 b6 01 04 72 5a 97 73 51 a5 1c 9f 15 7c 54 95 7d c9 24 a8 5d 39 1a 3e 6f 5d 9f cc 38 31 7d 26 67 fc 73 08 4f f2 7e 84 bf c9 d3 a4 2f b0 Data Ascii: JY%*@!mVvrf0 3pj:-S%J]I!RB\c(n6U{uCP8k'/OOSMSy3(hX1_,pGI1P]fg!WNycV&i_(rZsQ|T}$]9>o]81}&gsO~/
2021-09-10 09:33:46 UTC	160	IN	Data Raw: ed 6c be 6f ac 08 2b c2 03 d2 83 5a 8f cc 73 82 54 c7 cc d4 e5 90 19 36 41 dd 9c 12 d6 ae ec 48 0a a8 68 81 c1 36 7c f9 e4 0e 92 98 4e 15 1c ef eb 16 9c 19 c2 40 23 33 4e 9d 9f 66 85 76 b7 24 cf 95 a8 b0 50 58 4c 98 cd 1b fc 42 57 82 a4 0e 2e f9 e4 ff 00 dc 74 49 2c 02 71 50 90 32 d4 9b 5f 6f db 43 93 90 16 e5 d8 8a dd e8 28 de e6 85 bc a2 43 d2 85 fb 7a e6 a4 85 4c 72 a6 26 9d 07 b5 4f b8 48 ae e3 c7 2a a1 45 9f fd 10 f1 2b 52 56 c2 c2 8c 5d b9 5c 5e 0d c2 a4 10 4a bf 8b de 91 a9 97 03 26 76 af 14 6a e7 2b bb 8e d2 7f 9d 44 45 91 42 b5 70 bb b8 23 e0 1f 9e 08 eb 88 2c 92 a3 6b f2 d7 ba 7c c1 09 05 4a 62 f5 3b 67 0e 5d 00 c9 a4 7a 0f 58 40 8c 5b 23 2a 49 7b a1 3b ae 81 a3 08 8c ab 65 c8 27 9e 28 00 2a 8f 3d 27 8c 19 cc 0e 80 f4 ed b5 a9 82 e1 64 03 4e 6e Data Ascii: lo+ZsT6AHh6|N@#3Nfv$PXLBW.tI,qP2_oC(CzLr&OH*E+RV]\^J&vj+DEBp#,k|Jb;g]zX@[#*I{;e'(*='dNn
2021-09-10 09:33:46 UTC	161	IN	Data Raw: 1e a9 2d 71 b7 20 3d 39 88 a5 e2 51 81 44 8c eb 47 b5 fd db ac 56 9f 58 7a 78 ea cb 97 99 a7 43 b2 78 d4 c5 da 32 0b 99 d0 9f 0d b8 a8 e0 57 00 1f ee 7a b6 e0 e6 14 b1 51 a8 7a 7b 12 c0 da 83 4c ab 13 e1 78 b3 26 62 5c 91 6c 8b 9a 72 a0 f8 31 56 72 b2 f3 34 bf 50 ac b9 91 e4 41 1b 65 44 32 57 20 3c 67 97 db b2 36 e2 d5 94 51 23 8a 20 81 c0 eb 53 c3 ac ce 94 40 03 20 e4 80 45 2b 4f 47 6d a3 4f 2e 7e 20 95 95 10 0d 68 72 df 95 ba 87 86 94 fe b5 4c dc 9c 0c 41 0a 9c 4c 3e eb e3 41 08 50 f0 ab b0 73 ee 60 1a 5a b0 bb 9c 92 45 80 68 74 bc ee 0d 20 12 77 66 0e e7 bb 5e 34 5f 4f fa 92 d2 b0 8f b8 48 6f 09 20 eb e4 2c f5 ce f1 65 7d 10 d8 5a 9e 99 93 9c cf 16 30 85 a1 c5 99 63 99 bb 91 1c 88 e5 91 1d 21 16 4a 95 fd c0 0b 0f e3 8e b3 bc 54 b0 95 14 91 e0 56 c5 c7 Data Ascii: -q =9QDGVXzxCx2WzQz{Lx&b\lr1Vr4PAeD2W <g6Q# S@ E+OGmO.~ hrLAL>APs`ZEht wf^4_OHo ,e}Z0c!J TV
2021-09-10 09:33:46 UTC	163	IN	Data Raw: 9b bf 76 f1 87 12 17 72 c0 73 b8 29 5f 90 7c 72 48 3f df a8 2a 62 89 21 ff 00 7d 22 4f b0 6e 54 b7 c5 f5 16 88 79 e7 9e 7c b1 1b 22 94 8c 3e db 6e 45 a8 24 f1 ed b0 78 af f6 ba e0 71 c5 61 4a 4b 9a ea c5 af b7 ae f4 d2 3f 1d fd d8 c5 10 12 39 19 a9 50 9f dd 60 93 7c 8a e3 8f 1e 0f c5 fa 22 96 21 20 55 a9 41 9d e8 29 cc 9f c4 47 e4 45 1d 99 9e 37 8c 2c 6e 56 41 45 58 3d 52 b8 f2 59 1a 9b c8 e0 50 1c f5 15 25 ea f0 40 a2 90 68 e3 3a 96 cb ce ed b8 b6 b0 0f a8 ef 4d cf de 62 43 95 06 b7 06 55 23 82 ac 39 04 1e 06 e3 40 d5 d8 ea 49 41 49 e6 ce ed bd 7d d9 f4 ce 3a 66 5a 9c ff 00 1b ea 20 57 23 2d c3 05 99 01 8e 32 58 30 a4 2f e4 28 20 df 2b 7c 72 05 d5 0e ac e4 94 a7 09 b9 6f 82 fd e5 68 82 c0 50 6c 55 71 c8 56 ac c3 e6 ba 98 0f d6 b3 f1 e4 8f b0 19 f6 bb 7b Data Ascii: vrs)_|rH?*b!}"OnTy|"\>nE$xqaJK?9P`|"! UA)GE7,nVAEX=RYP%@h:MbCU#9@IAI}:fZ W#-2X0/(+|rohPlUqV{
2021-09-10 09:33:46 UTC	164	IN	Data Raw: 11 5d 28 f9 ec 47 cc 29 e3 4c b9 89 c3 e1 67 7a 67 71 d6 f4 ca b0 dc f4 8e 5a 4b a2 69 08 f3 3c cb 36 32 19 60 2b c2 4b 07 70 58 60 37 35 14 5b 63 66 a8 03 e4 75 59 c6 e2 4c f5 d3 4e 99 5b 7f 4c ae 62 c3 80 52 3e c2 12 0b aa c4 31 0c cd cf d2 d9 c0 f6 a3 85 87 16 ad ab 65 2a 9d 9a 9e 36 ec 5c 56 3c 5c 4a af 91 64 90 3f 4c ab 86 50 3c d5 51 3d 77 87 5b a0 55 dd 47 bb 0b 9d f3 86 a7 4b 40 43 93 98 34 a3 d5 f2 ec d2 b0 43 e9 ec 38 e6 d3 e3 61 31 2b 0a 14 40 e4 ee 43 19 0c a9 cf bb f6 92 05 d0 34 05 f4 0e 24 e0 98 92 35 0c 39 e9 f8 b6 bb ca 41 4a 85 2a d5 b1 67 ca bd fc 43 9b d0 72 c7 0c f9 51 7e a0 5c e8 a2 05 e1 b4 78 f2 8f b0 0a 36 1f 72 f0 eb e2 b8 e7 e6 ae 72 44 c2 a5 8a 1e ee 7b cb 28 b0 94 14 d4 c9 ea e3 32 69 e7 dd 20 c7 d4 be 9f c5 cd 96 7c 48 32 be Data Ascii:](G)LgzgqZKi<62`+KpX`75[cfuYLN[LbR>1e*6\V<\Jd?LP<Q=w[UGK@C4C8a1+@C4$59AJ*gCrQ~\x6rrD{(2i |H2
2021-09-10 09:33:46 UTC	165	IN	Data Raw: 6d be d1 7c dd 0b 05 6c 51 17 e7 a9 a2 61 18 73 02 a1 f2 f5 ef 58 9c c9 44 a3 52 f6 02 be 7d da 2b 67 d5 2d 0c 63 e4 41 98 be ed ed 36 34 8c 17 69 02 d8 04 71 c7 ed 22 81 e4 ff 00 1d 6c fe 95 c4 bc b0 14 7f 8b 51 ee 03 ff 00 71 91 fa bf 04 1c ea 68 48 de c7 67 a3 e5 e4 04 00 7a 0f d5 12 7a 43 5c 8a 59 03 36 3c c5 62 c8 8c 1a 0e 8e c5 77 9f 20 18 ef 75 70 49 1f c9 ea cf 8e e1 91 c6 48 c4 90 09 00 9f 09 2f 6b 52 bc ad a3 31 73 51 f4 de 38 f0 3c 41 94 b2 e9 16 27 63 52 e4 9a 8b de f4 76 8e 95 fa 1f d4 f0 cc 90 18 24 8e 68 25 48 26 59 51 c0 49 61 91 45 49 13 51 2b 2c 64 9b 51 c5 8a 27 9e 7e 7b c4 a1 a6 60 55 0b 96 d4 b5 1a dd be 51 f4 af a7 71 00 a5 f1 a5 44 8c 40 3b ea 6d 9b 58 e5 d2 2c 16 97 9c 92 c6 8c f2 24 cb 4d b5 57 68 76 0a 2b 74 81 68 2c 8d 7e 40 17 Data Ascii: m|lQasXDR}+g-cA64iq"lQqhHgzzC\Y6<bw upIH/kR1sQ8<A'cRv$h%H&YQIaEIQ+,dQ'~{`UQqD@;mX,$MWhv+ th,~@

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	165	IN	Data Raw: b4 5c 20 82 31 66 58 f2 1a 76 dd 61 93 a2 e7 ab 47 8f 1c 8c 65 8b 81 11 91 b7 98 9c 6e dd 18 3f b9 80 02 fe 40 e6 87 1d 56 99 64 b9 a8 35 b9 00 67 e7 ea 4e 75 87 a4 4d 21 22 58 af 89 cb 5c 0a 0d 1a da d6 db 45 81 fa 73 ad f6 32 04 b2 67 47 1c 92 48 10 e3 fb fb 6c 55 7d 9b 58 85 fd c9 cf b9 8d 78 20 70 45 1f 1b 28 3d 1d c8 36 df 7f 47 b5 3c af f8 3e 24 cb f0 17 16 67 a1 d0 01 bf 95 79 08 b7 9e 99 d4 5a 68 f1 cb 8b 8e 43 22 4a 4d 53 12 df a4 cb cd 8d ab 74 77 59 5a be 79 eb 37 3a 56 17 a0 7c 54 05 dd df d3 d7 2a 46 9b 86 e2 49 01 24 8a 81 7d 05 43 ef cb d5 e2 55 f2 67 8b 39 96 20 3b 64 89 77 2b 91 60 b1 dc ae 4d ed db ce e0 7c 0a fc 75 d0 80 c9 a6 61 f3 09 2e 2b 7a 65 4c ef 0e 09 84 b5 80 d4 0c b9 bf 75 d5 e0 ce 19 3b f0 7b e3 f7 88 d7 60 e0 6d 4e 15 ca f1 Data Ascii: \ 1fXvaGen?@Vd5gNuM!"X\Es2gGHlU}Xx pE(=6G<>$gyZhC"JMStwYZy7:V\|T*Fl$}CUg9 ;dw+`M|ua.+zeLu;{`mN
2021-09-10 09:33:46 UTC	167	IN	Data Raw: 3d 61 af 85 09 c6 41 0c 4c ca 8a bd c6 20 8a df fb 8f 04 31 da 78 1e 3c 7e 3a 59 63 0f 84 36 af 77 d9 fc ff 00 14 2e 54 d4 7f 20 5e 84 03 90 6d 33 6f 71 12 50 4e db fb 51 81 52 28 65 92 88 e0 8d ce a7 77 f2 3e 2a bf d7 a1 9a 8e 75 e6 1b 91 3e 55 8e 94 96 77 ae 7b f9 6f f1 a4 48 a2 ba fb 98 3b 52 b9 35 67 61 da 3c 12 68 ff 00 7f 83 ff 00 60 9b 9e 67 de 23 bb 7e 2a 73 2e 08 eb ec 69 ee 0d ec cd 2c ae ac 80 d2 04 5e 50 11 b7 73 78 bf e7 9b ff 00 bf 5c 89 a8 24 6d db 3b 6c 5a df 31 f9 e5 ed b0 05 ef 65 aa a8 5b 66 bf 23 8e 79 51 7c fe 3a f3 8b 3d 74 88 30 0f 40 18 da a3 2f 30 f9 5f a0 bc 7e 66 41 ed 2c b4 a4 20 7f d1 62 41 74 f3 4a a4 ed dd c1 f3 c9 e3 af 33 da 07 88 ff 00 d4 f6 e6 d5 fc 3f 9c 02 6a 59 e9 2e e8 e4 88 0b 56 3b 89 0a 42 81 f1 56 38 1c 1f f4 e8 Data Ascii: =aAL 1x<~:Yc6w.T ^m3oqPNQR(ew>*u>Uw{oH;R5ga<h`g#~*s.i,^Psx\$m;lZ1e[f#yQ|:=t0@/0_~fA, bAtJ3?jY.V;BV8
2021-09-10 09:33:46 UTC	168	IN	Data Raw: b2 bd a1 43 e4 29 a2 3c 88 48 56 24 82 f9 3b b6 5d 34 63 e5 99 89 71 48 62 c4 66 4f 30 2c 77 1e 62 f9 40 e4 58 b2 be a3 aa 69 e8 5a 56 cb c4 cb 5d c0 01 bf b2 c6 58 d4 1e 28 98 d0 30 e6 cf c1 ae 9b 54 c2 93 2c e6 f5 fd e9 6f c6 cb 24 39 9a 92 97 74 06 a1 26 d6 0e 2f 5a b7 ac 1a 7d 39 82 39 d7 4d 85 67 45 8b 1f ee f7 46 fb 89 64 69 37 ac 66 85 2d 92 41 66 34 00 3c f8 b4 b8 f5 5d 40 d5 7b df 22 dc f5 f3 89 f0 00 31 4e 1c 38 14 ec 6e f4 6c b3 3b 8e 4f 58 f3 ea 04 8f 37 3a 48 42 af 7b 1d f2 0e 2a c4 a0 84 c7 c8 de 92 29 35 67 75 06 35 c8 bb e4 13 d2 fc 32 9a 5b d4 32 83 bb 8d 6a e2 83 ad 21 d9 a4 58 d4 e9 7c b2 e4 34 a5 75 89 5f 40 c0 92 e2 67 e3 b4 b1 cf 30 c6 6e e5 02 3b 68 87 b6 77 37 3c ec e4 b0 a2 38 a3 c7 3e e2 d5 e3 94 4e a2 ad 45 1a 10 77 b8 f3 b4 17 Data Ascii: C)<HV$;]4cqHbfO0,wb@XiZV]X(0T,o$9t&/Z}99MgEFdi7f-Af4<]@{"1N8nl;OX7:HB{*)5gu52[2j!X|4u_@g 0n;hw7<8>NEw
2021-09-10 09:33:46 UTC	169	IN	Data Raw: c9 d6 87 71 9e 3d b9 13 45 04 9e 1d 65 0a ea e4 01 68 ea 18 6d 0a 40 a0 28 7e 23 36 59 50 47 fe ae d4 c9 87 57 c9 db ad 60 92 54 53 8d 34 cb 2c ab df 53 78 fb 2c 53 bb 4d 34 6e ab 03 c4 b2 64 31 00 ca 1e 37 05 94 48 7c 32 a9 1c 7f fa 6e 28 4b b2 4b b0 05 b5 af ec bd ab ca 0a b0 bc 05 48 35 da ec ec 6f 00 9e b8 d2 22 d6 30 b5 18 91 81 98 2b e4 c0 85 42 90 52 34 97 7a d9 f7 6f d8 c1 97 82 49 be 4f 57 3c 04 ff 00 b6 a0 09 a3 df 4d b9 10 40 8c ff 00 1b 28 ac 2f 1d ca 58 54 b5 98 72 f9 03 ac 54 2d 63 1e 44 78 a7 ed ed de 59 58 d5 6d 91 4d 01 e3 83 f2 7f 27 ad bf 09 31 05 0d 46 66 1c b9 74 f2 6a 46 1f 8c 92 04 ce 56 a3 f2 be b9 33 66 f5 2f 0f 0f a3 9f 53 4e 8b 99 8b a1 6b 53 7f c0 c9 29 4c 4c 9b dd 26 2b ca 08 a1 66 fb 4c e4 7b 49 01 6b c0 e3 aa 1f ad 7d 29 2b Data Ascii: q=Eehm@(~#6YPGW`TS4,Sx,SM4nd17H|2n(KKH5o"0+BR4zoIOW<M@(/XTrT-cDxYXmM'1FftjFV3f/SNkS)LL&+fL{Ik})+
2021-09-10 09:33:46 UTC	170	IN	Data Raw: 64 c4 83 b9 ee 34 ce d3 c4 6a bb 2b 65 8b 1e 06 f2 fb 7c 9b 23 cd 74 ce 24 59 06 c7 bb f7 4c e2 bc 4f 99 34 f8 f4 70 da 33 e4 35 e4 3e 1a fa 4e 8c 65 8d 26 9e 19 d9 4b 71 8e a1 d3 21 d9 86 d0 1e 45 24 94 a3 c0 24 0f f7 e9 55 4c 5a df 19 a0 ae 55 1e 5b 5b f5 1d 0a 48 25 22 85 26 c7 32 2f 5f 56 7c e9 0e 1d 17 d2 0e ca b2 4b 08 8d 51 14 2c 71 80 d5 4c 09 5a 6f 70 e0 80 cc 4e eb 04 74 ac d5 21 28 e9 73 9e 44 57 e7 a5 e2 72 f1 aa 60 04 51 83 b7 62 f7 6e a2 1a f8 1a 4c 58 d1 29 11 14 01 fb 4c 24 70 db 42 80 43 05 06 90 13 f9 e4 7f a0 aa d9 8a 27 0e 0b 07 b3 37 53 bf bd dc 3b 9c cb 48 5f 86 aa 34 b5 7b 3e 99 e7 13 bf 68 ea a1 54 3a 3c 80 29 aa f6 b2 9b 04 5f 34 c2 e8 0e 39 16 7c 74 bf 8b 15 6d 57 bf ab e7 fb de 0c 94 e0 3b 87 77 3c c5 28 dd 2b 5f 4d cc 4d 38 99 Data Ascii: d4j+e|#t$YLO4p35>Ne&Kq!E$$ULZU[[H%"&2/_V|KQ,qLZopNt!(sDWr`QbnLX)L$pBC'7S;H_4{>hT:<)_49|tmW;w<(+_MM8
2021-09-10 09:33:46 UTC	172	IN	Data Raw: 10 55 ad e4 a9 cd c3 52 c0 ea cf a0 de 13 da 0e 0c 47 d4 f3 e4 33 ec 8e 3d 71 e0 98 1f 2a 72 08 8d 0b 7c 98 df bf 61 be 00 16 7a b8 e2 14 af b6 91 46 37 3e 6d 9e b5 be c6 2a 38 74 ba d6 74 fc c6 0f 5d e3 e4 6a df 69 0c b0 c6 8f 8e 24 2b b2 fd c6 39 4c 12 3b ad 7e e2 50 02 6b 91 47 93 d1 b8 55 e1 c2 32 a6 d6 00 e6 f4 e5 a0 c8 40 38 b9 78 ea 2f 71 96 c0 77 fb 88 bf 49 6a 59 9a 44 da 32 46 bf 70 d9 7a 84 b1 cb 8c 0b ad e1 82 61 92 3d ea 77 7b 50 17 8f c7 b9 45 9a b2 3d c5 a0 cd 54 e1 a8 6c a8 f5 e7 53 e4 34 89 f0 49 54 b9 bf f2 0a 92 32 66 02 be bc ac da 88 75 6b 70 26 52 7d ce 03 46 59 b1 26 3a 79 94 fb 65 47 06 39 95 88 37 de 89 d6 c0 7b f7 31 52 39 e6 9b 86 25 0b c2 ab 05 30 19 76 dc be 4d bf 18 9f bd 2c 29 19 87 7b be 8d eb d6 16 fe 9b c9 fb 3d 57 1e 5c Data Ascii: URG3=q*r|azF7>m*8tt]ji$+9L;~PkGU2@8x/qwIjYD2Fpza=w{PE=TlS4IT2fukp&R}FY&:yeG97{1R9%0vM,){=W\
2021-09-10 09:33:46 UTC	173	IN	Data Raw: 06 c0 90 18 ed 6a 13 5d 1b 36 a1 5f a8 e0 93 5c 83 3b 1a 77 4b 88 64 45 89 24 c0 52 d4 cc bb 0b 37 25 64 42 36 95 35 bb c8 3f 15 b2 e6 14 4d c6 12 00 2a b0 a0 6a dd bd 29 47 d6 2d 54 82 b9 75 b5 aa 4f 27 6a 53 d4 45 7c d0 f4 79 b4 bd 63 5d 94 cf 69 f6 59 50 c0 05 58 01 49 c9 82 46 f1 b5 55 77 2b 01 44 35 79 ea f2 62 f1 4b 97 84 b1 25 36 3a 9f dd 9f 9d e2 97 87 97 f6 a6 cd 26 cc 47 9d f3 31 05 96 17 ed 26 85 77 14 d9 dc 86 aa b9 6d ac 78 ff 00 2d 57 cf 8f 3f c3 02 99 76 db 7e a2 0b 26 6b 06 60 9b 52 b4 77 3c cb ef 13 fa 26 a6 34 cc cf 4e bb ac 89 85 94 92 e9 39 d2 c6 03 1f b6 cd 56 8f 79 52 76 ec 49 59 0b 93 ca a8 dd 5c 71 e2 84 a8 12 f5 14 6a bb 6b a5 f9 da 97 78 80 59 94 a7 4d 46 6c 4d fe 69 71 b6 70 48 b8 a9 a7 7a 93 2b 19 d9 55 a4 c4 97 0e 64 42 c1 5a Data Ascii: j]6_\;wKdE$R7%dB65?M*j)G-TuO'jSE|yc]iYPXIFUw+D5ybK%6:&G1&wmx-W?v~&k`Rw<&4N9VyRvIY\qjkxYMFlMiqpHz+UdBZ
2021-09-10 09:33:46 UTC	174	IN	Data Raw: 7a d1 a8 63 2b 7f 4c 5f 5a 70 e7 0b a5 7d 43 c8 9f 15 82 c8 8d 95 18 2d 4f ff 00 32 d0 46 0c 6a 57 e6 cf 27 af 1e 25 00 1f f9 0d bc b7 a6 5f 83 04 4c ee 25 4d fc 87 9d 79 17 6f c6 90 4f a3 fd 09 fa 89 82 18 6a d9 79 53 bb ec 8a 6c ac 47 28 b9 0c ac 76 ef 25 7f 4a c9 dc 6a bd de 49 e7 a5 97 c6 84 78 82 ea 6e e7 96 f0 60 27 a8 39 2a 17 6f 17 b7 36 ee a2 1a fa 47 d0 2d 6d 9d 0e 46 a9 ab a6 c8 bf 56 11 2b 77 18 11 ca 07 db 45 45 dd a9 24 8f e3 a0 2b ea 20 53 f9 1b 64 6b bb fb fa c4 07 0f 35 46 aa 51 07 9b 0b 74 dd af 0d 8d 0b e9 34 f8 8c 23 78 a6 c8 55 11 17 92 62 5e 40 63 5a f6 ee 3e dd ca 69 cd 59 f8 e0 74 ac ce 39 4a 76 0c 3c 87 b7 f7 48 2c be 0f fc 8a 5c 83 98 bf ce 79 69 ab 3b cb 45 fa 63 87 b2 27 8f 10 6d 0a a7 f4 c3 ee a3 4e e1 9d 89 db ca d5 00 45 5d Data Ascii: zc+L_Zp}C-O2FjW'%_L%MyoOjySlG(v%JjIxn`'9*o6G-mFV+wEE$+ Sdk5FQt4#xUb^@cZ>iYt9Jv<H,\yi;Ec'mNE]
2021-09-10 09:33:46 UTC	175	IN	Data Raw: 8b 30 ce 34 fc 24 b2 38 69 2a 14 07 0d 35 a8 2f 9d 9f 9e 77 bd 8f f5 72 64 69 be 94 8f 63 a4 38 08 db 0a 6d dc 4a e0 2c 42 51 2b 8f 70 2a d1 f8 f1 45 6c 59 1d 66 b8 60 15 c7 8a 3b fa ba bf ba 56 8f ce 34 5c 41 3f ed 2a 75 b9 a3 d2 2b d4 58 93 1d 09 67 15 14 9a ce a8 73 e9 24 24 8c 58 a5 8e 08 77 5f 2b dc 95 c9 14 00 25 58 5d 0e 74 e0 83 34 81 fc 42 48 21 83 13 60 f4 ad 2a e6 b7 b4 66 38 84 82 a4 30 b8 05 f5 34 3d 6f 5b ea 21 d5 93 84 cb e9 cd 6b 5b c7 96 35 74 d5 b1 30 fd c3 95 92 09 3b 6c b1 d7 e5 60 1b da 88 16 4f 17 d5 3a 96 0c f5 16 0c fb 35 28 36 b9 77 d2 2c a5 20 fd 84 30 6b bd c0 cd ed 48 83 fa 86 23 d3 f4 0f 4a 4f 32 37 78 e9 4d fa 71 86 31 c4 99 19 93 3b 17 07 95 0c 40 54 22 b7 5d 8e 05 74 59 4a c6 a5 83 9b 61 7a ed 9f 3b d5 9b 4b 4a 72 42 52 85 Data Ascii: 04$8i*5/wrdic8mJ,BQ+p*ElYf`;V4\A?*u+Xgs$$Xw_+%X]t4BH!`*f804=o[!k[5t0;l`O:5(6w, 0kH#JO27xMq1;@T"]tYJaz;KJrBR

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	177	IN	Data Raw: ad 06 89 a9 4b 2b ef 37 f7 13 ce 92 46 2e 80 05 79 50 07 e3 8e 83 80 ab f9 28 1c a9 9e d4 23 e7 f0 d2 52 a4 24 a5 20 61 2e e3 f7 7a e5 f1 13 b3 69 66 6f 4a 68 39 52 5c cd 0e 17 d9 d8 2a 79 8d 81 db 55 6c 6c 86 24 02 47 17 fc 85 69 69 80 07 c8 bf 51 ab e5 d3 d2 1b 41 05 03 b6 cf e4 41 fe 0c 31 c3 e9 dd 1f bd 46 5b cd c8 90 b0 a6 5d e9 b0 0d 8d 61 ab 68 b2 36 8f 9a f8 e8 6a a9 2f af b5 a0 a9 0e 01 49 66 00 54 3b 96 b8 73 4b 8d ef 0e bf 46 e9 2c 7d 35 aa 6a 13 4f fa 6b a4 65 ed 89 77 0d 8f 22 f7 b8 3e 54 88 54 02 2f 68 e4 8f 3d 56 71 0a c3 36 5a 52 7f 91 18 80 3c 9e ee 5b cb d2 19 95 2d 4d 34 ae b8 53 43 66 2d 90 14 37 a8 7c eb bd 6b 8d 62 ce c5 f5 0e 72 7b 8f f8 6c 6d b9 5c 02 23 97 3d 14 29 26 ff 00 79 01 43 df 1c df c7 4e 2d 45 d0 9c b0 d4 6e 05 fb a1 0d Data Ascii: K+7F.yP(#R$ a.zifoJh9R*yUll$GiiQAA1F[]ah6j/IfT;sKF,}5jOkew">TT/h=Vq6ZR<[-M4SCf-7|kbr{lm\#=)&yCN-En
2021-09-10 09:33:46 UTC	178	IN	Data Raw: 7f c6 6d 0c a4 29 65 9f 66 a0 cb 3b 53 de b0 43 8f 24 59 66 2e ea 09 59 e3 88 29 89 aa bd d4 bc 1f c3 1b 90 d7 fb d7 42 47 dc 0a 63 67 14 b8 02 fa 67 eb e9 0d cb e1 d6 03 a5 4c 0d c5 0d 8d 6f 51 50 7a c7 cc 9d 0e 39 23 ee 34 6c d7 1b b6 ca 05 94 d9 5d e5 79 21 7e 01 fd d4 c3 f3 c9 de a3 11 d0 69 9f 7b c3 09 92 00 3a be a4 3f 7e e3 ca 4f 13 d3 6b 3a 62 44 61 29 ed 2d b4 a3 3a 33 6d dc ad b4 0f 62 a0 fd cd f9 aa e3 a2 ae 67 85 21 17 7a b3 5a ce 68 ff 00 9d ee 3a 99 2e 54 e9 25 2c dc 9f 96 d6 3c e2 67 4b f4 52 cd f7 95 8c c8 c5 95 77 76 08 12 12 d4 a4 48 58 aa c7 74 39 50 7f 15 e7 a5 d5 35 4a 21 25 5e 1b 17 cf 46 3f 8b fa c4 91 c3 78 82 52 92 06 64 8e 67 37 3a f5 82 b8 7e 9d 44 8b 19 8e 07 64 95 d2 1c a2 54 95 12 1b 00 29 dd c8 56 ab 35 c1 1e 7f 03 33 0a 4f Data Ascii: m)ef;SC$Yf.Y)BGcggLoQPz9#4l]y!~i{:?~Ok:bDa)-:3mbg!zZh:.T%,<gKRwvHXt9P5J!%^F?xRdg7:~DdT)V53O
2021-09-10 09:33:46 UTC	179	IN	Data Raw: 48 03 81 c0 37 44 dd 70 7f 4f 5a 9c ac 16 c8 3f 6c 3f 7a c6 6f ea 9c 78 47 85 2b 71 66 0c fe 6d ae 63 4a e5 1c a2 fa cd eb ed 67 d7 3a 9c d3 65 bc c3 1f 1d 8a c3 0f ed db 6c 08 6d a8 d5 2c 53 0a da 18 06 17 7c f5 b0 e0 38 54 49 4b d2 cc dc b7 ed e3 e7 bf 51 e2 15 3d 65 9c 02 7e 4f 7b c5 57 d7 34 8f ba 6c 64 2b ee 5b 67 02 3d 8e ed 4e ec 09 b6 bd 84 22 80 6b 83 5d 5f f0 f3 12 90 30 9b 8f d6 ba bb b6 db c5 34 e1 84 90 da 6e d4 1a fa 7a 18 5e 6b 3a 2a 4f 9b 89 a6 e3 46 d3 66 65 81 8e a8 b7 ed 77 60 ac c4 00 49 65 2d ed e2 bf bf 56 12 a6 04 62 98 ec c9 77 a1 0e d9 57 93 8a 53 3b 83 4d c4 4b 33 95 2d 38 5c 95 55 a8 c1 ea ed a5 5e af e4 22 ce 7a d2 08 fd 2d e8 5f 4d 7d 3d c3 d8 19 57 13 2f 53 60 e8 49 65 4f b8 cb de a0 82 c4 00 aa 43 82 db 8a 8f 17 d5 47 0f 34 Data Ascii: H7DpOZ?l?zoxG+qfmcJg:elm,S|8TIKQ=e~O{W4ld+[g=N"k]_04nz^k:*OFfew`Ie-VbwWS;MK3-8\U^"z-_M}=W/S`IeOCG4
2021-09-10 09:33:46 UTC	181	IN	Data Raw: cc 03 48 dc 9e 1f 8a 06 ba 92 26 15 64 e4 3f c6 83 f7 f3 09 d2 d0 b5 50 1b b8 62 5d 80 6a 88 ec ab 4c 56 30 c1 bd af b8 55 8f 6b 01 f8 23 c1 24 78 e3 ad 91 99 5a 36 cf 78 f9 d2 bf 89 3c bc df f5 18 04 e6 b7 55 90 28 f2 3f 07 c9 ff 00 4e bc 56 4d 1b 6b f2 fd c0 63 04 53 2b 33 48 ec a7 7b 50 5a da 01 5e 3f 75 9f 1c 73 ff 00 d3 a8 a5 45 21 87 3a f7 9c 75 25 8d 03 98 c1 24 89 8f 2e 54 cd 6b 70 9f d4 b0 41 e0 d0 66 fc fc 0b ae 3f 9e a0 28 92 59 ae 5b e2 0d 2c e2 2c 68 da 50 e6 4f 77 f6 8a 73 eb 7c 95 81 f2 86 d9 36 ca f9 33 6e 60 09 12 24 f1 90 77 f2 6c fb 94 d7 1b 6c f8 f2 ac c5 95 13 fe 35 15 17 61 cc 75 cb 2e 70 c9 a8 01 ed 9f 57 ab 36 bd de 13 da 2c 91 9d 6b 27 35 e7 28 cf 0c 92 c7 ee b5 ee 22 d2 02 7f cc b7 cd 0f 06 ee 8f 51 52 d2 95 24 1a b8 2c 4e c6 9e Data Ascii: H&d?Pb]jLV0Uk#$xZ6x<U(?NVMkcS+3H{PZ^?usE!:u%$.TkpAf?(Y[,,hPOws|63n`$wll5au.pW6,k'5("QR$,N
2021-09-10 09:33:46 UTC	182	IN	Data Raw: af 09 70 4f 76 3d 1b de 29 04 b0 a4 24 12 43 3f b9 fc c4 c6 81 ad e7 68 5a 8e 2e a7 a7 cf 24 19 38 87 70 64 34 19 54 ab 34 6c 7c 94 75 07 70 15 63 8f 8e 94 e2 e4 27 8a 94 b9 6b 03 c7 47 cc 12 18 1e 96 ab d1 fa 33 c3 71 2b e0 a7 21 68 3e 10 52 e9 25 83 3b 1d 5b fa d2 3a 03 f4 c3 ea 76 37 a8 b0 a0 9a 39 7f e3 20 55 6c bc 31 cb 7b 8d 17 52 78 2b c1 20 af 2a 38 3e 39 f9 ff 00 1d f4 e5 f0 d3 30 28 28 24 13 85 6d fc b5 db 7f 28 fa 7f d3 7e a2 9e 2a 4c b2 92 eb 61 89 24 b0 48 d1 ee 5c d2 b4 d2 91 6a bd 3b ea 94 98 aa ab ad a6 cb 43 5e e5 20 30 00 12 19 4f ce e1 cd fc 75 43 3f 87 b9 4e 2c ae 3b f8 f9 8d 2c b5 f8 45 43 90 29 de d4 f9 78 b6 9f 4d 3d 6a b1 c9 0c 6e fb 95 94 6e 56 60 76 00 39 0c 4d 6e bf 81 f9 fc f5 4b c5 c8 c6 08 a8 2c 6d 5c a9 b8 70 2b d2 2e f8 49 Data Ascii: pOv=)$C?hZ.$8pd4T4l\|upc'kG3q+!h>R%;[:v79 Ul1{Rx+ *8>90(($m(~*La$H\j;C^ 0OuC?N,;,EC)xM=jn nV`v9MnK,m\p+.I
2021-09-10 09:33:46 UTC	183	IN	Data Raw: e7 bd 69 bf 38 00 d7 32 5c 65 54 8e ad 12 39 91 69 82 15 fc 46 c0 80 4f c1 bf c7 f3 d2 eb 96 49 7a f8 6d 43 5a dd fa f2 d6 8c c2 05 8b c2 cf d4 ba b4 51 c4 aa b2 a2 97 25 84 7b 8f 80 47 1b 45 32 ad 9e 4f ff 00 2a e8 fc 22 59 4a c5 9f 2a 30 b0 36 bc 41 65 64 95 06 02 9d 28 75 e5 f8 ce 14 fa 96 ac d1 09 37 cc a1 99 82 28 56 a5 50 ff 00 f4 9a 04 d7 21 99 7e 3f 9b eb 86 50 c4 a2 c0 78 9d d9 c9 de ba ff 00 59 40 c4 d2 09 04 87 c9 9c 53 fb 16 78 54 7a 8b d4 f2 46 db 44 c3 ee 25 66 0c 8c c1 51 58 9d bb ad 47 2b b4 02 17 93 43 9e 6e e5 2c 10 a0 e5 c3 86 d9 af e7 b0 e7 ac 20 b9 ea 33 14 30 03 bb 9a 6d 7f c8 f9 4f 7a 97 d4 51 61 c6 56 4c d0 ce ca c5 dc be d5 dc 3c 46 dc 1d a8 7c 81 43 c0 17 c5 f5 60 53 88 61 01 ed 7a e7 53 97 3e 50 13 3f 0f 8c 80 1b 76 ef bd 22 a5 Data Ascii: i82\eT9iFOIzmCZQ%{GE2O*"YJ*06Aed(u7(VP!~?PxY@SxTzFD%fQXG+Cn, 30mOzQaVL<F|C`SazS>P?v"
2021-09-10 09:33:46 UTC	184	IN	Data Raw: e0 91 b5 8c 91 cf e2 e9 89 d9 28 06 ff 00 e9 24 13 e4 75 25 ac 39 21 46 ac 58 6e 1c e6 79 57 ce 22 99 58 cb e0 14 39 1a d3 41 6d ea cf 78 65 63 61 cc b8 78 8f b7 15 b2 4c 52 48 92 ee 1b 5b 1a 25 fb 69 a1 7e 06 e9 a1 28 e0 c7 fb b6 95 26 fa aa 9e 14 54 ce e1 45 ce a1 98 d3 cc f9 65 0f cb 04 a1 94 00 c3 6d de b9 e9 a0 cc c6 d0 9d 66 c5 d5 b1 f0 e2 1d 8f b2 cb 85 a3 ae e2 f6 e3 c7 8d 15 c3 1b a2 c3 73 0f 8a 1f c7 56 52 cb a6 5b 96 a0 43 de e7 3d fc a1 39 ce 92 4b 50 28 0f 7a fb 5f 66 80 9d 1c 47 97 e9 a4 8a 08 8a 98 23 0c 66 de 48 ed 08 a4 c7 2c 7c 00 50 8d c0 9f 85 37 c8 1d 31 2f c1 38 cb 55 43 31 a5 4e 9b 56 e7 ab 40 56 91 31 04 87 0c 9a b6 45 ff 00 62 bf dc 32 f4 bd 7a 1d 5b 48 d1 06 44 82 17 86 37 d2 33 f2 4b 53 6d c4 60 23 99 80 a7 da 52 5b de d6 08 f1 Data Ascii: ($u%9!FXnyW"X9AmxecaxLRH[%i~(&TEemfsVR[C=9KP(z_fG#fH,|P71/8UC1NV@V1Eb2z[HD73KSm`#R[
2021-09-10 09:33:46 UTC	186	IN	Data Raw: 62 f1 ac cd 67 85 8e 51 db 3b 08 34 ca ca 85 85 78 1c 9e 4d 75 e4 2f 12 8e 1d 2b 9d 41 be 7b 75 cc 08 e2 c1 09 65 7f 20 7a 0e fd cf 91 8f a5 55 17 32 08 0a a6 fd 73 4a 93 09 05 fe 99 c9 ed bc f1 b3 16 34 19 64 c7 20 0f cb 0e 7c 0e 85 35 4c 4b be 43 d0 9a da b0 69 48 c4 82 c4 0b 33 f9 8f 53 f8 83 1d 3b 1e 5c 8d 3b 23 1e 45 58 be f3 4c ce 8e 02 4e e5 19 11 33 37 2b 5c 78 aa a2 7e 3a 4c ad 26 61 b8 74 a9 22 d7 14 ed b3 87 65 82 94 b3 3b 37 2a 7c ed ad 72 8f 31 c3 f7 ba 7e 21 98 a0 95 21 86 66 90 2e e0 86 12 1f 9f 1b 40 28 47 e7 8f 17 d5 6a 54 53 3a 62 0a 9e 84 8c 39 d4 e6 7d de bb 52 2c 8a 01 e1 c4 ca 31 0c 06 75 7b 8b 5b 78 5f fd 57 d2 d8 ea 39 ab 84 c8 b8 f9 78 b8 59 c8 ac 02 a1 6c 9c 6b 90 86 6f 87 96 30 58 f3 b8 13 60 75 a3 fa 64 e7 61 98 cb 4b 50 fa 3d Data Ascii: bgQ;4xMu/+A{ue zU2sJ4d |5LKCiH3S;\;#EXLN37+\x~:L&at"e;7*|r1~!!f.@(GjTS:b9}R,1u{[x_W9xYlk o0X`udaKP=
2021-09-10 09:33:46 UTC	187	IN	Data Raw: 9d ac 1c b1 b2 c0 9d 8a 0d 8f 92 84 c2 92 4a 40 2e 34 d7 f1 b4 32 b9 09 52 13 89 24 db 2f 2f 33 53 eb 1a cb ec c7 9d a6 ac 87 52 8d b9 58 90 17 9e d0 50 2c 3d 91 b8 a8 02 f6 db 1a e7 a5 d4 09 14 82 4d 93 89 b0 50 e1 66 57 a5 1b f2 fc e2 1d d9 66 de fb d4 c8 84 5a 48 0e d9 0f c8 6f 01 02 f8 3e 2c 1f 1d 0c a0 80 4b 8e cc 2a a4 99 64 25 44 28 e4 52 43 76 33 11 94 e7 c7 ed dc 12 24 44 05 c2 f0 d2 c8 06 c5 0a 1b 80 3c 73 e4 f1 d0 94 c5 4c 41 7d 9b 9e bf 8f 68 28 90 b6 77 4d 79 fe 28 de ed b4 6b c3 90 ad 10 72 aa c5 da d8 58 dd 19 05 bc 58 f6 f8 3f ef fc 0e bb 85 3a 5f af ef 9c 09 7e 02 c4 87 da b4 fc 76 62 27 36 7d b6 ce 14 42 a0 b0 db 22 aa 87 23 8b 27 f0 6a cf fa f5 10 9c 05 d2 c0 69 6e 9f 88 0a 91 42 c6 f9 0c 88 76 b3 9a 1a 53 e2 07 db 37 1e cb 97 85 d0 31 Data Ascii: J@.42R$//3SRXP,=MPfWfZHo>,K*d%D(RCv3$D<sLA}h(wMy(krXX?:_~vb'6}B"#'jinBvS71
2021-09-10 09:33:46 UTC	188	IN	Data Raw: 48 4a 48 2e 6a 46 86 da f5 e6 d0 29 28 c3 8d 4a 0f 8a b4 ab 0a b5 d9 ba 73 30 17 e9 fd 2d 63 f5 67 ac 63 31 c8 22 9b d3 d9 59 85 67 49 63 6e f4 ac 32 9b b6 ef 6b 71 31 45 75 e3 e0 fc 8e a5 c4 3a e4 4a 52 48 04 10 92 f5 7a 17 0f 9d 9d d8 e5 91 8e c9 48 54 f5 30 64 e1 76 55 dc 1c 9b 36 39 b8 b4 65 d6 b4 f8 f5 0d 63 4a 8a 45 0d 1e 5e 0c e8 02 8b 3b e5 85 24 2e 11 00 0d b7 6d 1b 35 46 cf 27 a2 f0 aa 98 d4 b3 31 6d 76 e7 9c 7b 8b c2 0d 39 7b 3b f7 93 44 e7 ad 35 59 63 d3 7e 9f 6a 38 58 ae 71 a1 f4 ee 38 d5 32 59 cb 15 93 33 22 47 cc 56 00 5b c9 2b cd 23 b9 71 e1 57 c9 eb c2 51 33 09 5a 81 15 a5 ce 47 4a d9 cd cb 86 6a bc 0d 33 82 10 05 58 d2 95 d7 b2 62 07 48 f4 fa cd 87 ea 18 3e dc a0 38 59 59 b1 db 80 08 82 68 a5 8e 48 c3 54 46 55 8d 0b 01 7d cd 84 ad f0 3a Data Ascii: HJH.jF)(Js0-cgc1"YgIcn2kq1Eu:JRHzHT0dvU69ecJE^;$.m5F'1mv{9{;D5Yc~j8Xq82Y3"GV[+#qWQ3ZGJj3 XbH>8YYhHTFU}:

Timestamp	kBytes transferred	Direction	Data
2021-09-10 09:33:46 UTC	189	IN	Data Raw: 00 ee 3c 8e 00 eb a8 47 fc 84 bf 80 a8 39 d1 b2 1b 72 bf 48 5a 7a ca 90 90 f5 42 14 08 ea 39 77 e7 15 27 d0 d3 ce 9e b0 f5 ae 66 a0 d2 d4 99 e9 12 d1 f6 47 dd 94 08 9c b7 96 f8 1b 4d 07 37 cf cf 5a 75 ca 2a 12 3e da 5c 78 4e 94 a9 22 a7 2a 53 f0 5b 2d 2f 12 0c e3 b9 0e 4f 23 9d 7d 2b 6d a2 33 17 52 7c 94 fa 90 a6 3f ba 8f 22 58 22 91 5d 01 ee 34 b9 27 19 5d 49 a2 22 4f 69 61 5e d3 c8 fc f4 ca e5 84 84 e4 a0 1d b5 36 a9 0f e7 5d 0d 2f 04 4d 24 aa c5 f4 e7 43 95 77 07 20 c2 ad 0f e9 e0 fb 9f a4 7e 90 58 ca ee 87 47 d5 b0 56 32 c2 c4 ab 2e eb 23 f0 7c 2d 1a 1c dd 75 8e 13 d5 2b ea 0a 41 4d d4 70 d9 8f 7b b5 fc b5 88 97 f7 38 34 b2 98 e8 2c d7 a3 6a e3 a4 57 2d 61 9e 1c 9f 48 e1 e1 21 51 95 24 4f 2b a9 27 66 4c 40 34 b1 b0 07 85 75 52 7e 78 e3 f8 eb 41 c3 14 Data Ascii: <G9rHZzB9w'fGM7Zu*>\xN"*S[-/O#}+m3R|?"X"]4']I"Oia^6]/M$Cw ~XGV2.#\|-u+AMp{84,jW-aH!Q$O+'f L@4uR~xA
2021-09-10 09:33:46 UTC	191	IN	Data Raw: 66 23 74 8a 78 b1 b9 43 06 11 aa 5d f8 5f d4 6f 1b 05 72 6f ae a5 09 49 25 81 24 5e d5 b3 e7 f3 72 cd 17 89 9a e8 c3 85 e9 b0 a1 cc 9c b6 0d d4 43 0f 49 99 5f bb 2e f2 cc 36 ad 50 ed 86 2a 14 ec 52 4e c5 1b 40 51 64 9b be 0d f5 dd 2a 3e 4f 5f d4 01 86 9e 75 83 1c 04 89 80 95 9f 64 b1 82 d1 87 56 91 2c 8a 34 8b fb 79 36 6a b9 f9 ea 4c 82 9a 9a dc 06 cc 58 58 ff 00 51 29 93 7c 00 03 40 c0 b9 a3 8a 1d 29 46 68 31 d2 b5 34 21 dc 4e ae b0 2f ea 05 3b 19 e2 46 40 7b 41 cd 89 0d 9f f4 14 3a 9c 9c ce 4e ef 42 18 33 f4 19 f5 2c 2b 0b cf 92 00 0a 34 c4 c0 6e f5 bf 4c fc c8 86 9e 0c a3 50 8d 8c 6f 06 3a 4d 84 f0 47 24 4a 64 9b 0e 31 3a 4b 3e 46 c0 ea 1e 63 12 f6 44 96 0a 17 b1 f9 ea c2 49 13 10 54 92 e0 12 09 d3 be c4 55 2f c2 bc 27 f9 50 e1 7b 81 7b 53 4d 7c a3 36 Data Ascii: f#txC]_oroI%$^rCI_.6P*RN@Qd*>O_udV,4y6jLXXQ)\|@)Fh14!N/;F@{A:NB3,+4nLPo:MG$Jd1:K>FcDITU/' P{{SM|6
2021-09-10 09:33:46 UTC	192	IN	Data Raw: ed 05 b2 c4 43 7c 2b 2e 26 0c 6c c2 34 ef 65 24 6b 3c a0 b7 04 a4 22 95 aa c1 b1 d6 ae 59 1f 75 22 ec fb e6 3a fc d6 32 13 94 4f 89 41 99 47 a9 63 93 6d fb 8d 3f 43 46 9a 76 26 50 85 03 cd 9b 19 fb 86 53 64 92 01 0c 8e 3d c5 63 5a 0c 3c 1b bf 3e 3d c6 1c 4c 3f c4 0b de c5 d8 65 99 e7 78 f7 d3 92 0a e6 63 ff 00 23 e1 b3 9e 5d 3f 23 58 b5 1e 96 c5 87 03 07 5a c9 2f 24 b0 a6 83 85 8b 28 85 f8 11 77 22 92 54 11 0a 0c ec 58 2d 9e 5e eb c7 3d 66 56 8c 4b 5e 22 cd 88 87 7b 07 66 67 15 a4 6a 64 1c 0d 84 68 1e c0 97 cf 99 a5 2d b4 11 7a fd e1 c8 f4 ae 3e 7b 4a 02 64 66 e9 c6 3f 96 9a 49 93 67 db 85 a2 09 bf d3 62 2a a8 5f 22 fa 5f e9 e1 42 64 c2 68 14 48 15 ff 00 e2 df 22 0d f5 39 aa 32 90 c9 fe 2c 09 d2 94 cf fa e8 c4 6b e9 f6 4a 45 0e 16 54 f1 2a c3 0e af 88 98 Data Ascii: C|+.&l4e$k<"Yu":2OAGcm?CFv&PSd=cZ<>=L?exc#]?#XZ/$(w"TX-^=fVK^"{fgjdh-z>{Jdf?lgb*_"_BdhH" 92,kJET*

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2880 Parent PID: 5176

General

Start time:	11:33:26
Start date:	10/09/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll'
Imagebase:	0xc80000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391622099.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391468389.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391668872.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391496685.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391695930.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391358945.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.525372552.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391423871.0000000003138000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.391520743.0000000003138000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3428 Parent PID: 2880

General

Start time:	11:33:27
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 3556 Parent PID: 2880

General

Start time:	11:33:27
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\MGrYFpGLQ7.dll
Imagebase:	0xc40000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311865061.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311769510.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311540194.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311670564.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311984449.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.312268208.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311633818.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.311573394.0000000005538000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.527384744.0000000005538000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5040 Parent PID: 3428

General

Start time:	11:33:27
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\MGrYFpGLQ7.dll',#1
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313451317.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.314268795.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313872965.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.314181933.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313395188.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.526965041.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313701626.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313576458.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.314078107.0000000004C88000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: iexplore.exe PID: 4728 Parent PID: 2880

General

Start time:	11:33:28
Start date:	10/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff648b30000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Registry Activities | Show Windows behavior

Analysis Process: rundll32.exe PID: 2624 Parent PID: 2880

General

Start time:	11:33:28
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Bighearted
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.311422020.0000000006CB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 2576 Parent PID: 4728

General

Start time:	11:33:29
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17410 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5352 Parent PID: 2880

General

Start time:	11:33:32
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Soaking
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311090164.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311152381.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311345831.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311203958.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311364814.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311042721.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.311282599.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.310694636.00000000070D8000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6276 Parent PID: 2880

General

Start time:	11:33:36
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Turnipy
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000002.328237107.0000000005588000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 6320 Parent PID: 4728

General

Start time:	11:33:36
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82952 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6424 Parent PID: 4728

General

Start time:	11:33:38
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:17414 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6432 Parent PID: 4728

General

Start time:	11:33:38
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82954 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6536 Parent PID: 2880

General

Start time:	11:33:40
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Watertight
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314377890.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314521084.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314475815.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314245766.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314318653.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.313929901.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314563024.0000000006878000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000010.00000003.314146839.0000000006878000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6708 Parent PID: 2880

General

Start time:	11:33:44
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Dithery
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000002.346412042.0000000006C48000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7000 Parent PID: 2880

General

Start time:	11:33:48
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Anhimae
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355232631.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355592572.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355040596.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355268021.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355464241.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355144752.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.354973566.0000000007528000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000015.00000003.355518422.0000000007528000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 7140 Parent PID: 4728

General

Start time:	11:33:50
Start date:	10/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4728 CREDAT:82976 /prefetch:2
Imagebase:	0xe90000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1496 Parent PID: 2880

General

Start time:	11:33:52
Start date:	10/09/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\MGrYFpGLQ7.dll,Anostraca
Imagebase:	0xba0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001B.00000002.361195316.00000000074A8000.00000004.00000040.sdmp, Author: Joe Security

Disassembly

Code Analysis