



ID: 452723
Cookbook: browseurl.jbs
Time: 18:59:34
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 4
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 40
No static file info 40
Network Behavior 40
Network Port Distribution 40
TCP Packets 40
UDP Packets 40
DNS Queries 40
DNS Answers 41
HTTPS Packets 47
Code Manipulations 49
Statistics 49
Behavior 49
System Behavior 49
Analysis Process: chrome.exe PID: 3500 Parent PID: 4672 49
General 49
File Activities 50
Registry Activities 50
Analysis Process: chrome.exe PID: 4588 Parent PID: 3500 50
General 50
File Activities 50
Registry Activities 50
Analysis Process: chrome.exe PID: 6532 Parent PID: 3500 50
General 50
Analysis Process: chrome.exe PID: 3708 Parent PID: 3500 51
General 51
File Activities 51
Registry Activities 51
Disassembly 51

Copyright Joe Security LLC 2021

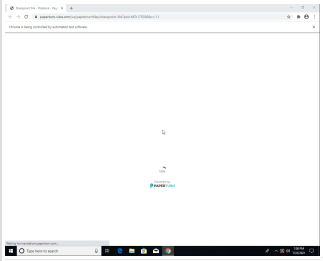
Windows Analysis Report https://www.paperturn-view.c…

Overview

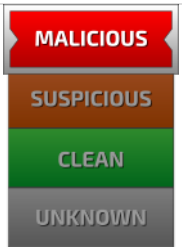
General Information

Sample URL:	http://https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1
Analysis ID:	452723
Infos:	

Most interesting Screenshot:



Detection



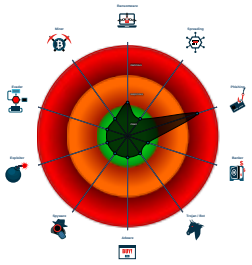
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Submit button contains javascript call
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3500 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4588 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6532 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4612 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3708 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=3848 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:



Yara detected HtmlPhish10

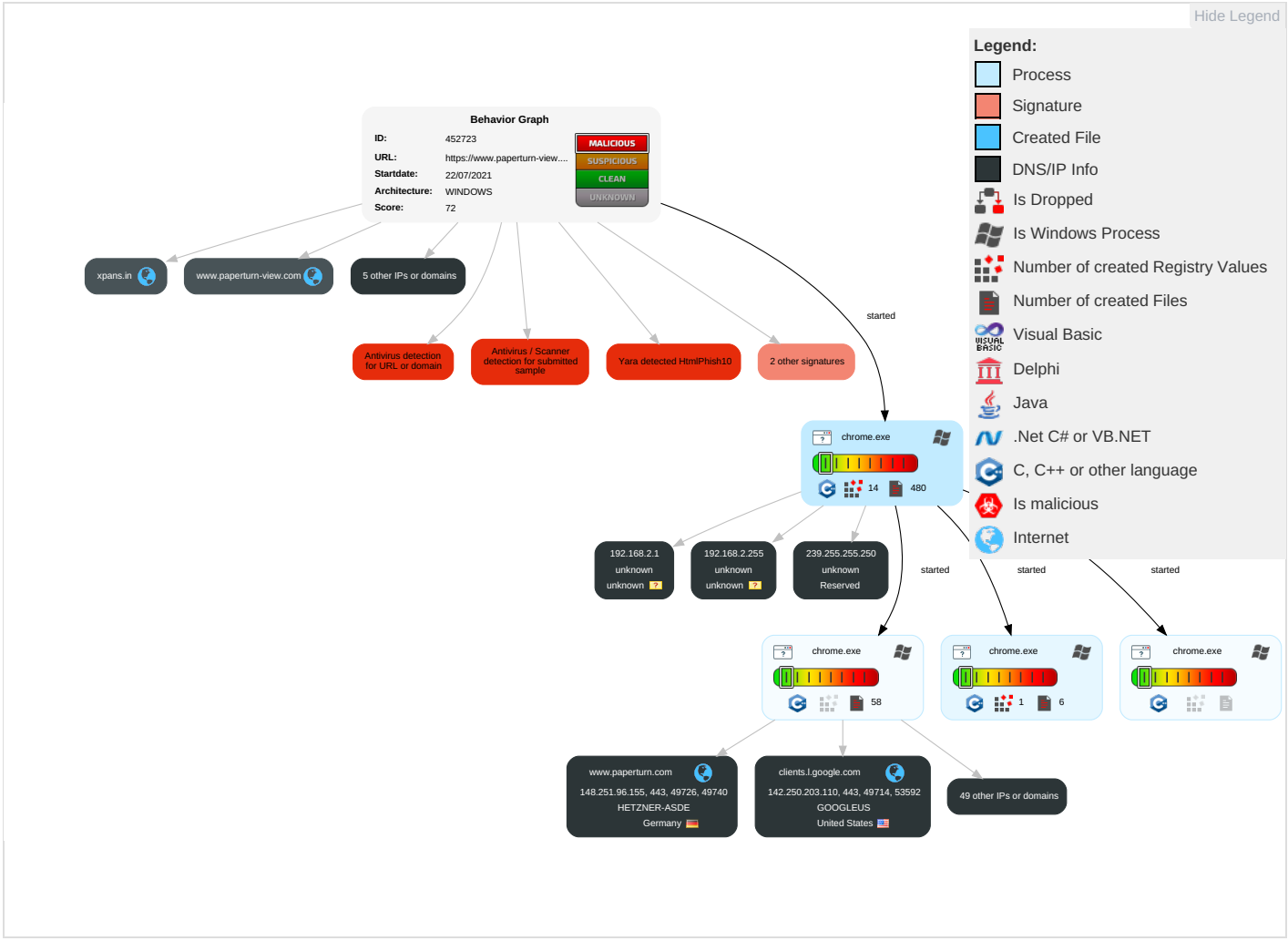
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Scripting 1	Path Interception	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

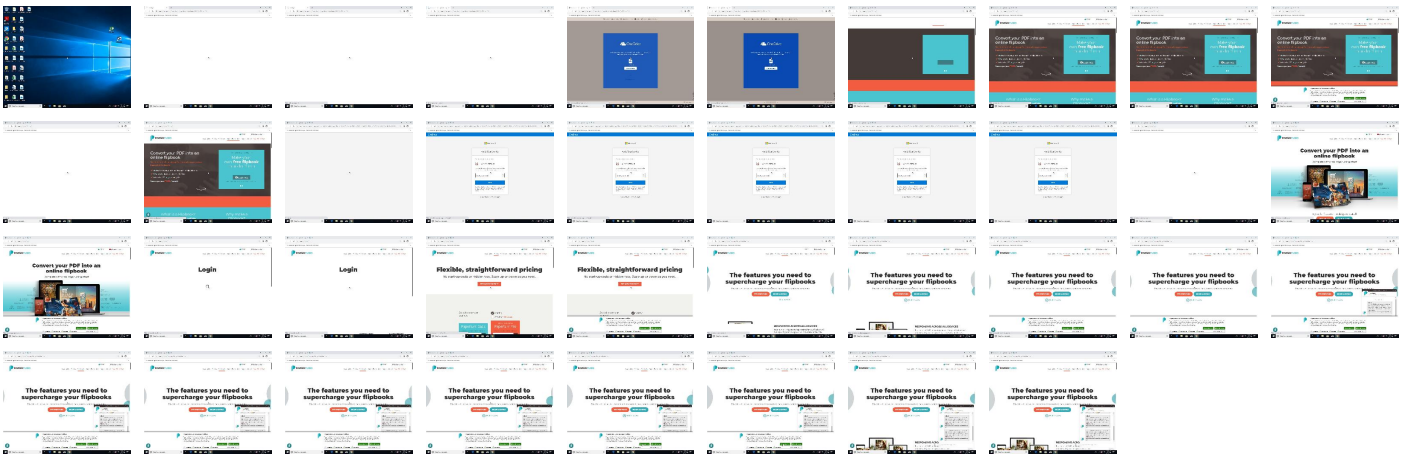
Behavior Graph

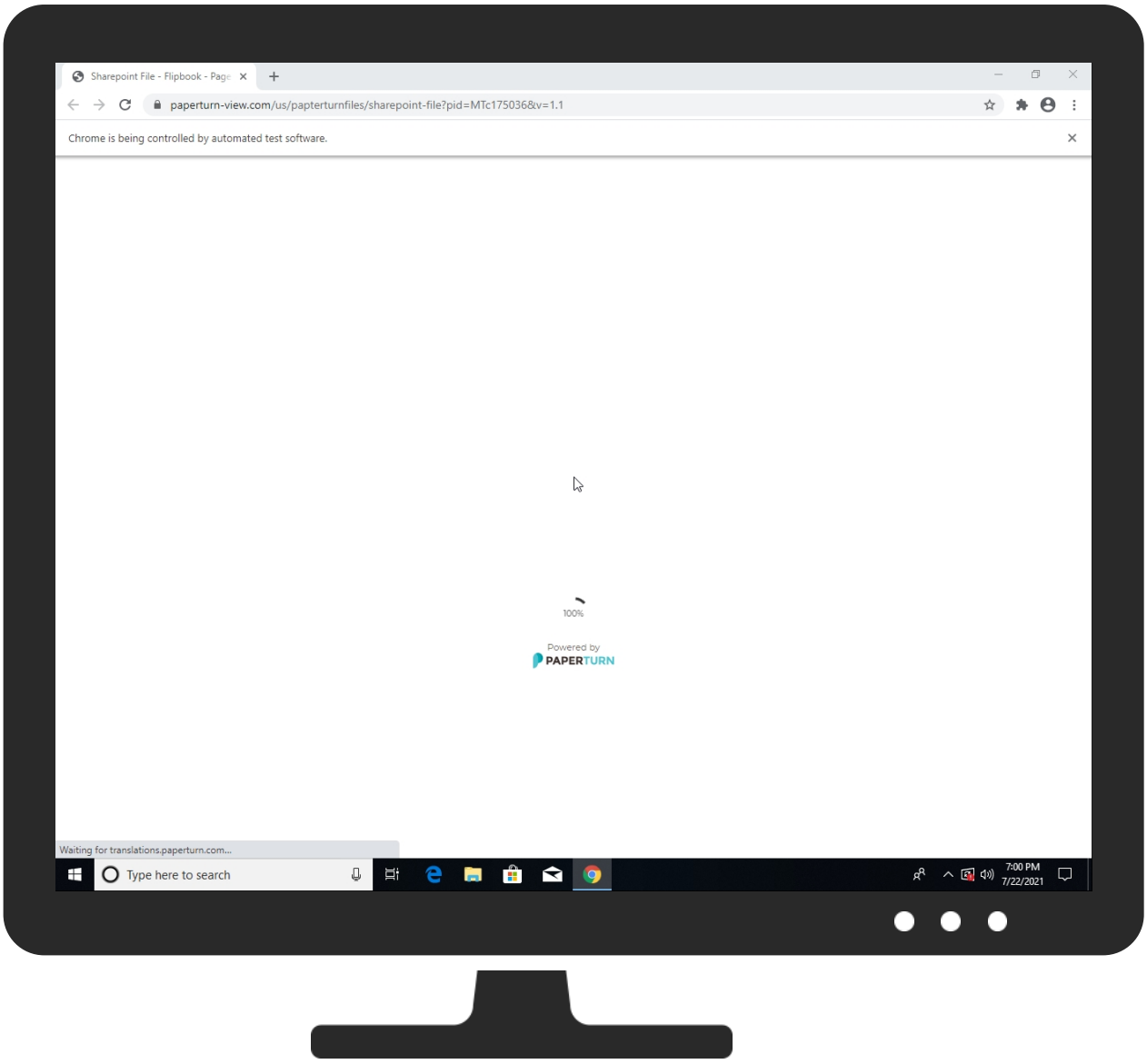


Screenshots

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
http://https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1	0%	Avira URL Cloud	safe	
http://https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://xpans.in/document/Drive/vynii1ggv7u34dlblu2qibdn.php?89bi9G16269732590bcc1ac9819c9793d16548a8c40cc8510bcc1ac9819c9793d16548a8c40cc8510bcc1ac9819c9793d16548a8c40cc8510bcc1ac9819c9793d16548a8c40cc8510bcc1ac9819c9793d16548a8c40cc851&email=&error=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://www.paperturn.com/cache/v2.3.12/mini-b6b0e1e2a9cc4a10cafe9a7b0396818b.jsaD	0%	Avira URL Cloud	safe	
http://https://paperturn.com/id	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/prices#	0%	Avira URL Cloud	safe	
http://https://paperturn.com/s	0%	Avira URL Cloud	safe	
http://https://paperturn.com/l	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-d0f4fc79d4063f6d5171f399465f6cb6.js	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/flipbook8Flipbook:	0%	Avira URL Cloud	safe	
http://https://paperturn.com/e	0%	Avira URL Cloud	safe	
http://https://www.paperturn-view.com&	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/loginLogin	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/uk/Convert	0%	Avira URL Cloud	safe	
http://https://paperturn.com/HL	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/pricesCheap	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/prices/&W	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-b6b0e1e2a9cc4a10cafe9a7b0396818b.jsa	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-af8546ccbc09deec7e6b7a04c8502a92.js	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-8e659b93bd027876d82817aa95060866.js	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/online-pdf-flip-book-features515	0%	Avira URL Cloud	safe	
http://https://paperturn.com/i2	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-2c7001179082c8031f506f1a6a77ca2f.js	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/report-to/downloads-lorry	0%	URL Reputation	safe	
http://https://www.paperturn.com/online-pdf-flip-book-features15	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://images.paperturn.com/g/favicon-new/favicon.ico	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/Convert	0%	Avira URL Cloud	safe	
http://https://paperturn.com/9v	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-b6b0e1e2a9cc4a10cafe9a7b0396818b.js	0%	Avira URL Cloud	safe	
http://https://paperturn.com/d3	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/pricesICheap	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/o3/resource/js/lib/angularjs/angularjs-lates.min.jsaD	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/	0%	Avira URL Cloud	safe	
http://https://www.paperturn-view.comh	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/cache/v2.3.12/mini-5a97efeeff018a0419f17b6689972674.js	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/flipbookFlipbook:	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/o3/resource/js/lib/angularjs/angularjs-lates.min.js	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/pricesI	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com/uk/8Convert	0%	Avira URL Cloud	safe	
http://https://www.paperturn.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
i.ytimg.com	216.58.215.246	true	false		high
d2mvl3dkxvehny.cloudfront.net	143.204.225.47	true	false		high
d3euuwqpqlzvic.cloudfront.net	13.225.29.76	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
static.zdassets.com	104.18.70.113	true	false		high
www.paperturn-view.com	143.204.225.123	true	false		high
photos-ugc.l.googleusercontent.com	172.217.168.1	true	false		high
ekr.zdassets.com	104.18.70.113	true	false		high

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	172.217.168.68	true	false		high
v2.zopim.com	104.16.106.139	true	false		high
www.google.de	172.217.168.3	true	false		high
star-mini.c10r.facebook.com	157.240.16.35	true	false		high
v2assets.zopim.io	104.18.204.90	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
stats.l.doubleclick.net	64.233.167.157	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
www.paperturn.com	148.251.96.155	true	false		unknown
static-doubleclick-net.l.google.com	172.217.168.70	true	false		high
youtube-ui.l.google.com	172.217.168.14	true	false		high
assets.paperturn-view.com	143.204.225.93	true	false		high
googleads.g.doubleclick.net	172.217.168.2	true	false		high
xpans.in	144.91.89.225	true	false		unknown
widget-mediator.zopim.com	52.29.88.9	true	false		high
acsbapp.com	206.189.187.108	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
translations.paperturn.com	143.204.225.69	true	false		unknown
d3jodor2jgify2.cloudfront.net	143.204.225.4	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
static.sharepointonline.com	unknown	unknown	false		unknown
use.fontawesome.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
consentcdn.cookiebot.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
assets.calendly.com	unknown	unknown	false		high
consent.cookiebot.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
static.doubleclick.net	unknown	unknown	false		high
cdn.acsbapp.com	unknown	unknown	false		unknown
images.paperturn.com	unknown	unknown	false		unknown
d8n9fts9ic943.cloudfront.net	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.paperturn.com/prices	true		unknown
http://https://www.paperturn.com/flipbook	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
206.189.187.108	acsbapp.com	United States		14061	DIGITALOCEAN-ASNUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
143.204.225.47	d2mvl3dkxvehny.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
66.102.1.156	unknown	United States		15169	GOOGLEUS	false
104.16.106.139	v2.zopim.com	United States		13335	CLOUDFLARENETUS	false
52.29.88.9	widget-mediator.zopim.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.225.93	assets.paperturn-view.com	United States		16509	AMAZON-02US	false
143.204.225.123	www.paperturn-view.com	United States		16509	AMAZON-02US	false
148.251.96.155	www.paperturn.com	Germany		24940	HETZNER-ASDE	false
172.217.168.1	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.168.2	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
144.91.89.225	xpans.in	Germany		51167	CONTABODE	false
157.240.16.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.70.113	static.zdassets.com	United States		13335	CLOUDFLARENETUS	false
13.225.29.13	unknown	United States		16509	AMAZON-02US	false
64.233.167.157	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
143.204.225.69	translations.paperturn.com	United States		16509	AMAZON-02US	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
143.204.225.4	d3jodor2jgify2.cloudfront.net	United States		16509	AMAZON-02US	false
216.58.215.246	i.ytimg.com	United States		15169	GOOGLEUS	false
172.217.168.70	static-doubleclick-net.l.google.com	United States		15169	GOOGLEUS	false
104.18.204.90	v2assets.zopim.io	United States		13335	CLOUDFLARENETUS	false
206.189.191.180	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
13.225.29.76	d3euuwqpqlzvic.cloudfront.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1
192.168.2.255

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452723
Start date:	22.07.2021
Start time:	18:59:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1
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:	22
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:	mal72.phis.win@45/253@49/34
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.paperturn.com/flipbook • Browse: https://www.paperturn.com/flipbook • Browse: https://xpans.in/document/Drive/ • Browse: https://www.paperturn.com/ • Browse: https://www.paperturn.com/login • Browse: https://www.paperturn.com/prices • Browse: https://www.paperturn.com/online-pdf-flip-book-features
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:00:40	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA

Copyright Joe Security LLC 2021

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_33E8F98A524575FDD27708D6D61F97ED	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	471
Entropy (8bit):	7.165262112463007
Encrypted:	false
SSDEEP:	12:JY0Exc5FZp3TxYu16IDDpbMQwpntPN2BWNoczW14cb:JY0Exc3ZpxYu166btQ+4cb
MD5:	51F89A3EAD171C099581D6FA7FC20050
SHA1:	39C9F05034A23680E7572FD19F4166EAFDD13E50
SHA-256:	49ABDFD49D478D1EB231199F88AC7FD8476F71F4977A6530B48B2EDA95810642
SHA-512:	F6296033604BCEACBEB7A53D808464217A51FD0A0BE8813E0D98F993F4A9CF3E536A84B770ECFE0FB06CF6DFAC17E1E41B54BE9FEDD10682AE2F5E1DF387C35C
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....>.i...G..&....cd+...20210721222013Z0s0q0I0...+.....(..A..B..G@B.X....>.i...G..&....cd+.....V....r.....20210721222013Z....20210728222013Z0...*.H.....I&L.n{....@..fG.\M\...\..<..$s"....i1.....\&pj."....r...;*Zb..x?.}....b...L.&..aj.....&#...fM...V..~...Y...~.g....%.:..]oR./cN.....=.]A.8...X...irU..i.X.`...D...=\|v.#$X. ...A.t.4...|..!.s..Z.....E..@.%#.(.J.f.....%.....K.3../..d....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1392054451166236
Encrypted:	false
SSDEEP:	6:kKffqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:3fG5kPlE99SNxAhUe0et
MD5:	5F7022610D28099D8053D3DD4220766B
SHA1:	20BAFB97B231372268C6345738C3FC552B897176
SHA-256:	8C3ED4CD9BB870B757446DA39001AF76FEA41FAF0E97379AA180C337A8665FEE
SHA-512:	971B4F95C7927ECD9E578743402E49EEAC4B98E07A8CF2195D13EB384288B77FBA623F952E7AEB49242F70A3E5C82BD8AF672C0390E1954B447831996EEDDEA
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Reputation:	low
Preview:	p..... .....f...(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_33E8F98A524575FDD27708D6D61F97ED	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.844855388633013
Encrypted:	false
SSDEEP:	24:IXmxxvnFqYwJNEMtsq4nmxxvnFqYwJNEM6:IXODkqosq4nODkqH
MD5:	8D16F2BE30A07A55563325EADA586AD0
SHA1:	05ECD7358FE5D1FA4F43E116CAC068662531CAEF
SHA-256:	36EB42CF57E349ACB9017B22F1FE565146B4FA01ABFE036522801BE47DC1F556
SHA-512:	C556272F03A0C8A6AFF72563FDC80AC6CD591DE05CF4D55BFD39560EDE14EF55F9CA541C1AB5DB0C26B6908EA3E2D1C963D53049DA0225F98A5B8256CFC278
Malicious:	false
Reputation:	low
Preview:	p..... .....th.f...(..... .....o..~..?8.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.K.X.B.1.Y.M.1.K.n.r.v.%.2.B.J.y.8.e.C.W.2.I.I.%.3.D...".6.0.f.9.2.c.c.4.-.1.d.7."...p..... .....th.f...(.....L..~~..... .....o..~..?8.....h.t.t.p.:././.o.c.s.p...d.i.g.i.c.e.r.t...c.o.m./.M.F.E.w.T.z.B.N.M.E.s.w.S.T.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.f.q.h.L.j.K.L.E.J.Q.Z.P.i.n.0.K.C.z.k.d.A.Q.p.V.Y.o.w.Q.U.s.T.7.D.a.Q.P.4.v.0.c.B.1.J.g.m.G.g.g.C.7.2.N.k.K.8.M.C.E.A.K.X.B.1.Y.M.1.K.n.r.v.%.2.B.J.y.8.e.C.W.2.I.I.%.3.D...".6.0.f.9.2.c.c.4.-.1.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\0079b35c-f8fa-45a7-a8b7-bdf8eba80ff1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	368958
Entropy (8bit):	6.027723401716834
Encrypted:	false
SSDEEP:	6144:6euVhcD1QqqO9y+9pjtKb8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHL:SV21H99ttxzurRDn9nfNxF4ijZVtilB0
MD5:	DDC37B1394D8170271B8E953B9E44550
SHA1:	CF8A54F5434FA2A5496C7897C45725C88755B6BD
SHA-256:	A4694446CF4B822446D23BF233671874009B460C4791C909A0DE1101DDD513B1
SHA-512:	68D3236E5875B408556F8CB676DEB62AC33D7E3A3031A5465EA8A8A395D2D1E718AF75757F77C14BB685AB40677136BC3CC4DC82E3FC7AFE62E2961924AAD7A5
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62700563214231e+12,"network":1.626973234e+12,"ticks":4358913301.0,"uncertainty":4536820.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075900350"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\0ef446f5-5daa-4ac3-b591-1c4784fc95ce.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	365377
Entropy (8bit):	6.01522968420814
Encrypted:	false
SSDEEP:	6144:xeuVhcD1QqqO9y+9pjtKb8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHL:BV21H99ttxzurRDn9nfNxF4ijZVtilB0
MD5:	8DA00429ECCA7B8F115ADBC40CF22513
SHA1:	9CB88E3508E59C79972823E9FB3D767802F97DC6
SHA-256:	A0B107246388F873DDA12C41CF0BEB2D40968455C26A9E2301D4AB1C342B4BCB
SHA-512:	D6261342670151AAC3D3CC011F6C715A33B175B7A976268F3FBD3054CA328046DBB8AB2A4B54D59CA695046BFA6D8018B63E0DCC979BB7E51CF1D27D58D74CB
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\0ef446f5-5daa-4ac3-b591-1c4784fc95ce.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62700563214231e+12,"network":1.626973234e+12,"ticks":4358913301.0,"uncertainty":4536820.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075900350"},"policy":{"last_statistics_update":"13271479227799

C:\Users\user\AppData\Local\Google\Chrome\User Data\50907df1-3712-418e-9e91-0ec9028aa3d5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7515847627811647
Encrypted:	false
SSDEEP:	384:HDadlbAODHABMNxr6vVv3ex7OHfGGClrQTV1xuvbrar4pmwrQvRFpqO7LdNA1ZAs:qKtFufqGQebpLHEnrCzKpPlFM
MD5:	D534EA9DA5F31B5222BFE87AF2A87B6A
SHA1:	BF08A3A545ED125BB19B16CFF22C72340AAABE70
SHA-256:	E92694DA6082826279A9336607F81EB3FFA6362B81A911065C71AF4C8A902B37
SHA-512:	2264D8F1ADAF9C070488889AA5FFB1D09F5EE59EBCE1830A21CF6D73192B166495DE615B735459E4F2BBBFBA83884E6C13B96C67473F3F1292970AB09E5A851E
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...z@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\72446f73-412e-4b09-a7fe-857f99e52227.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	365376
Entropy (8bit):	6.015229686192827
Encrypted:	false
SSDEEP:	6144:IeuVhcD1QqqO9y+9pjtKb8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHL:QV21H99ttxzurRDn9nfNxF4ijZVtilB0
MD5:	A434BAE75CDAC9A45FEB9C8490ADAAAD
SHA1:	D274178754FEC25B3F87AA24ADC98521940CB638
SHA-256:	F769CF63C0BB78A7EC4A57BFEB0131434D6FB157AB571215860E6973710A5ED2
SHA-512:	5552F236DDEB3711B6FDCE73E74B849AB9472989B689671F809AC4867025401488171A2DB6103E8BC7B426BE4D6DFC8198340771095259D792149EB2669383B2
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62700563214231e+12,"network":1.626973234e+12,"ticks":4358913301.0,"uncertainty":4536820.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13271479227799

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\09e8ef0e-a23e-42cb-a038-ed5f9c541cbc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1373
Entropy (8bit):	5.592535852544843
Encrypted:	false
SSDEEP:	24:YEyKeUutoO9RAeUupQx6H0UhHbrfwUut1UyG1KUfcmNaUeCis7wUfQRUeIQ:YOeUpCieUWO6UUhAUF9KUkmwUeCi6wUM
MD5:	7D901AB2096BE1C7F4F6B7C3140D2C2A
SHA1:	A00C5C4B729A02FD744F9C9185B450DC5C2AA486
SHA-256:	890840039E3D503906BD00AC4AF49F724BCE2A3F481B336AA9444A13E817438A
SHA-512:	5E34F86FBAF83CB82FFBF3F1CB89B56CDED1E6A4FE25AB62CCFC02781D60CDFBAD1DBACA60BFDD254D73D02E17D002874D3B72AE3958DAF96748BCB9BDD E0E0D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1637892033.911582,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1627005633.911589},{"expiry":1658541632.988816,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_in clude_subdomains":true,"sts_observed":1627005632.988822},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"for ce-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1637892033.322103,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlN C4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627005633.32211},{"expiry":1658541639.72814,"host":"nAuqgR4iEWti7SOdT3UHPl6rm ZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627005639.728145},{"expiry":1633013040.850112,"host":"5EdUoB7 YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\466b524a-38ad-4c10-8896-c1e117ba52a5.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5706
Entropy (8bit):	5.184610668893168
Encrypted:	false
SSDEEP:	96:n3rssHMXiSKIiIk0JCKL8hkX116AbOTQVuwn:n3rBMXiSAC4KikXb
MD5:	8EBCD08D073C42600AE6B7D561C58779
SHA1:	8F0B80B1860A766DD88409F24A0B909EFB0DF57B
SHA-256:	014EE7C8AAFF7E1C2FC77081566CEDA0C9A4A8BE5902EED58C5656CFE8BF3F51
SHA-512:	5CEF899757E8423129087D1D5AA1E939A2B41A2A08EA08C7A863045FD522E41AE1D06BC80B9C93FFFB8E83BE881A6B259FE0B3099DB149A90254754DDF32A86
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271479228160554","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6ee6eeaa-d560-48b5-a23e-bac9f35a5672.tmp	
Category:	dropped
Size (bytes):	5062
Entropy (8bit):	4.969698035661608
Encrypted:	false
SSDEEP:	96:n3rmoGMpSKIiIk0JCKL8hkX116AbOTQVuwn:n3rSMpSUC4KikXb
MD5:	8568C403C8B51136BDD84B3742BE37DC
SHA1:	9154FAA2DD22FED96B9ABD9C99AC1DC54BF7FE37
SHA-256:	3F6C1AC8C16C56F0498D0466F9A981A4530A9B45A6C3F4A86F16824BFF3822DD
SHA-512:	6C0DD433AF838E84E4B92B40F00D89B2248A4926BBEB091769AD279B6EF2A7B77435990C5AA55F4F680942B3A0CA0AC076AF5F4C1E8DEAE1587B464858CC7C2 1
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271479228160554","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a0401b1-ba1d-4486-bd77-cf1fa87cf2d8.tmp	
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324854 2628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{ "advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.goog leusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\907f1a37-8d8c-4587-acfa-f9d67eb86453.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.173287362129446
Encrypted:	false
SSDEEP:	6:mfRSLSueN+q2P923iKKdK9RXXTZIFUtpURSLSkZmwPURSLSEVkwO923iKKdK9RX3:YSmuXv45Kk7XT2FUtpISmk/PISmE5L51
MD5:	F0AD8EE11238B60B963C5FF7023B3D5F
SHA1:	CCB95F6D57271A55D61A68AA4732FE7DBE06FE70
SHA-256:	21F50DE6A6019DD3C37719CE64A09D1DA28FA066DC35429FD898C7456E6967DB
SHA-512:	2F630F1F7960F475925EFCD4DEA0F315843D4D70DBA7228FAD4CC026771C14139C42AB5EF88C19E4E770995DB0553F09EA32C3AC462B35ED6E61716784B2B60
Malicious:	false
Reputation:	low
Preview:	2021/07/22-19:00:47.749 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-19:00:47.757 1aa8 Recovering log #3.2021/07/22-19:00:47.757 1aa8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.142157628015787
Encrypted:	false
SSDEEP:	6:mfRSLSQ+q2P923iKKdKyDZIFUtpURSLSOdFZZmwPURSLSOdFNVkwO923iKKdKyJd:YSmVv45Kk02FUtpISmOdX/PISmOdF5L2
MD5:	3A8B2989AA6780AB15B5CF6543E664F5
SHA1:	E6E7AC06EEDD9CD0ED7DB2379321C05A6920D8DE
SHA-256:	BF603A382C98906F17C7E8AB6D53EBC63E8F0EA19A6E0543833D99DB1D2C54B7
SHA-512:	582B0255CB554BD4386799A527C916FDF831E62384ED48342896D43307C18351A1AE99EB315531CA06ACF15508C8C86448727214A710F642EDE45CEFED4E6E12
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Reputation:	low
Preview:	2021/07/22-19:00:47.717 1aa8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-19:00:47.719 1aa8 Recovering log #3.2021/07/22-19:00:47.719 1aa8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ae6b52f6e424e4e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1170
Entropy (8bit):	5.416534278704916
Encrypted:	false
SSDEEP:	24:i7xfo1o7WfDo7FvfJo7rfNo7Axft3o7f4fG:yxMYWbYpRYrlYAxF3YQe
MD5:	AAF47CAAA2B306A88CD470B43EBAA058
SHA1:	6D4B8274C6EE8C6A8B8E130F3DFCF02A2339BA55
SHA-256:	A420DE67B54E7F92E448F87B00E64A3189772A1DB3F35279A509C070D6B1C556
SHA-512:	D66E3E20D077CC92D10DFC36A8D57243A1B0C22BAADFDBC088B4173E7AB2169663B91341D5F28C45267A9BDD688D3BD26B789BB8EE1A21A9AF2025F98F86C2A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....p....._keyhttps://consent.cookiebot.com/uc.js .https://paperturn.com/l...W&/.....b._y.i...|y...v*.OG7z...y..O.A..Eo.....=.1.....A..Eo.....0\r..m.....?....p....._keyhttps://consent.cookiebot.com/uc.js .https://paperturn.com/..<.W&/.....b._y.i...|y...v*.OG7z...y..O.A..Eo.....A..Eo.....0\r..m.....?...p....._keyhttps://consent.cookiebot.com/uc.js .https://paperturn.com/...W&/.....<m.....b._y.i...|y...v*.OG7z...y..O.A..Eo.....N,.....A..Eo.....0\r..m.....?....p....._keyhttps://consent.cookiebot.com/uc.js .https://paperturn.com/.=..W&/.....b._y.i...|y...v*.OG7z...y..O.A..Eo.....DW.....A..Eo.....0\r..m.....?....p.....__keyhttps://consent.cookiebot.com/uc.js .https://paperturn.com/..).W&/.....:.....b._y.i...|y...v*.OG7z...y..O.A..Eo.....2c.....A..Eo.....0\r..m.....?....p....._

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\105618d59203ef9a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.645904494553558
Encrypted:	false
SSDEEP:	3:m+l3+ldA8RzYrSLIpRKsWXWb6u1NRPguGTKg4R2QKt/lHCNNEm9x744m2/pK5kt:mm+9YGLIGg1NpguG3c2ntgNNlx88K6t
MD5:	09C63BB72E759C8D4A35862A4FC035D3
SHA1:	0649193A1CADA600EF6995CA52359C0CEA390CD1
SHA-256:	35A3D9F2EDB4E62D47B062483B48634559B8645C75879CAB182472195C8ABE86
SHA-512:	023EECAC334CC134D7759828594416E472D58373ED9E83ECB39B56A4648C284673777EBA00F5350F6A5F8367117423EEF93B2948D4D6411940D588C0A362055C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e....65M...._keyhttps://www.google.com/js/th/rri_UWQ0J4KTeoiEc0uqeM0aau5ykYMkDZQXo2HoPhc.js .https://youtube.com/....W&/.....s.....VV.:..GYc...P.....fw.OT..O..Hi.A..Eo....._E[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\16d9c28137016842_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2268
Entropy (8bit):	5.71434316734612
Encrypted:	false
SSDEEP:	48:1M9ZU9ehDrM9ZU9eh6rM9ZU9ehxrM9ZU9ehtmNrM9ZU9ehNrM9ZU9eh7c:Y2Z8AAA
MD5:	248E43BEA24A2BB21795FCE131C7F521
SHA1:	5C7009B9DF3D30E5679F773DE91A6AC01084C343
SHA-256:	A8D78843C2F0565313C2CA016EB2371224761FAE1631B49374FEF1B2FBD84A96
SHA-512:	78CDE3A4B9C13EA014D94E467EF6AF73A0CC1354B0C2F64825A5AB210FFF1B397B5C9921F79D987731FC997A01EA5DC37D1E8DB9C11B1D5502E85B5C6990B92
Malicious:	false
Reputation:	low
Preview:	0\r..m.....)....._keyhttps://consent.cookiebot.com/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/cc.js?renew=false&referer=www.paperturn.com&culture=en&dnt=false&forceshow=false&cbid=15dac99d-cb99-4df3-83c0-6e8c10ac66d8&brandid=Cookiebot&framework= .https://paperturn.com/'V..W&/.....cy.P`...bbv.&....,!...y?.....A..Eo.....<.....A..Eo.....0\r..m.....)....._keyhttps://consent.cookiebot.com/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/cc.js?renew=false&referer=www.paperturn.com&culture=en&dnt=false&forceshow=false&cbid=15dac99d-cb99-4df3-83c0-6e8c10ac66d8&brandid=Cookiebot&framework= .https://paperturn.com/8.U.W&/.....cy.P`...bbv.&....,!...y?.....A..Eo.....e.0.....A..Eo.....0\r..m.....)....._keyhttps://consent.cookiebot.com/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/cc.js?renew=false&referer=www.paperturn.com&culture=en&dnt=false&forceshow=false&cbid=15dac99d-cb99-4df3-83c0-6e8c10ac66d8&brandid=Cookiebot&framewor

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\236c9a70f6d402a3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.530424800010962
Encrypted:	false
SSDEEP:	6:ma//XYcvhAbuB4XEbsvNRs2buBaontgwMll3yvCfK4LpnK6t:HXJuUIz0AonBk5fD
MD5:	AFF349F40939C94E43ADAC122961CBF4
SHA1:	44C47EF1C5445C67976539F64B9E77D6532AC589
SHA-256:	0642415E6436A120C0772A201EFEC0EF1F31188F567FE89ED4BCBA01B84B1CCB
SHA-512:	AB0E1426F466C990B07D0541617B8087D738D9A1A890DFC2EA14A5F5E9DFF00C31E0B740C0B0D49D888D6A00D82AF8D415631E045B381FC0BFCD5E42D76AFC6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...4N.D...._keyhttps://assets.paperturn-view.com/components-TopBar.54d5964a.js .https://paperturn-view.com/.At.W&/.....T.g`Rg...I1y. 0.?.@..d. .A..Eo.....C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\335e69ddec2b9ac6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.32763920704684
Encrypted:	false
SSDEEP:	6:m9XYGLKd0Kc5noguGFYgPUodQSQCw5r10/hK6t:9WPoguG2ooO
MD5:	27DC5F0D3B49BC5198BF9B1A3AEA7612
SHA1:	A8CFC60C8B7B4AB3098DDAC5E389C8470B701EE0
SHA-256:	6B5F11C606B548E5AB411B9B4F21FC922996A4F59B6B2F798AB6D9BB3C69E071
SHA-512:	2E152CBF483021A5C8E1E3368391FCDD73EF44F684BF8F8424335E20B38D99FE3C0E38954D2C7B561B1303C85E316BF1543EDA8185E6E6D0F24B44263260500F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...E@S...._keyhttps://www.gstatic.com/cv/js/sender/v1/cast_sender.js .https://youtube.com/wJ..W&/.....Tt.....1@dbM..w./.61...wt...R..u.AU...A..Eo.....2.p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3aa07428c0e4d4b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	159032
Entropy (8bit):	4.544605782778889
Encrypted:	false
SSDEEP:	3072:queY/O6AUnY/75bg6xCbsd/fuBT5chElus/di1wuNjkGsR7JhH43AsCvvVOzsuJH:qqO6wPwb4wMahY3AVvv87F
MD5:	64E167F2235FB642CE28B83B60D556FD
SHA1:	A9A20993A0DE130D0DFE1E8948CB167928F8DF83
SHA-256:	F6137E70C63FCB4BAFA95C77058F19396D87DF364FE19CACEE4CCBBC94D31411
SHA-512:	1E3C027B71C4D8904308237057F4643DE8327E19F25451EFCDE8B433CF4D8F9D1514AEDA1B879CB07F7D711CEB00B672119C0222186E053C50494C98BE894A21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....i....A46A4BACBDA6493C18D52D950BA55B74358D15D3599484FFCE96C2C2F844F3B3.....'.....O....@l..H8<&.....D...`.....d.....(S....`..... L`.....(S...`.....8L`.....@Rc.....Qb&T.f....d....Qb.....e.....M.b....d.....I`....Da.....(S...`.....L`....I..Qc.R.....parseInt.q...Qd.'.....fromCharCode.....K`....D{ ....i.....&....&...7..&.]...&.]...&...8..&..#j.....&.(...&.%.@..&.Y.....(...&..$&.Y....4.....,Rc.....`.....aJ.....e.....G.....@.-....\P.a.....P...https://www .paperturn.com/cache/v2.3.12/mini-2c7001179082c8031f506f1a6a77ca2f.jsa.....D`....D`$...D`.....`....&...&..!.&..!.&.(S.,..`....].K`....De.....&.%.*....,Rc.....I`. .....Qbb.2D....k...a.....b.....1.d.....&.(S.(.`.....L`.....Qb~..Q....\w+...K`....Dd.....,Rc.....`.....a.....d.....`....DI]d...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ee3277df70d5d32_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.5409136631190705
Encrypted:	false
SSDEEP:	6:mmnnYGLUxGBznGKT2buGguGpKtgnaGF6P4bUK6t:gGBR6buGguGpN6P5
MD5:	489FF5F6404E029694DEB0C4D201ABAE
SHA1:	BEF14BF06EC79021FE7EB8236EE9AC5501FF46C8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ee3277df70d5d32_0	
SHA-256:	23837E3E8312DC2D5218BDA0BB9A558E5D587980A96BAA9CB223C62ABA71103C
SHA-512:	DC1D0544699D2D092DFBD409FB32A61846636C0DF792FAB407EBDD977558A1296F2191F92816EE28FBF6987CB9A54AACB55A6840CA6F4CF988F6CE0964FD256
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...$....._keyhttps://www.youtube.com/s/player/3804dce2/player_ias.vflset/en_US/remote.js .https://youtube.com/L...W&/.....s.....T.U.>...ij"..u<)..h*.T%,Du .m.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f84843334707219_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.571933396919997
Encrypted:	false
SSDEEP:	6:mUNU/PYcvhAbuB/KSbJESO6os2buBADug9bdvKekAxhK6t:pN0XJNK6JESOZ0Snb4Tq7
MD5:	E5C3561CC34FBF79A910519D73D18F91
SHA1:	6E99B0E050FF0899159B40AFE8E87D050B05AF79
SHA-256:	7EE1599F2A68D2CCF98A033C57645804000BA9BC6FF63597958F389B3BE9C8B5
SHA-512:	D8A3DB4E7381D3A75350AF745A244BB956D843A1C3B226F43E104723D84C02EB62E439D70FCBB0267BD8A7789C5825499A4CFBCA6F1603ED666A0D2F019DC53
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....\....._keyhttps://assets.paperturn-view.com/vendors~components-Newsflash.b7b94969.js .https://paperturn-view.com/.7..W&/.....S.M.....yz .G.]...&tO/X...M.....A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\402f710388ce73f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.517101235613113
Encrypted:	false
SSDEEP:	6:mKYcvhAbuB/KSDTLzs2buBTgol/MxBy4mJ/ZK6t:DJNKe0DCyRJr
MD5:	556008CF93B693F15A74A009C84D7497
SHA1:	3876183B13DFF6B4A8B5137EF3443434B9A48919
SHA-256:	8DE27A1DEB0488437870E7C632C66122C35745C7EFCCF34B2EC33C557CE014F5
SHA-512:	EEACDDDFCCAA62ED3D4FD37A70083A65C3C96124AEAF8788C4764DA5A051B48DC5CBFB21C576C38E1CFBBF3305BB2DD7D367A1E22570C51DC88700C5AC14 25B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...*.R~...._keyhttps://assets.paperturn-view.com/vendors~components-ToolbarButton.aafd698b.js .https://paperturn-view.com/..x.W&/.....x.m.-.. g....'.JT..b.^...%J.h]..A..Eo.....T}j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a93ae2abbf51303_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.492178418923658
Encrypted:	false
SSDEEP:	6:moYGLUxGBzn871j4PY0c71j4GguG6tg1AilThXO0/40DK6t:eGBU1sPjcRsGguG6oA8V1
MD5:	516DEB4E5859928C602AE6CCE2B1431F
SHA1:	BF5229E9B3F7F52AFBA7EC14EF2BA14AC2E92835
SHA-256:	2A06EBC089F6275A11906D838A3ED911EAF9E138A7F5DBDF92E23BC5D2CF6F67
SHA-512:	89FDEBE09DED5DF2D7AF50435938E1AE861E0F1FD5DFDBB77CF8C38A0667B038AE26C697365967C4CBE2C80A9258958D8EC60954E99CDAD819B9499572DAC 9A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://www.youtube.com/s/player/3804dce2/www-embed-player.vflset/www-embed-player.js .https://youtube.com/.%..W&/.....eo.....?.... C/a...+i..d...B.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b4ae9e2956257f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4b4ae9e2956257f4_0	
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.54224819164011
Encrypted:	false
SSDEEP:	6:m6YcvhAbuB/KShXEbjfs2buBIvtgD/Pc1nC/bK6t:3JNKpX0OvNU/N
MD5:	0098A805BE93A3DD27B322A8B825C3F8
SHA1:	3835D397C3D573EF6D10E9DFE41FDEA2D1A3B8F7
SHA-256:	C6905CF1B75684E45FFC2693A2A0CF8BB61D69AE95552029F2A4D13870E45E87
SHA-512:	A8EB2C0D757A43745CD26BB27BAC9522F15EB4667288658D45ADC85585D36B36748A3F645A9653340922C37E7278206BD82688E8AA28F8E01D63DD1CB104F001
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...!I.1...._keyhttps://assets.paperturn-view.com/vendors~components-Tooltip~components-TopBar.09a36c1b.js .https://paperturn-view.com/XAt.W&/..... ....]s..Y..J.....)X..S.....1C.A..Eo.....v.S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\505f12502b0e1e8f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.491594431666653
Encrypted:	false
SSDEEP:	6:m1PYcvhAbuBM27sRs2buBVtgflQilpBY0RK6tW1PYcvhAbuBM27sRs2buB3ygP2l:4XJ80jAlJNrSXJ80l1+
MD5:	9507CCEC2048B94ACA593FC74FBE0389
SHA1:	37A1B3DDFD1CC61222E9BA805D3E922E777EDA65
SHA-256:	4B56766F12A36DCFD5C3B2667D4A4861AC57A560DEEF8BDF66FF58EE769E6B4A
SHA-512:	D203ECB99998588C2857ACD4DA7B4A11DA836AC9805B146836D7C378345E4317EFA07C4E63521D2C8615F781909FBE2DAF688B7C05374FE9228187720B3EFA57
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...-d.E...._keyhttps://assets.paperturn-view.com/8.e31fc8b3.js .https://paperturn-view.com/9.\.W&/.....n.....9.u~....&.....Y+:..n ..."..A..Eo.....t%".....A..E o.....0\r..m.....P...-d.E...._keyhttps://assets.paperturn-view.com/8.e31fc8b3.js .https://paperturn-view.com/(..W&/.....9.u~....&.....Y+:..n ..."..A..Eo..... 7J.f.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\57849aa2afcf52a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.573012435911901
Encrypted:	false
SSDEEP:	6:m3tVYcvhAbuB4bJEnnAVRs2buBSHgBqjzr5hnd6hK6t:2VJubJEnWR0MmYzrDda
MD5:	9765D9A91E589048FA49E9203F3CEC44
SHA1:	547DADDE8FB8DE0CE4C1C846F50EFF9A54669169
SHA-256:	6D4825A8F8BD57E928947D147FAAB6ADA32D3061221827BDABE5176462289570
SHA-512:	1D90009DCA39159BBBECCE4C0950C670FB38F29FDC3DFC3948BB3FDCF5E320ABE0457B3CF0ABFB14FAF5FB2A50E6051DDD6E9ACBB3095BC9F07B97B18069 6EC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....:....._keyhttps://assets.paperturn-view.com/components-Newsflash.389922b8.js .https://paperturn-view.com/>=..W&/.....P...>...aO.i&..j.>..Rc...z.. M.A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ae823d24fa20467_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.469641644901993
Encrypted:	false
SSDEEP:	6:mQAsPYcvhAbuB4nxwRs2buBoofvtg1EtsE6CSp2+K6t:KQJunK07essld
MD5:	5CE9304E6DFC12322B89F45EF2174246
SHA1:	D914B3CBE643715A65DFEBD66E879B30CAFBC0E8
SHA-256:	4776E13DB1E6E7B14013569BD7D4E1627951BF56CE683B6F76924C00BECF4638
SHA-512:	78A322E18B32CF9CA0C0F17F0B9174AC35E508E0D1EE6D0B05AF2BAAA05EF1A8062FC9F2DB3B5756D369CCD861BAA566B142A7C00E85AAAA88ABB50FBB7F6 66F
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ae823d24fa20467_0	
Reputation:	low
Preview:	0\r..m.....a....,ei...._keyhttps://assets.paperturn-view.com/components-Toolbar.0413dfe3.js .https://paperturn-view.com/.ev.W&/.....8Svn.]...a...x.|).....].A ..Eo.....v!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c8938a5f2f8b277_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.646374113787241
Encrypted:	false
SSDEEP:	6:mayEYcvhAbuB/KSc/QOly7ryIObb8XcrvNRs2buBjFgnlfvTr4p/bK6t:Py0JNK/oOErR5Xcrz0uZHs1
MD5:	6C52963A967576B7FFD290386D6298FE
SHA1:	245D41CDFDC5DA1A99C5C9BB2C55B1554D968E97
SHA-256:	7892142AE215555D84059CC6203E2C0A601473D1E7C091DA8D6CD295C4DFC0D6
SHA-512:	2AEBA0B05CC71203248B78E29D643143E461CCDD7D8A7231597627354610 7E84AC1F8D7D1A1A38E9EC3326E5E4A51E635F7240AC4C397177550DEA0B92F5F4A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.paperturn-view.com/vendors~components-Alert~components-BuyBasket~components-Dialog~components-FirstCustomization~comp on~3fad5945.d972b361.js .https://paperturn-view.com/.Yn.W&/.....6..9VbG.S.j>.[@.<Z..LS./.../.A..Eo.....F+.&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e756fb02c040fa1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.937518762158875
Encrypted:	false
SSDEEP:	6:mqOYGLibtGqlbcYFos2bt40tgOVCD6rdK6tkDKaE4UVtpPVCD6rXI:oqSYCk0n8mTDaEZ3pP8mz
MD5:	9E08DC60334946906534D2E9AE10A408
SHA1:	02EC03425529664305D5B3BB604730F8FCD7514C
SHA-256:	BB9F12B43F7A3076D923F11FF45BADC74F5D6B1DFC042F48FD842D8512709238
SHA-512:	EE370B190793C3055D4AE8771131C7F4F62CDB2F426E86836C96187A94B422E8AA2066589B8A0FA53F137264E03EB63AD347E71E83B7117BEF7457B44A21D1CC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...t..'...._keyhttps://www.paperturn.com/cache/v2.3.12/mini-b6b0e1e2a9cc4a10cafe9a7b0396818b.js .https://paperturn.com/....W&/.....;....DOXj.K... ..x>.0....A..Eo....._.aT.....A..Eo.....W&/..f..8E88A35BD36F53D98288D14D5E501E2F584B9B2AF358BA6A88F63A1F7303D98B.....;....DOXj.K.....x>.0 ....A..Eo.....xj._L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\641fb3ab98d94d28_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.6101694919205425
Encrypted:	false
SSDEEP:	6:m3YGLibtGqaDeSLTOFzs2btmpugVuDtwByp9K6t:OqaDNOR2fuq4X
MD5:	3816E65F2DBD6765C641BF712A6F827B
SHA1:	575CC4A7EE2E62019B4120CE7E8A251790825BE1
SHA-256:	8825C41D44CAF08790BD161EF28E4828113BCED426AA2F5A3AF6515ADF014866
SHA-512:	6E0FAABB66A7C54BFFE822312E3E3C914C79921C664B2AC13D7421619C25C47EC18DEF57744C8908B4B5CF054DC17D306D7F81745C94240C62B8BB2C0D7744
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l.....l....._keyhttps://www.paperturn.com/cache/v2.3.12/mini-8e659b93bd027876d82817aa95060866.js .https://paperturn.com/|...W&/.....2....i....P.d..... |..5d..u+..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75180a52d49873b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.4229210743168155
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75180a52d49873b5_0	
SSDEEP:	6:mZBXYcvhAbuBKB/2uns2buBhugIEVd8iKdhK6t:i/Jsou0eMw
MD5:	85E57A4ED2D9953690DA1F134836F48E
SHA1:	2FAC72AA8EC9E441252276919A8D58E5A9722E7A
SHA-256:	1DFAB13BFD533275B6F82950D9134B32108EBDBAFC0CA0ED2424D541690126CC
SHA-512:	C2DDC61A7963620C7839C89CB2C7229F4BCA8784ADB82DED15292267C2A75D2133852BDD6AD3504377715822AC7E8A1AF4F47901AC32309734B35F2CA79B503
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...'r-....._keyhttps://assets.paperturn-view.com/index.js?20210723020032 .https://paperturn-view.com/coY.W&/.....n.mU.mluW..33..<?rbE;..C0. ..e.A..Eo.....2|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75c880fe196c95da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.578332801734761
Encrypted:	false
SSDEEP:	6:mE2VYGLUxGBznGKT2mABSguGsvtgmXll3A6a4r/6DK6t:z2aGBR6mkSguGOvxZr+
MD5:	73AF076A872457C99407FB96D1C1A69A
SHA1:	0F386D137233C42F4E144C535431C5B6BCDF7B49
SHA-256:	B1C868ACE553F3FA087D7142754E7ED30FD4185E13D77D96A52C397DA390F4E3
SHA-512:	98E5B1FDAEC6B96A2F29A11B2082C9051153F7843BA69FA6F134C68980E341C498AE94456751D7AEE565ACD031BD3C86142FE1D64F1ED5A04461DF65258BD8D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d.....T2...._keyhttps://www.youtube.com/s/player/3804dce2/player_ias.vflset/en_US/embed.js .https://youtube.com/.%..W&/.....s.....z....._nq..+.#~.%..c..... ..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78971c5f3b10669d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.4978824196153955
Encrypted:	false
SSDEEP:	6:mJ1/VYcvhAbuB4h4uKzs2buBSgw1LYt8bF5PbK6t:+9VJuauo0s51
MD5:	8A23AA6577A31C363ECDFB690D348194
SHA1:	8236E2B3D727BCE880167344024AE0028DF188FF
SHA-256:	7437D0000AE1F3B2B4494E0AB47822E8B4C657E9BFEDF643F377AD7C1639C856
SHA-512:	EB789E74158ADF8C3D3C3FE075E5ACAF4D9C0B84C92C8F9733FB81D57B0F28A38BAE71A7BE6AAAA16310076D25B14198741690316DB6A3E09E45FEDD5645E1 A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a.....ea...._keyhttps://assets.paperturn-view.com/components-Tooltip.d369b3de.js .https://paperturn-view.com/..{.W&/.....gO..g.m. ..q.]....CF.`=..*.6.. ..A..Eo.....6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78ec281d449072c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	345
Entropy (8bit):	5.8792102489469125
Encrypted:	false
SSDEEP:	6:mUYYcvhAbuBfm8s2buB9Ktgil5g7DVyAgK6tWo/82emkzLsc0KMYiCStHg7DVyAR:EJN0LK5EHVy1wo/83BPD0KMYnHVye
MD5:	84C6F5CB554F45C2B637BB615E2994CA
SHA1:	04009A702317C4242E0DE20757A9F38327FBCB47
SHA-256:	C7C6337393325C2CDFE0DA4E5E33F3AB7FF0C261F643CFA57F9C3444C775BF72
SHA-512:	080827EFF2E465086AE18D559D60D7F8961246066F87C15C686BCE7DC999C5C94F73CBBCF33A45DD99AEF11B2E47865DDA1CAE3842A24E26DE9B59E8FFA9B5 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....Y...._keyhttps://assets.paperturn-view.com/12.dc063ac5.js .https://paperturn-view.com/ .\.W&/....._.H..._.....K....iosD.gT..C...A..Eo.....}..f.....A ..Eo..... .\.W&/.H...8389C906E744D8A135784F72A1F058BC57213A6C3D384DFC165AFEF5F291D058..._.H..._.....K....iosD.gT..C...A..Eo.....mt4.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7a24f279f3c8e97a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	640
Entropy (8bit):	5.59352073339948
Encrypted:	false
SSDEEP:	6:m2XYcvhAbuB/KSXyc/blytMSgORs2buBlgiXcL+AvwK6tW2XYcvhAbuB/KSXyc/Z:3JNKm6MQ0D0+2SNJNKm6MQ0g8+41
MD5:	9404BFF386371657DA5423626768B82C
SHA1:	DA91C3670663CB6ACA57F7BFA36DC2AF9CB00619
SHA-256:	B26886FDCCB4665B189E74B8055DBA59F2662441125B329DDD41BCECC9788D80
SHA-512:	CA96CAEADC0563DCDC6D6D234E07316C7A8B9308F1ADDD267C0501C21F623C395F45756CE764203DB6FC2BFFE840FBC41369503110FD7E3719363876DC0E72
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://assets.paperturn-view.com/vendors~components-AddToBasket~components-Alert~components-Basket~components-BlockingPage ~components~b32f8ea9.41aa8c5a.js .https://paperturn-view.com/,ge.W&/.....E.....G....y.M.]d.....q|-o.A..Eo.....J.....A..Eo.....0\r..m.....o....._ keyhttps://assets.paperturn-view.com/vendors~components-AddToBasket~components-Alert~components-Basket~components-BlockingPage~components~b3 2f8ea9.41aa8c5a.js .https://paperturn-view.com/.(..W&/.....R....."E.....G....y.M.]d.....q|-o.A..Eo.....^Y.I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80d379f7f5b93e31_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	545
Entropy (8bit):	5.524706577381669
Encrypted:	false
SSDEEP:	6:mezs6EYk+tHh4Kk6s2btWMg9xccqiH/YpyhK6tmgEccqiH/YAa6ugrBccqiH/YQ8:o6U+tHh4YyOiHTliHxWiHlEiH2AiH
MD5:	76FCF113E5087320F299D68D4E7C57D7
SHA1:	0F7474467C0378A4B7CAF94FD4206C65FFE86C38
SHA-256:	FAE05E851FE4B443D29C96AC2410E999741F2FF0CA38443E59A8F2C9B2CEE6BC
SHA-512:	1A3AE1E27345E0F2FB2A2B8BC03F4010BEAEA59212D66CAD50F337D1CDF3825F7C33EFBBCC0FD200FD5C0C86B65A5EEA073E21CFD224DECA2B5685C4D3848 1D8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....E.R...._keyhttps://static.zdassets.com/ekr/asset_composer.js .https://paperturn.com/s..W&/.....*.....[..z...\.t.O.&....P...VX..Cs..\.A..Eo.....,.....A..Eo... .....W&/.....Q.....[..z...\.t.O.&....P...VX..Cs..\.A..Eo.....0..*.....k`.W&/.....[..z...\.t.O.&....P...VX..Cs..\.A..Eo.....x.uj.....b.W&/.....[..z...\.t.O. &....P...VX..Cs..\.A..Eo.....m.....W&/.....j.....[..z...\.t.O.&....P...VX..Cs..\.A..Eo.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8140b5c475fbdf1c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	623
Entropy (8bit):	5.425356890061851
Encrypted:	false
SSDEEP:	12:dUOLE/33+71xsP/u+RsU7y1Vt/u+Rq5Xi1n/u+RP1ol/u+R861Tlf/u+RDU61DlJ:4/33k/sP/GU7yl/liR/RE/O6dt/1U6N5
MD5:	D812E1B250BFD3521961063343150BD0
SHA1:	32B884D46F91213B47C97D38A90527EB255F1F20
SHA-256:	D74A3E071FF50CFF2892E3BC726FBE385DC01AC8F15BD6BD523A03CB406E07FA
SHA-512:	2666761D5BC277E622270467EE136F229060E92B34C6A9BE9CB909376A5DEC0C4E619AB8808A663F54B5C20AEED5189D981762C089C32EAD02521D4F5657B3F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G....._keyhttps://acsbapp.com/apps/app/dist/js/app.js .https://paperturn.com/.4..W&/.....c.....b..WQ47.>\.J..e.K#.!..\4.....A..Eo.....b.....A..Eo..... .....4..W&/.....b..WQ47.>\.J..e.K#.!..\4.....A..Eo.....e.....4..W&/.....?n.....b..WQ47.>\.J..e.K#.!..\4.....A..Eo.....3.....4..W&/.....b..WQ47.>\. J..e.K#.!..\4.....A..Eo.....H.....4..W&/.....b..WQ47.>\.J..e.K#.!..\4.....A..Eo.....%.....4..W&/.....-.....b..WQ47.>\.J..e.K#.!..\4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\823f8fc18e89de25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.70465334362172
Encrypted:	false
SSDEEP:	6:mxYGLibtGqtIelRs2bt0QDugOXxe5UY0DK6t:4quelRDiLJ1
MD5:	5E6A064066501A6404A17A93EA1DF64C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\823f8fc18e89de25_0	
SHA1:	59D0A5527B999A2A7DE578AF8CA11778CD2267D9
SHA-256:	92E53743184BFD3B77A8D159723F9CD613E65B17F30CEA6A84648113AA31B199
SHA-512:	A2CC1741E27490C36E3F89E5F0D938D4207DF7CB669099076423340E1E7A6BB56559C06274F3442641C09456D7C3BBFAAB47D90EB975D25F329F4DAF8F359BC9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...n."...._keyhttps://www.paperturn.com/cache/v2.3.12/mini-5a97efeeff018a0419f17b6689972674.js .https://paperturn.com/..k.W&/.....j.....2...3..N. .hF.....O.A..Eo.....X.T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8421b1b3082ac36c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	470
Entropy (8bit):	5.6020510631814515
Encrypted:	false
SSDEEP:	12:0/JuXs9QWFz0lwJDvYkHP6/JuXs9QWFz0HswJDvYkHKsT:wRGGlPqR3GlH
MD5:	2EB48BFF929A07AF08EA44C1F1342E83
SHA1:	CC7DA02F6BD8A7104F32A5803AF425A014B23EB5
SHA-256:	C60CBC3743E27100E54DD360653D4176FDF9B3627B7ADEFF51CF63B5DBE86EAC
SHA-512:	A0FEFF481FEEA2441C09567A36570FC179E03E9F4839634849DEB5590D21AC35BA13E3923D1DC07CD7C500EF733EA008D41FE58CC214C2C335FC938799D5452
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...l..{...._keyhttps://assets.paperturn-view.com/components-ErrorBoundary.3ef6552e.js .https://paperturn-view.com/..b.W&/.....l..&...X.a7...|UEg.....b. .9.G.A..Eo.....X.....A..Eo.....0\r..m.....g...l..{...._keyhttps://assets.paperturn-view.com/components-ErrorBoundary.3ef6552e.js .https://paperturn-view.com/. ..W&/.....l..&...X.a7...|UEg.....b..9.G.A..Eo.....(.k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\859d57729f30e053_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.5893133213756325
Encrypted:	false
SSDEEP:	6:mtYcvhAbuB4Y3WKzs2buBPygysS8YT6AZsK6tWtYcvhAbuB4Y3WKzs2buBbuygcE:0JuY3l0bYGn6JuY3l0tuvYGLT
MD5:	834CE5A8A4B2BB9ED29D368FC8EDCA97
SHA1:	A4F91405EDB0469B1FB47272720AB9411EA19D0E
SHA-256:	9BA3DEEBD3CFA9220091253824AFD62AB430F30046BEE16209D3A0B033F96679
SHA-512:	B925196AB1370F2CB4A1D572FEC0202D0267A3B6476EC543A07F3DABC492EF8571118A78185E58E987F2EF0CA64C40BE0C31195545E7ACC7F0A00D2582B2E085
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....?.7...._keyhttps://assets.paperturn-view.com/components-Styles.e7b2b5dd.js .https://paperturn-view.com/{8r.W&/.....Q.....g.....5FX..@.~...b...J7....a.. A..Eo.....2&r.....A..Eo.....0\r..m.....`....?.7...._keyhttps://assets.paperturn-view.com/components-Styles.e7b2b5dd.js .https://paperturn-view.com/U...W&/..... .....S.....g.....5FX..@.~...b...J7....a..A..Eo.....G..(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\878756e158c08974_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	170480
Entropy (8bit):	6.203814751146289
Encrypted:	false
SSDEEP:	3072:xK25x4AMhS3MPmaQ4+/cAuZKYa9PvfI4hGT6inQQddy:82KPm4gzY6B6fRddy
MD5:	AA80529BE26D226942F5E6D0756CD316
SHA1:	1D98423F0111CDABC7D0290513C2A842D0E3D2E0
SHA-256:	6464700AEF9C08656C71A2369E16AF6C5C05CDDF42E9C568FAEDC741DC5ECFA0
SHA-512:	ACA1EDE93EB8D72F0877CB2CA4BFA3BE0FB3FAD9FF6BDD57C8F601CC76F30C54190162EFEA2D8FA7836944EADF855848B7FF334CFE295C9A190A6B6A65EDE 4CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...^.....8389C906E744D8A135784F72A1F058BC57213A6C3D384DFC165AFEF5F291D058.....'.....O7...@.....p.....@..... ...T.....l.....|.....p.....4.....|.....(S.]...`n.....L`.....Q.@fr.G....window...(Q...`@...._\_L OADABLE_LOADED_CHUNKS_....Qb.5.%....push.....`.....L`.....`.....Mb.....`.....a~.....Qb...../qGLC..Qb~.....02tDC..Qb.Z4.....3uHEC..Qb...n....4GVaC. .Qb..um....58rzC..Qbb.....5l27C..Qb...=....AZXiC..QbrE.#....DHZpC..Qb>2.....DXALC..Qb...2....EtmHC..Qb.F.Z....GsHdC..Qb.WC.....IDU+C..Qb... ....IOplC..Qb.8)V ....JmTYC..Qb..{.....KiHeC..Qb.....KkK4C..Qb.....Lu7cC..Qb.....OoD+C..Qb...\....RkXmC..Qb..&....cqR5C..QbFo.....ctS7C..QbR.....hGZ5C..Qb.y.....jrqJC..Qb.5Z.... .lf30C..Qb.%.....m2f9C..QbJHP.....nZn8C..Qb.=N.....oOYKC..Qb.....q72ZC..Qb:.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8936c0436506fed9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.580214739740404
Encrypted:	false
SSDEEP:	6:mmTXYcvhAbuB4sLPks2buBPygHXYMbWxKZ9nK6t:TJugk0ta4bp
MD5:	53EA4D652233A19CBF0986981BD54C2E
SHA1:	78FA50229125B73D44F18AC516EE0C2670F70270
SHA-256:	4BD773D866B51EB76C3697732A8EA26B8CD9F54C160715608AE265A56930E710
SHA-512:	58BB9BFC8373CE6678773340E908D98363D7E7887B12CA871997231AB621EA3B733818C07FB12D1906E1E277126D0D71A2EBB8B8275C322D22A040BA08E92CD6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....F...._keyhttps://assets.paperturn-view.com/components-ToolbarIcon.687326a7.js .https://paperturn-view.com/..x.W&/.....H.....J...R..5.8i.&.....'M.g 1C...A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8959e7f160a77ede_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.666849382989875
Encrypted:	false
SSDEEP:	48:g9EjQaSm9EjoEam9Ejx0m9Ej9u/m9EjU4m9Ejhj:1QrKYKn
MD5:	247BF292A331862DA1C1C6189285F218
SHA1:	ADDE55FDCC0D7E605A970A33923B5A7A9F520130
SHA-256:	01A8FDF807719B8560129A13679BA0704B8E47FA32709E2B4A11B8BFF525FC3C
SHA-512:	1D5C099BBD671651F73EEB0AD5531C656D631A87AAD2A5C35AC1526A5B75590DE044CEA06459EC45EA0B343F1B0482EE976459196F922D411ABDCFDE406A5F 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....._keyhttps://consentcdn.cookiebot.com/consentconfig/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/paperturn.com/configuration.js .https://paperturn.com/e... W&/.....# Cl.{.....<,\p.X.'..h$.....:.A..Eo.....d.....A..Eo.....0\r..m.....3....._keyhttps://consentcdn.cookiebot.com/consentconfig/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/paperturn.com/configuration.js .https://paperturn.com/.>F.W&/.....# Cl.{.....<,\p.X.'..h$.....:.A..Eo.....3.I.....A..Eo.....0\r..m.....3....._keyhttps://consentcdn.cookiebot.com/consentconfig/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/paperturn.com/configuration.js .https://paperturn.com/id..W&/.....tn.....# Cl.{.....<,\p.X.'..h$.....:.A..Eo.....A..Eo.....0\r..m.....3....._keyhttps://consentcdn.cookiebot.com/consentconfig/15dac99d-cb99-4df3-83c0-6e8c10ac66d8/paperturn.com/configuration.js .https://paperturn.com/M&..W&/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d4436abab9cbffc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.501108649011263
Encrypted:	false
SSDEEP:	6:mYeYcvhAbuB4cNQUuRs2buBitgus/lldVLDBSENr4o5RK6t:F+JucNCR03lrhNzr
MD5:	5FA5CBAC01EA6CE1A7DEBF8B40D57ECD
SHA1:	AD0A8BA43398CC9A660A64295A28AC58A01C61E2
SHA-256:	04A6F38EAB4656FB40F70B68BB9A69D19A942A6F5A16199E6DD415CB36057B54
SHA-512:	C1078EDECF061EEA542FFD07F8E001663218C7B6B1A090A5A434EA6FEB4C21EC252C10CF33AC7BA596D6CDE3D347EBF8F1936DFA267D2918DA635115A2B198 32
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....o%....._keyhttps://assets.paperturn-view.com/components-Alert.22553599.js .https://paperturn-view.com/.`n.W&/.....B*".mH..X..}.....$t.<.....A. .Eo...../]7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e8595a5d4720c28_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.699302458141952
Encrypted:	false
SSDEEP:	6:mAYYGLibtGqkS1Ez7ks2btgbKvtgPkiKSM0v/dK6t:2qgzgMbKikiKS1f
MD5:	A5D81F18605593E4DC566CB14EB4578D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8e8595a5d4720c28_0	
SHA1:	78BC98ABE21391D874B97B384CEE6DCFD3E91838
SHA-256:	C1CE03853E6EAAAA9B65D72013D10602C8A267B57CC367AB99BA0BED3D0B290B
SHA-512:	BDA53A273D5C20BA7FA4D066F86FE5DEC3E7436EEFD5946F8CCBA14C31400C87F867B3F57BE0EFC7F026A815CA5ABDA3CBA6CCC91C284C06DA5EE45BF9C6 0884
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l.... ....._keyhttps://www.paperturn.com/cache/v2.3.12/mini-af8546ccbc09deec7e6b7a04c8502a92.js .https://paperturn.com/d3..W&/.....m.....$...L.....7...~.... .)B..'..C..A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91b9b5ff6833c0d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	98088
Entropy (8bit):	5.942967621197124
Encrypted:	false
SSDEEP:	1536:p/NHbZHKH0cfuUzfbHLFn+5RxJmKGcEc6DnPViLAcIRNoCbhdIcBwBHzs:pB6023zHLF+5gxcEc6D4NMdIcBw1w
MD5:	9C808A9D225536F8D4BB6F7C644E5BA8
SHA1:	BBBAC35E1E8C9B4ECD92A7BE26C7FA2F61657CBF
SHA-256:	FE093A51056C6513CE5EF1C7490F63D7D5966984BB45694EC5D86E4A50C77BB8
SHA-512:	7D385AEE4B6EC8A8858CF632F046D46AA9BC92900F0976985C2368CFD51D720865CE6AF68696C88150A6EF4A7D5760BBD69B5F109812DF6D28DC70CEA6DE8E D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...Hv.....8A34A66321308543B62F72F0751030C47E71FF01705F36D714FB0C0F9194AC13.....'.....O"....}.....((.....H.....p..... .....8.....(S....`.....0L`.....(S...)(.`.P.....L`h.....Rc.....Qb~d.....w.....Qbfx.....oe....Qb.....Wb....Qb.qTu....K.....Qb&. .....wa....Qb"8.X....r.....Qb.f>.....Oc....Qbr.....Xb....Qb.#w.....pe....Qb.cr.....Yb....QbR9:Y....O.....Qb.[.....qe....Qb...F....Z.....Qb.}.....$b....Qb.....D.....Qb..K ....ab....Qb.....la. ...QbN.....ac....Qb..;%....x.....R....Qb..Z.....B.....Qb:.b.....Nc....Qb.._*....E.....Qb.....Y.....Qb..t.....fa....Qb*.+....bc....Qb.....C.....Qb.....$a....QbJ.....Za....Qb.....bb....QbZ. sQ....Na....QbB.....re....Qb.sC^....Zb....Qb.u.....te....QbZ.....ya....Qb..<.....cb....Qb..c.....pa....QbB.....cc....Qb..g>....sa....Qb.X.....db....Qb.</.....Ra....Qb.^S.....Qc....Qb...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\95fee99bab72dc0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.564605602535899
Encrypted:	false
SSDEEP:	6:mVltXYGLUxGBznGKT2duguGxZvtgH6XEOklBVhnL+nK6t:AwGBR6lguGX/UOkRN+
MD5:	340821E5AB3BDD4B9735C5B3A1A971EB
SHA1:	E8A502F73980090CEAF9260F3D2F3881EA0BFCCE
SHA-256:	16804A94446A6E24D59F7E7B79432C8E72D7DF3174EABE59DB2EC746DEB77240
SHA-512:	60C8FFFFBA9188E8DF0D9378D89299DDA13CC5DBA02050814B902D307471225595E9F48BC509E6D12596A2DD4C43420C5F9816EC7DBC4D47C1F7509898D6A26
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....T....._keyhttps://www.youtube.com/s/player/3804dce2/player_ias.vflset/en_US/base.js .https://youtube.com/....W&/.....pp.....M.x.7.3.g...Bl7..9..|.Cw.o.9. X..A..Eo.....,*O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98f7ac3352864cdd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	506
Entropy (8bit):	5.517868925878412
Encrypted:	false
SSDEEP:	12:gJNKO1b805sXcyo0E+m6Qqtl7qJNKO1b80Icyo0E+mCYY:XOV8BX5o0E+ttl7tOV8Po0E+8Y
MD5:	6209398C629A006D6EBD44777F66E8EA
SHA1:	B86EE0CA05A457377DE295E3B7E5E4FA9F3AF905
SHA-256:	DF80806AAFAA37E902C86A208F08EFF3644075D65DE3EF4D4CBA713E5764F644
SHA-512:	F740E9571FBCF0B35D0AAE6E5D1C44B6517C0B28EB1D6F95488B7DE2475FB260551CBA148289934156F5B4B3945148611945B69DDF6053D79D21C5500DA465E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....y....._keyhttps://assets.paperturn-view.com/vendors~components-Pages~components-Search.4fcb49bb.js .https://paperturn-view.com/@.x.W&/..... .....v.....kz.<Adp..*E.2r..GaT...A..Eo.....45.....A..Eo.....0\r..m.....y....._keyhttps://assets.paperturn-view.com/vendors~components-Pages~components- Search.4fcb49bb.js .https://paperturn-view.com/OA..W&/.....v.....kz.<Adp..*E.2r..GaT...A..Eo.....n .}.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9aeca2548873487f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	353976
Entropy (8bit):	4.121726950379738
Encrypted:	false
SSDEEP:	6144:yHyGURF39jLLzg1FK3oqQFVLzFCfu1uVg:XQFvXf
MD5:	78E233A563F1D56617D30E83BD60233F
SHA1:	82E9F1CCCA52FE9A3FE3173CD28099BB118C4449
SHA-256:	3C209DC0507F8B8DAE36EBD79576F5C9CEEEA533C84E98B25490774C39A7E858
SHA-512:	2B34B381A5B80BB5023D03F7BF5628BF4FF74CBC93BA632E529D0A39A15C8F33959DD64828886A0BDCCED6163C7192FD37F98266820D413DCC9EA279C7159AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...p$.....8E88A35BD36F53D98288D14D5E501E2F584B9B2AF358BA6A88F63A1F7303D98B.....'.G.....O.....e..[.....D....d..d.....4....(S...`....L`.....(S...`.....8L`.....@Rc.....Qb&T.f....d.....Qb.....e.....M.b....d.....I`....Da.....(S...`.....L`....I..Qc.R.....parseInt.q...Qd.'.....fromCharCode.....K`....D{ .....i.....&....&...7..&.]...&.]...&...8..&..#j.....&.(...&.%.@..&.Y.....(...&..$&.Y....4.....,Rc.....`.....aJ.....e.....G.....@.-....\P.a.....P...https://www.paperturn.com/cache/v2.3.12/mini-b6b0e1e2a9cc4a10cafe9a7b0396818b.jsa.....D`....D`(...D`.....`....&...&..!.&..!.&.(S.,..`....].K`....De.....&.%.*....,Rc.....l`.....Qbb.2D....k...a.....b.....1.d.....&.(S.(.`.....L`.....Qb~..Q....\w+...K`....Dd.....,Rc.....`....a.....d.....`....Dl]d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9bec16c4529e250a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	454
Entropy (8bit):	5.564515944967586
Encrypted:	false
SSDEEP:	12:FtJuNt0TpIHPPEX5wPtJuNt0rmHPPEX5ip:6tspIH3EiAtTH3Eop
MD5:	3EF19B8EAA74511294F841A18AD89C58
SHA1:	DABA9ED71609F7BA20DA40F6CC64451778799DFF
SHA-256:	37F08BC67BC8FB878EA87E114A2651C3FAEEBFD86A0743E4E3200F482155603A
SHA-512:	A14019EF72993958D2A96A194FB19D507F95D2935AE4BA863C544F3962426BC5F293F969FDC7DAAA381A9E63D683568CB9D3B9FA277ADDFC5B0CA911DFE6E825
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....$....._keyhttps://assets.paperturn-view.com/components-Pages.5c372095.js .https://paperturn-view.com/P.x.W&/.....]...T$.BB.;U..=)..@=...)..Sd.0.A..Eo.....R.Rf.....A..Eo.....0\r..m....._.....$....._keyhttps://assets.paperturn-view.com/components-Pages.5c372095.js .https://paperturn-view.com/.A..W&/.....]...T$.BB.;U..=)..@=...)..Sd.0.A..Eo.....MB.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a07811dab2c1a983_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.531377111764403
Encrypted:	false
SSDEEP:	6:mVIEYcvhAbuBV9XYSRs2buBnWtgLVslNnk4KK6tWVIEYcvhAbuBV9XYSRs2buBsi:CI0Jz1bR0E2sXk/UI0Jz1bR0HsXkb
MD5:	E079C0A6786BEE30F511A972AE41BF7A
SHA1:	ED11C6B72AE2041B7588810ACB27AB95057685A6
SHA-256:	51135D37656A0F1E8CD5A4CE2699A8C5F0146FF1C08B4DDEDDFEDA248A83AE65
SHA-512:	A955028E7360D27370EC089D4513D050AD6E6A589A7C03F9641651A16703DD1EE91193006C33B59448D6D776CDE5A44B8B7344201B6EFA9E4C6DF2E79B665C80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....3....._keyhttps://assets.paperturn-view.com/7.0f628dc6.js .https://paperturn-view.com/..\.W&/.....u..(...e.../.:)...q.$\x(.t...=.A..Eo.....!.....A..Eo.....0\r..m.....P....3....._keyhttps://assets.paperturn-view.com/7.0f628dc6.js .https://paperturn-view.com/....W&/.....u..(...e.../.:)...q.$\x(.t...=.A..Eo....O.P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a2a9870c369aa42b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.591537159900901
Encrypted:	false
SSDEEP:	6:mdtXYgcOEQfu9a/Wn/bWnSsN3Lqug1rWefYXplbK6t:uckkQyWnxLqLWsKLN
MD5:	DF292C4865279697D7F067C261DA7898

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a2a9870c369aa42b_0	
SHA1:	455E111D4AEDC7C6274BC4D9E36146AB47992714
SHA-256:	8F8EB144CEB6CE79669AD648BF798180674CA0D7B395957098FD4BF09390F2E0
SHA-512:	357AE191B52E9173BFB6E6BC211417C5123038AD57256C0FE09481E4B0414C4A48FFCF6DDDE1EBE29D09F53BA90F6F680905FC0AC5C63E972942D86541BF1B5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z....%.^...._keyhttps://spoprod-a.akamaihd.net/files/odsp-next-prod_2018-11-02-sts_20181108.001/require-a19851d1.js .https://xpans.in/..r.W&/.....Q..... ?5.....r.2,d.O6pN..GZ..9.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a2df7e764a389255_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.4759910476283356
Encrypted:	false
SSDEEP:	6:mU6EYcvhAbuB/KSlYoNRs2buB0tgb9l0TF+hfqRK6t:p60JNKq0KiaTF+pqr
MD5:	4DC9F0F469C4B3C66A61ADF8C8A9AF11
SHA1:	38CBFDC52DFF79433423BEA58BD124CDE63B2FED
SHA-256:	767ED770A1BE954AB817EC56E715BBFF649D0B23CE5039231F572BD4FA7CAC1E
SHA-512:	EA24C5059F9549024E7594D3AF49D1CEE767DDCF19459C05EE29F98E76A952AD8C5B06C5FD45EAEF6CABD94EFD03935243FD9AF318404215CFBBBBE4E1F38E 7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...f.Fp...._keyhttps://assets.paperturn-view.com/vendors~components-BottomBar.e724eb41.js .https://paperturn-view.com/PEt.W&/.....R./>.].DN.{ +mA.L.....f^.I+.@.q.A..Eo.....~3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a3b9cf33e4506e9e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.46301282753867
Encrypted:	false
SSDEEP:	6:mytgEYcvhAbuB48yHabbs2buB32goRMkTplK6t:vvJux6/0k7TN
MD5:	8C3DBDB5C1181E478F6F3BFD4AD8FFEE
SHA1:	2A42803BBC60ECF4A1B7AD861701C2F3FB26F2C3
SHA-256:	0A218717D96E048931262C2116BA8AD91BBD637F898FBBB3EAFA770B1F834E56
SHA-512:	68D56B1EAC76EEA69556003C433125893EC5040D86FDF9FB5FE77F56F4CE175E039366EB5EF2CBA8017010F94910F1AD3C276349C5A70C92444CF6F2FAB5B0A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....._keyhttps://assets.paperturn-view.com/components-PoweredBy.81832c27.js .https://paperturn-view.com/uVn.W&/.....t.....^..so}.-.....'..4..X.j... .A..Eo.....1.a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a6de80f86bf10fb4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.560093072536592
Encrypted:	false
SSDEEP:	6:mwmYcvhAbuB449bMIL0GUos2buBteNHgDUAs6tlmrNTnK6t:PmJumtL8o07AXUcZTp
MD5:	9B01A0DC8468E8CA6CB8F95D7D656EEA
SHA1:	6435D88CD163E10083BEBC1C4EB112046587E1CB
SHA-256:	A8E15FCC4C5B68F02E23E266597E1AD5D8DE709E49759B88253FEECC0D1018B2
SHA-512:	4CFD2C71D6C03886E2418C4E501427EF00D0BE73B713E72E677847ABB5AC380D80DDBCEB3F6A04BE37DCA192E2A71F1350D4E8AA926D6B5468355AA4FC0B48 77
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...#.._....._keyhttps://assets.paperturn-view.com/components-EmbedFullscreenSwitch.b1cc3074.js .https://paperturn-view.com/.:..W&/.....W(....g. vC.:.."UsG.n[.n..I."J.A..Eo.....E3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab2e7647897bb5a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab2e7647897bb5a2_0	
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.54179192846904
Encrypted:	false
SSDEEP:	6:mR0EYcvhAbuB4PpjgvNRs2buBHSD+1tgIbIGPbg41JhK6t:u00JuhEz09bpbgo
MD5:	663DF95C003348D1B0366EC716957C3E
SHA1:	7323F6FBFB24B3BCC7E06292450D5E969DF12EB0
SHA-256:	A4ABD3148B86A80FF8689574021630B88B5723B29225AE573DE26A9CCD533663
SHA-512:	E7E47F8B8C50F21013E0F40896A443AFA36BFA108229AC52D5EF1EBAC1049169EFE2AD93CCABB1A90E911ADE118C825CA6C1E7736AEF8A8120004690944EFDAB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....._keyhttps://assets.paperturn-view.com/components-Preload.8e1d07ba.js .https://paperturn-view.com/!.k.W&/.....F..y.]...@I.....qjq:..cC....I.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab9b9b92e56d5efe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.479560551570538
Encrypted:	false
SSDEEP:	6:mNyXXYcvhAbuB4EQRs2buBWFgb5ceYvYZcnK6t:JJu50Ge3cp
MD5:	C7D001491CDA1DB50E59CA967B5A9C45
SHA1:	3BF241BE8A4CE8B0B2C19F232C74B5F2C8AD67FD
SHA-256:	F2917578E8F3BF6D031F9E4513E3726DB0093DAB87E57901653B77BCC9159377
SHA-512:	BA59F84CCADCDE99211804DB807F5D723DDB1C6CF8091A51D25A6D340C92D294D6664C48C39F993FF6617217A0E0F7CBC884BB62549E52AC922BEC8791763F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....._keyhttps://assets.paperturn-view.com/components-ToolbarButton.4ce3af8a.js .https://paperturn-view.com/@.x.W&/.....>.....*..... X./.rh.....\....8...A.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4191926631e1e0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	578
Entropy (8bit):	5.609303466251818
Encrypted:	false
SSDEEP:	12:PJNK/OlD24R0M193Gy79JNK/OlD24R0l2193GUi:O/OlD2uZssQ/OlD2uZsUi
MD5:	F81D94E1EDD077F53626F5D6C1DC0619
SHA1:	FB2049514BBDAEE4A855E7F1D6960B0B29B50C41
SHA-256:	12A67270FD885E1F633A0B6D48A5F2237D6EBEA4C9D5730422EB63AFF4CE5FF9
SHA-512:	FDA0809AA2246A15CF2DCF40CACFBCCE82223F851F5F44825930DA2F32A9F2167786E65885A3CC2DFA0B234C5C36434AE630C89E7457590708DD5DC5ADB6C19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://assets.paperturn-view.com/vendors~components-BuyBasket~components-SendBasket~components-SnackbarProvider.39ec3713.js .https://paperturn-view.com/..f.W&/.....C.....F..=.;~.....m.7j(...P.A..Eo.....P.....A..Eo.....0\r..m.....r....._keyhttps://assets.paperturn-view.com/vendors~components-BuyBasket~components-SendBasket~components-SnackbarProvider.39ec3713.js .https://paperturn-view.com/.)..W&/.....F..=.;~.....m.7j(...P.A..Eo.....g..O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b868e2287919f738_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	6.325424734669373
Encrypted:	false
SSDEEP:	6:mjIEYELaKJQFtaxiR1z52pEjkJry6YgLqrRUNsQ9qS2tDnxgL+c3nLUgmnoFUOK+:P0LaK6axo8JryvgsU7YSwuT3nLuno9
MD5:	FDB338562A9845C548390C5C26B079FB
SHA1:	66F4F853BB70C91A2089B40BA966718698F604AA
SHA-256:	138C370A12F2040DBC2A94DB488E60FE3437E882F275DE0C35F334C4D4246288

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b868e2287919f738_0	
SHA-512:	76F2759C19A1ECA5606FA037EE437CF141CE56ABEE0B7471401B8A5B6711000F529CCF3B3612BE57420952B148D6381A5A628CB2AE79D075C34D5BF86D2CEF2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://xpans.in/document/Drive/asd/ScriptResource.axd?d=P9Sp2kK_d4BNWXJEemNdILK9AkaZTG86MaHXVWE9ulLLVoOV2_uW1v0US-bX7dmgAnCfaQZZr5Xs_PMb2qlY_PZzJWUXIvFhdqwbDETknzEmfBkVtnOHt2UrW1fhYKSvnNu6LRTwvwsd5-_je6Walguw52MlxQXzYUZD9J954ItjszBMdOwHNUoRr-iIqIr00&t=545ba255 .https://xpans.in/]kr.W&/.....Y".....M}.....(.|.0.S...8.`>D.....A..Eo.....;Gj.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bbfcd0a0712d3aa4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	261
Entropy (8bit):	5.604148725483563
Encrypted:	false
SSDEEP:	6:m3nYgcOEQfu9a/Wn/NziRzg6VN3LrRiHga1yaqaL/I6AxK6t:WckkQ0mRL3LtlaqqQ6o
MD5:	19E2D9DD2FD5ED18B346457A20CA8980
SHA1:	8582F3C8B2C615287409E39D7B20E03E4C2D4B26
SHA-256:	DBF4AC83BD022DCF1B4B4574BE6E1A2282A64DC1AF1C8E203911BA8758755265
SHA-512:	CDCAB9A3791A82E766B2C6179DFFDD72C4D158FBBAD0CEA0D6E9D53F7694744C1B556406CC04A62582AB48D071C91731B55C8C623B5975C23ED3BF376A5C2AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4....._keyhttps://spoprod-a.akamaihd.net/files/odsp-next-prod_2018-11-02-sts_20181108.001/spoguestaccess-f1ac83f1.js .https://xpans.in/..u.W&/.....;...)...,.....J..=.I...;.N.h.A..Eo.....-D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf709059c5fc7310_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.527410248112826
Encrypted:	false
SSDEEP:	6:mu/yEYcvhAbuB45RLs2buBzLugeS4swbdNubK6tWu/yEYcvhAbuB45RLs2buBwH4:XvJu5RL0yRJYNvJu5RL0eBRJKr
MD5:	9480A5B015E3FDB668B47EC83E289F2C
SHA1:	B977199AFDF13570AEC5736E2163D8693847C951
SHA-256:	35BD9F7432D76ECA74BB62EEF6DB3CA178CEF99CA02DB40E1D42C74E682BB5C7
SHA-512:	2C000F67AB231CE16691AF4C2DD3C6D45BA25C657D25EF964749EB7CF39F95074DD4E8F752BD858E6732418416E6D33690B03530317873CB52DA9A6530E9BB3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....|...._keyhttps://assets.paperturn-view.com/components-Viewer.775a1c39.js .https://paperturn-view.com/.9r.W&/.....].....`Or].A.....U1.H...._.].A..Eo.....A..Eo.....0\r..m.....`.....|...._keyhttps://assets.paperturn-view.com/components-Viewer.775a1c39.js .https://paperturn-view.com/...W&/.....W.....`Or].A.....U1.H...._.].A..Eo.....>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c693e56ec7dc32cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1278
Entropy (8bit):	5.487719356668925
Encrypted:	false
SSDEEP:	24:MoEJRI0JmpOoEJReJArOoEJR48JuOoEJRkzJQOoEJRUJwOoEJR+SJ8:REPVJmpfEPeJsfEPlJufEPkzJQfEPUJ4
MD5:	CE413CAA5F78CDE0A475D8DD009AC7A9
SHA1:	3A6B7F81B985AA9020F47DFD2DF69F268A3AF640
SHA-256:	A962A40D7C50DC454F371804772DA153810DCF26413BCAB437097E6BB6CA28BB
SHA-512:	B98968EBEF86AA73778B420EF38780F6452049F2490791C414F1B7D60EAF77688B134EBE7F6D463916CD4B463DE2849DB2A5BC0136FF4676D67683473C1F1AAA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...X....._keyhttps://assets.calendly.com/assets/external/widget.js .https://paperturn.com/'t..W&/.....~.....p.....LK..W.`F..!E.Z.@9..I..A..Eo.....Ev.....A..Eo.....0\r..m.....Q...X....._keyhttps://assets.calendly.com/assets/external/widget.js .https://paperturn.com/..?.W&/.....@.....p.....LK..W.`F..!E.Z.@9..I..A..Eo.....^..9.....A..Eo.....0\r..m.....Q...X....._keyhttps://assets.calendly.com/assets/external/widget.js .https://paperturn.com/i2..W&/.....m.....p.....LK..W.`F..!E.Z.@9..I..A..Eo.....M.....A..Eo.....0\r..m.....Q...X....._keyhttps://assets.calendly.com/assets/external/widget.js .https://paperturn.com/....W&/.....p.....LK..W.`F..!E.Z.@9..I..A..Eo.....A..Eo.....0\r..m.....Q...X....._keyhttps://assets.calendly.com/assets/external/widget.js .https://paperturn.com/....W&/.....p.....LK..W

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7dbfff3f5d11b28_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	424
Entropy (8bit):	5.576882292689583
Encrypted:	false
SSDEEP:	6:mmKEYcvhAbuBHwPsLs2buB7ugZgmr8xzbK6tWmKEYcvhAbuBHwPsLs2buBJQygUC:E0JqPsL0NfTgpO0JqPsL0iTfN
MD5:	7E00D779B7E59C412EEC50360490125F
SHA1:	7DDEAB34C7168971B926BCEC5988D036FA59656C
SHA-256:	213D1916A834C75B66CFE242621ABF23ACE6B738FB72CB0921B7BDCDE20B93EC
SHA-512:	970B420C76146E2FE3328E5DBDF14CF8B578D090CFD71587D04F161BD603B541F95F30DDD74AC1BA22C5538032CA335A9453B83FADBA33450DB125499ED6785
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://assets.paperturn-view.com/6.f4dbef67.js .https://paperturn-view.com/..[.W&/.....c.....$3x.....).sO&R.....i....d..A..Eo.....8.....A..Eo.. .....0\r..m.....P....._keyhttps://assets.paperturn-view.com/6.f4dbef67.js .https://paperturn-view.com/G..W&/...../.....$3x.....).sO&R.....i....d..A..Eo.....+.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c968078420fe3f97_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.575034352655751
Encrypted:	false
SSDEEP:	6:mZYcvhAbuB/KSXyc/blyQOlyKHBUVRs2buBlag5qWWaLW4/1K6t:oJNKmhOVo0HFPP
MD5:	21D97C685E676615EB6C1A18F0E2F44C
SHA1:	1C04E82F55CF1B1B3620BD4A591C7EF1812B5F83
SHA-256:	72EF2303DE7674E9DA78F26D636CE7CCBD2E33B765BFB2DF00EB4EF8EEF7AD9A
SHA-512:	63E95404F33280C1C707A74FF08D99A121DA0BC9A9448373BD42675806D33F1278BD56F5CCD156F962B4CB6183F3EE1728E6C7B7C5223053CB03BE73109F985A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3.K...._keyhttps://assets.paperturn-view.com/vendors~components-AddToBasket~components-Alert~components-Basket~components-BuyBasket~c omponents-Di~52c89d82.7a50110a.js .https://paperturn-view.com/DWn.W&/.....M.5T..#...V)....d.C..=..R{..G;$.A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca3cacf61e20435d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	5.536227725617456
Encrypted:	false
SSDEEP:	24:wIQazLtBSIQaMtgSIQaCRtwNSIQactaSIQa7tYSIQaTtg:wLaVBSLaKgSLaCjmSLa6aSLa5YSLahg
MD5:	79CFA599D8AEDC11B77883FBFDF37E24
SHA1:	E1622938B129E8717ECD96A2777E616F107482D4
SHA-256:	78E72469146AC63FF0331E940F292CECD76BE09156120469E0BB8DE2C8949E83
SHA-512:	AD2700086442D0A2C10FB986673ACB28CFDD1F7BF24639C975B5EBA8FA755D7A19F31D798AA5C5FEA912A865EC994D4032EEDCF3755637FE377F7BB846F9D9I 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...G(....._keyhttps://www.google-analytics.com/analytics.js .https://paperturn.com/U..W&/.....I.0..w.....~E'5M..T.=b.m^..D..A..Eo.....5.X.....A..Eo..... .....0\r..m.....I...G(....._keyhttps://www.google-analytics.com/analytics.js .https://paperturn.com/..C.W&/.....I.0..w.....~E'5M..T.=b.m^..D..A..Eo.....?ftn.... .....A..Eo.....0\r..m.....I...G(....._keyhttps://www.google-analytics.com/analytics.js .https://paperturn.com/....W&/.....n.....I.0..w.....~E'5M..T.=b.m^..D..A..E o.....A..Eo.....0\r..m.....I...G(....._keyhttps://www.google-analytics.com/analytics.js .https://paperturn.com/....W&/.....I.0..w.....~E'5M..T. =b.m^..D..A..Eo.....~.T.....A..Eo.....0\r..m.....I...G(....._keyhttps://www.google-analytics.com/analytics.js .https://paperturn.com/.R/.W&/.....I.0..w.. .....~E'5M..T.=b.m^..D..A..Eo.....`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb14d97ede8b4cfb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1422
Entropy (8bit):	5.746208547991548
Encrypted:	false
SSDEEP:	24:cLWHBe6LRB+N6LVBd6LKB66LkBt6LClBr:w522N2R2l2E2C3
MD5:	A5C5E810FD57A6FA30040CF9CFF02498

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb14d97ede8b4cfb_0	
SHA1:	4FA0BAD619B410CF26183268B5C2EE431BC5A27E
SHA-256:	0855FDC6AF83218B5FE6FA498D6FE6A8A88234DAB22036C7FE38D92F4866BD34
SHA-512:	2E33A5A50E3457C969A33D91C56B5BD674132016F6A30A3FFE30C012C646CADCC29DFECCF628505E71BD736BF6079E66B79D1B5D5A4F0EDE05DC3BBA33EFDA6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....U.B...._keyhttps://connect.facebook.net/signals/config/808672289198286?v=2.9.43&r=stable .https://paperturn.com/.&..W&/.....*...R...=....pz.n.%w...1D..#.A..Eo.....6.^.....A..Eo.....0\r..m.....i....U.B...._keyhttps://connect.facebook.net/signals/config/808672289198286?v=2.9.43&r=stable .https://paperturn.com/..G.W&/.....3.....*...R...=....pz.n.%w...1D..#.A..Eo.....A..Eo.....0\r..m.....i....U.B...._keyhttps://connect.facebook.net/signals/config/808672289198286?v=2.9.43&r=stable .https://paperturn.com/u8..W&/.....m.....*...R...=....pz.n.%w...1D..#.A..Eo.....x.....A..Eo.....0\r..m.....i....U.B...._keyhttps://connect.facebook.net/signals/config/808672289198286?v=2.9.43&r=stable .https://paperturn.com/.:..W&/.....&.....*...R...=....pz.n.%w...1D..#.A..Eo.....D.....A..Eo.....0\r..m.....i....U.B...._keyhttps://connect.facebook

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d1d96ac840cd7ef0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.921737387086463
Encrypted:	false
SSDEEP:	6:mBPYGLibtKFANFoCQOB8As2bt89HgLRl/g9QO1kYsSK6tMCiSpE8QFmlVmIO1kYY:0p6N2TOBxg9EI9bW9SPuqB
MD5:	10AF160B3376A79633047ECB7C34A400
SHA1:	895B87856B76E9AEF9BEA0B7423CDA5A24EFCD3B
SHA-256:	0563A5D9D3A3C960CCFAEF17A2FA8B60C5C645096C20536512FCA4497B299001
SHA-512:	26C78DC8DF5E77FE8BCFA2FDC766107902E74BEFA5DD64DF67A5F22D806A4608205F2117E669AD6D0D6C12256A562A6DBD235E517D75FD3CE4E6CF90699FAB7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....._keyhttps://www.paperturn.com/o3/resource/js/lib/angularjs/angularjs-lates.min.js .https://paperturn.com/..W&/.....]pf.....>..x.1...L/...?6n.*.A..Eo..... .....A..Eo.....W&/..~..8A34A66321308543B62F72F0751030C47E71FF01705F36D714FB0C0F9194AC13]pf.....>..x.1...L/...?6n.*.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d2b8a8d9a2d95859_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.562062884418913
Encrypted:	false
SSDEEP:	6:mU6/XYGLUxGBznUk006guGRUtgmll0WO/prAlhK6t:pKwGBUf06guGW/SWO/pUN
MD5:	2F6A3D1ABA20413216938D9BE8E44561
SHA1:	AAB14B42475D6C1DDF97F52C85AC0791646461E9
SHA-256:	99D2E2E59C49C610B4F4E111DB25345B168DF1CB6BEB79EA1C41CF57DB9FCBB9
SHA-512:	580BB622BF22AA6585DCE9BD60174E5B09BDEC3DC5CAA1B1EAE91766A3C4B4DF7BFCF3E4C6CA5ABC83CD68EFE45E97A08B1410A5AADC31C15B92AC1329E1D3E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....?....._keyhttps://www.youtube.com/s/player/3804dce2/fetch-polyfill.vflset/fetch-polyfill.js .https://youtube.com/H&..W&/.....qp.....6z...J.....tY0.....(..Sf....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d5ef84d81abcea8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	444
Entropy (8bit):	5.604797346491657
Encrypted:	false
SSDEEP:	6:mHYGLSmXZC2jns2buBxWtgC6XfO4z68RK6tWHYGLSmXZC2jns2buBig76XfO4z6K:MZ0k6XPNruZ0b6XPj
MD5:	6B5A6A904AE3A9786348666BA611B5DD
SHA1:	D60A221516BB4A474AAC914C550763051331FE6F
SHA-256:	DD488B696FEE136A1CAFA00B259EAE6477B7D384BF734797426900E10B02A5FF
SHA-512:	C4C508EFC77EAF3E69258336C4F05D0A4FBF123893448E7872E311BE1A652608B25A937C02D5A903649B499C865680DC66A393C8849066BDDF6E1DA0523A2368
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d5ef84d81abcea8d_0	
Preview:	0\r..m.....Z...p"....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-47719712-4 .https://paperturn-view.com/..S.W&/.....0.5}1.....:.z+..".....O.b..A..Eo.....:.....A..Eo.....0\r..m.....Z...p"....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-47719712-4 .https://paperturn-view.com/.?..W&/.....0.5}1.....:.z+..".....O.b..A..Eo..... /.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d80a1cc1e7bfcfc1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	338
Entropy (8bit):	6.117126609709782
Encrypted:	false
SSDEEP:	6:m7llXYELaKJQDmQQy/OWQlxDEU5US0LCUBc+erRVL0FgnvJt6K42iDK6t:iLaKizGJF5US2KrRVLRt6p1
MD5:	071031922354AAF101007464D61B1EA2
SHA1:	5161766A8377831A01D1B8AB7B0E85DBCDA5B6A9
SHA-256:	665EDE2960A3FE2A407C6419D9614E9DF8F157AD9F1DFED2A7C4AEC82C9399E3
SHA-512:	E30424D5CCC1A0EFFED946FE7B24B6D5F2709C731121B0C837A7C0ED83A330CD0974CF3F5E7386105DA7441E831BC07ABCA5DAD8E14F1AAD3C01FC334230F 66
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]>...._keyhttps://xpans.in/document/Drive/asd/WebResource.axd?d=Vseh0_O29CS6SASZGjJ5B50eCxofIEK9mDd5NZNa5k8KtiJMrh6DL1CqUg bSMvuYp9XMuEXY1onzPRs6Z1nFvYLL4ESa9mSIGj7DzvVHhP41&t=636686402738678653 .https://xpans.in/F.p.W&/.....T.....r..PGE.NDA...b3.....:j....@F.A..Eo..... .t;k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ddf29fd5d7ab777f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.8843265360354104
Encrypted:	false
SSDEEP:	6:mGmXYGLibtGqlIEvSb4s2btiA+HgvtlW0OkbIahfK6ty9Msx7u8cDgNWOkbIahyl:PmtqlIJ89lWNa/G5a4
MD5:	A91E42BD767B2F0AD2BCD233C2AD4EA2
SHA1:	71E36235B1E495E06257767994A4FFE87EDE2EAE
SHA-256:	61101E718E6D4DA259E924BC0DEAD54785030EF338E68747D13B39C6A76DC278
SHA-512:	48C09DB69F9146A2AE052E26009BDDC2F9B2181774693B2523DAB6AB3889203DDB53B16B25B50D33ACBC61B87EF6F351BB693AB0F9AF73E21BED132F258FB79 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...).)b...._keyhttps://www.paperturn.com/cache/v2.3.12/mini-2c7001179082c8031f506f1a6a77ca2f.js .https://paperturn.com/9v..W&/.....,.a..E.....za.....g ..?.R...E..A..Eo.....=.....A..Eo.....9v..W&/..l..A46A4BACBDA6493C18D52D950BA55B74358D15D3599484FFCE96C2C2F844F3B3.,.a..E.....za.....g..?.R. ..E..A..Eo.....3E.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ddf7e8582ef3dff7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.501565690531915
Encrypted:	false
SSDEEP:	6:m6VYGL+MIwJJas2buB4ug/GS6IYFtbK6tW6VYGL+MIwJJas2buB7TlgqeS6IYUgJ:LIwva0D9ftNxIwva0N9e9B7
MD5:	14029B1260CFABE9AA5C8BC13BC92E07
SHA1:	624FD6917C456AA685FBDF565EB05CC09274F292
SHA-256:	C025FE2F4CFCBAF3478344B95ACED3EEEE741CB0E5745F349829EC3C006F8504
SHA-512:	5CB237901914EFC8EAB078C4B13BC5F312217AE84EE6E447E456686BF9515B4910C13A4702BE8E224173921053F0D59ACA04AD5D6AB902FE3B471DD580EB31C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...s..F...._keyhttps://www.google-analytics.com/analytics.js .https://paperturn-view.com/..X.W&/.....Z.....F. ./..3....V...c..U.....A..Eo.....z.....A..E o.....0\r..m.....N...s..F...._keyhttps://www.google-analytics.com/analytics.js .https://paperturn-view.com/....W&/.....Z.....F. ./..3....V...c..U.....A..Eo.....oz..... ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e41c3bf86352e7cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e41c3bf86352e7cd_0	
Size (bytes):	222
Entropy (8bit):	5.538090585196531
Encrypted:	false
SSDEEP:	6:m0nYcvhAbuBKB/2uhs2buBigr5x3vnxuK6t:hJsoe0z5NvxQ
MD5:	6F1B306DE23CEBD2C7C4DE5CEBDC86BF
SHA1:	2459E2646E1CD29E840EEE742D5DE64F4B3AB1F0
SHA-256:	6B6E35A95D4A23204499287F918F7FDD2C70165DA4F472DBBD32518513878B50
SHA-512:	C83C6AA11D58CBC65E98AB69573E9D90838C4FCB5F5F0614C0F4419A97D6DB654F9F717F68CCD512A599662210E3575F570CAFAC250C9F27073188B8D8818ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z...'XR....._keyhttps://assets.paperturn-view.com/index.js?20210723020133 .https://paperturn-view.com/d...W&/.....~.....&]...ey..u.....1Sp.d.t.fZ.!.A..Eo .....5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e65797cd70a56c3a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.554909789196034
Encrypted:	false
SSDEEP:	6:mwFYp3zJs2bt6HgKlQdfF4/nSK6t+9Hgj8edfF4/nd+d9HgwnlQdfF4/ndLS9Hg+:dsFW0dckMredcuPlQdcdL+sedcg/dc
MD5:	00E5DF6070ED6E14625A544A12025CC8
SHA1:	621159ACB26AA96EEEB5AAD81E6F01B6A59BDCB7
SHA-256:	172B431581D0858BE9DEF0EE62C4192A1B1CFEFF7C980F44809BE58511CB0070
SHA-512:	967054845BBD640A1373D24D32BA8B2A5171E26CB097497A79DD202940923B9AB8E395FAA8D2B3FF8EBCF7BCAF6BB8091F7283325337CF224ED13C0773EACCD 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G....t.&...._keyhttps://v2.zopim.com/bin/v/widget_v2.329.js .https://paperturn.com/.l..W&/.....;0.....n.dl..hd.....$....\.<.....A..Eo.....K.[.....A..Eo..... ...l..W&/.....n.dl..hd.....$....\.<.....A..Eo.....C.....l..W&/.....n.dl..hd.....$....\.<.....A..Eo.....W0.....l..W&/.....j.....n.dl..hd.....$....\.<... ....A..Eo.....P.....l..W&/.....^.....n.dl..hd.....$....\.<.....A..Eo.....v^.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e78a65cbed4dea02_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.703882154487978
Encrypted:	false
SSDEEP:	6:mokYGLibtGqd45rn1Qjzs2btIgO/mlVrbzbK6t:iqd41AzwmIV/p
MD5:	1403038EC9FFD542E35BA74E6028C027
SHA1:	7D7950A1C3CE5632186F62CA1D3719DBE4F8E508
SHA-256:	C2F67272FA7DB13384095F778C7E1630C6A9CAC9471392F2AF553AA8C52FB6C5
SHA-512:	3A3FD4BBDC545DCA9D6EF31FB6EEFA6F686D066241F830975723DFC3716551FA0537CF9F6A5BE578A8DC04D5EAA5801E0E97A234CC03181F11F585A8BB28AA A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l...'.^)...._keyhttps://www.paperturn.com/cache/v2.3.12/mini-d0f4fc79d4063f6d5171f399465f6cb6.js .https://paperturn.com/ T+.W&/.....)...X...)...C"j.]. .L..s$2hr.B.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7eeab8bd5560049_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	476
Entropy (8bit):	5.606218219962993
Encrypted:	false
SSDEEP:	6:mEYnYcvhAbuB4a+1h2Z7vNRs2buBmDug4mIGnEK6tWEYnYcvhAbuB4a+1h2Z7vNp:OvJuvD2tL0yGvIvJuvD2tL05Lxdqp
MD5:	5A61AC31E29FBB0F651134605ACC6A7B
SHA1:	284408987DF33334CF35A71B34FFEA743C892D4F
SHA-256:	59A596444E398ECE1C446217E00093E114FB7F23E7BC0BF5650A33CBD4E3A791
SHA-512:	088154BAF967EEE7ADBF9B6F8971ECDEA852F9229AC93E4BD0F2E1ED3F4BD694944DC22A5A25075B74A80F30FC4F3A2E6D2BF1BB88F6E8E93129EDD9E4A679 AD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e7eeab8bd5560049_0	
Reputation:	low
Preview:	0\r..m.....j.....5...._keyhttps://assets.paperturn-view.com/components-SnackbarProvider.b1a734fc.js .https://paperturn-view.com/..f.W&/.....G.....?.N.Mv...s.C#c5..d....QX....A..Eo.....].....A..Eo.....0\r..m.....j.....5...._keyhttps://assets.paperturn-view.com/components-SnackbarProvider.b1a734fc.js .https://paperturn-view.com/A)..W&/.....s.....?.N.Mv...s.C#c5..d....QX....A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e8a9b928233b277a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	403
Entropy (8bit):	6.210332409062683
Encrypted:	false
SSDEEP:	6:mrS8XXYELaKJQFd/OKtqfUmtI7Jsb+vamvAipfYBxkfrQxLRtgallGmdvgzk4A0H:ES8xLaKS/m3tIlHSm3ox9xLztgY/g
MD5:	8F6F4AB12C5E151D09A121C6A56A5E1E
SHA1:	3A646F5B58AD8E638B558764B5106403FC66C7A0
SHA-256:	9553EBF8F92705DE7C67DC23BA64D97425557174426F8A1F40D9474312D57425
SHA-512:	E2C84C9184EBA725385DA1572C9EAEF133A0707C603EDD412BABFEB2D78A0F1726D3F73791B05D4707E18B6A98B7F2921421597D18C8956CF638C6137C0630C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://xpans.in/document/Drive/asd/ScriptResource.axd?d=KozZrTVT8ndoIojtkc7ps-zrkEG427bomy-mzEko1QrwRvKEBPnBH-eEBG-fwBgYq7vo370eJLLGk7WUP2b7mI8TDWlp_qYPfXW_5pbAQZLH8_PPmuRYZVil-z0367-tVCsNT-4DayceIpClEr2xh51rkJ0nz9Zws1FVvy1dbq41&t=ffffffffab5b37cd .https://xpans.in/.p.W&/.....W".....0."..i^E...E8F..08.3.U0x...[....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ed55c9f01fcca8ed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	474
Entropy (8bit):	5.5145729087981445
Encrypted:	false
SSDEEP:	12:UJu5080NR1+EeUfA3T2Ju5080ZEeUfyr:+8C+XUfC88eXUfS
MD5:	FE21CE46DE6F1B412664686E038D39B2
SHA1:	8769C378BDEC1C128587ADC929C730F15B8B8D48
SHA-256:	118EB9E48DBC803E5645072C4CC4059C928ABB5ADA786FB21088ACFA7693F796
SHA-512:	ABD5A30283647F50937A45A9CAD53ADF6A9377EDDE6F20BDA3AE04C9EA8CE4488CC778A1B253AD53916D9B3653C7795318375671D6963616E0DC463D53A8EA4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....!....._keyhttps://assets.paperturn-view.com/components-ViewerContainer.a8be06bc.js .https://paperturn-view.com/.Mt.W&/.....N.....7..Q... x .GQ..wW.D..U...e...A..Eo.....A..Eo.....0\r..m.....i....!....._keyhttps://assets.paperturn-view.com/components-ViewerContainer.a8be06bc.js .https://paperturn-view.com/...W&/.....7..Q... x.GQ..wW.D..U...e...A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f4692d38da8f7d92_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.538136501360896
Encrypted:	false
SSDEEP:	6:me6EYcvhAbuB/KSXyc/blyb2WoXamZvLs2buBgyg58msaAnnK6t:P/JNKmvWYz0YHsaqp
MD5:	89FCE1604A62273840A4C6CDCF6CC645
SHA1:	51761C3CE4755B475892BB5E69871445FDF6B876
SHA-256:	EAD36D112729585BC2933A7AE27E270DB7F117D3286B09AF7E62B4AA1989F041
SHA-512:	0C34D037BB05DF3F585565033CF7674341450DB5F3D092ACBBEBFF5279888E77E8660CE66BC2FF4E9AFD87DE175849C8329135416CB2CD3975ACC73755EE969
Malicious:	false
Reputation:	low
Preview:	0\r..m.....$....._keyhttps://assets.paperturn-view.com/vendors~components-AddToBasket~components-Alert~components-Basket~components-Basket-BasketItems~comp~3396e82e.035b7405.js .https://paperturn-view.com/8Xn.W&/.....s..C.0Z....!.....-.. 3....A..Eo.....d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f5e415729b027894_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	426

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f5e415729b027894_0	
Entropy (8bit):	5.617893101705748
Encrypted:	false
SSDEEP:	6:m3inYcvhAbuBUSNRs2buB4Wtg64ErlFh+fRK6tW3inYcvhAbuBUSNRs2buBMgoEh:DJmu03mwPhCrRJmu0OwPhXp
MD5:	155AFF630B70D48796DA2561542EDCBE
SHA1:	227A6FC0ED591452793B21AB6EFCDE6489B899E2
SHA-256:	81371976BAB8AE8234FDFD37A1942DB77D73D4342467166912FBB866594E7DEE
SHA-512:	960ADEA8CDD2F4347B65DC6FB413360F8E4ECAD3BE38824C6DB147AE10C2687BABD374FE50F6D07C422855CB082DE3CD426FC4AA844D03F8C37CDD0BF1A5 B24
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...J....._keyhttps://assets.paperturn-view.com/13.9cb813a3.js .https://paperturn-view.com/..\.W&/.....R....)^.}..f.CK.|..R...g.`.7..A..Eo.....NQYt.....A..E o.....0\r..m.....Q...J....._keyhttps://assets.paperturn-view.com/13.9cb813a3.js .https://paperturn-view.com/....W&/.....R....)^.}..f.CK.|..R...g.`.7..A..Eo... .....dQ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f7733717fc9a9560_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	5.526249243571525
Encrypted:	false
SSDEEP:	24:7e58DyrMf9e583rMnr9e58XrMD9e58IQrMO9e58NirMD9e58cErMD:7K8GrMf9K83rMr9K8XrMD9K8IQrMO9K5
MD5:	D80757EF1EBD9C569AA22C6E6699C673
SHA1:	3A3FF97B27B06169D6C88493BF74E30D292BDD28
SHA-256:	41832BB7AE7C64A95DCF0F80B7751C18D3EC55F2B09CE98F573E1854AA14A0B8
SHA-512:	18DEF44E2878D6698175E4A0BAE30848E81FA052C364BE00FB0E11CF1A221F6E7F542C7281A800603226B1368117B818B1FE4439587AC2BF6C37B14B55CE7E33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://paperturn.com/....W&/.....%.....{....1;....t...N.....A..Eo.....A..Eo..... ...0\r..m.....J....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://paperturn.com/.5>.W&/.....%.....{....1;....t...N.....A..Eo.....A..Eo..... .....0\r..m.....J....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://paperturn.com/...W&/.....dl.....%.....{....1;....t...N.....A..Eo.....5.....A..Eo..... .....0\r..m.....J....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://paperturn.com/....W&/.....%.....{....1;....t...N.....A..Eo.....m<k.....A..Eo..... .....0\r..m.....J....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://paperturn.com/HL,.W&/.....%.....{....1;....t...N.....A..Eo.....0.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f99d6da11388c29b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.452964540637544
Encrypted:	false
SSDEEP:	6:majYcvhAbuB4VGYRs2buBItgxtsZnn6Fk84+nK6t:7JuVJ02isQFk8Xp
MD5:	A8729B6C74C6222CCC5093E537B02017
SHA1:	04DEF8997060DAB8A2D54EAA7F5B4F7B77A3235A
SHA-256:	F6624E747D5FCB44B449EDB9EF00D9584C7D08383218580D084BA0654E04E150
SHA-512:	12E767FB6377E8248679014F335F547257F1170B314EBD408772271BAD025ECA9E9688B5F8B233D7E249C6AC949111D05BB9BF05E80BD15F17D750183B27CBB4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...w#....._keyhttps://assets.paperturn-view.com/components-BottomBar.9060c6c1.js .https://paperturn-view.com/$Mt.W&/.....@.7.~)].&/..+....o..=l... w.A..Eo.....lM.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd410d0fcd87a62a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	6.256769339267302
Encrypted:	false
SSDEEP:	6:mGYELaKJQF0EKi3PmsPVqXtq9IvrQCykZrxgKzG+MeRN3nLyDugy7BnoyP49QzbD:hLaKyf3Gq+DIKzG+/N3nLykRomB
MD5:	8CA8C4F837A6BE6C1B8D6F6F6B567A36
SHA1:	1738DA7E298BF5DA90DACA08946BBA03BC9749A6
SHA-256:	5EF8ADACE12CA9EC14FAE096D39A2BCB752FC3CB512EAA603ED8A63AA1642B44
SHA-512:	38EB8386D602F138E25D9552749A4C0E3CC98A700F3A3475D9FD0E591B3C0B94535A113A420596D4C7C63D3595B81011BB958323663CA0F7F7578B2DBA396EA6
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\fd410d0fcd87a62a_0	
Reputation:	low
Preview:	0\r..m.....Ok....._keyhttps://xpans.in/document/Drive/asd/ScriptResource.axd?d=YfbPqEYj0W31Qd6b83PGlWON7nZi7y2471DNsdTWssElkCGzwOy2JjZMN6Q2J0CxzcQQMZxoFp-M9jgIk2__cRVfgn6cWZ7Z_b9bpoSJ9398HB6BkZgWc5aKYHnJsU-BmVVRY4UUCV5Fic6Gmpm_oZLb8Buaqp86-tiOy7lm8vuLYoTaNPLJWb1IMmHTO7uG0&t=545ba255 .https://xpans.in/5.q.W&/.....X".....,.t5Go..,..2..*.....U..m.A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1776
Entropy (8bit):	5.354397763326519
Encrypted:	false
SSDEEP:	24:qVV6jzvl3CCpMM84fFz9dw2A+xKO13sn/hO:k8zv177dnnU/hO
MD5:	4614BBAB23A47A09FAF1733D27A476B0
SHA1:	3D8B771E76494C1696121FDB4A6CC4071B947024
SHA-256:	12E020281B8EA264F85BF4C01D8278089C3AA42789FA6919F977D2C6D97BDB05
SHA-512:	F6DED58B6CB3E3CE2A83DD421EBA87CEE49958657BA3F805339B7D45A2C4DDA1062A3AA43EB57B0937FF577EF0C6A57F7A69494DDB885A961FD0BF61125B6E3E
Malicious:	false
Reputation:	low
Preview:	....1Hr.oy retne....H.....R....W....W&/.....k.....W&/.....rp43..?....W&/.....%.R.....W&/.....L.R3.....W&/.....s..Y.p....W&/.....S.0.rW.....W&/.....c&.....W&/.....Bh.7.....W&/.....I.V.....W&/.....z...y.$z....W&/.....I.*..!....W&/.....X.....W&/.....x.....W&/.....L..~.....W&/.....x..r.....W&/.....(.....W&/.....+P._P....W&/.....{..W&/.....Rc.;..{..W&/.....~.`..Y..{..W&/.....]C ...<.{..W&/.....2..n..@9..W&/.....`....7s.@9..W&/.....NNBn/.....W&/.....%....?.....W&/.....M..e....W&/.....(M....d..].W&/.....+..i^3.. .W&/.....l....u.. .W&/.....V... .W&/.....2]..}'.>.. .W&/.....r.....W&/.....*..J....W&/.....(.r.....W&/.....l.p.W..u..W&/.....1>...y..3..W&/.....8..y(.h..l..W&/.....*.....A..l..W&/.....:-q....l..W&/.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	24576
Entropy (8bit):	1.834741055616875
Encrypted:	false
SSDEEP:	48:TekLLOpEO5J/Kn7UieSxfvv3TS4+RPu/yLSIbXZLLOpEO5J/Kn7UGMzSyfvv3TS0:dNwunQLRPKUSeNwENLRPBUSdJW
MD5:	079A6353B1DE774B3D4E4E211608F5D7
SHA1:	1351279DFB3155F246A8207A8CBC91B73ED9CBA1
SHA-256:	12476646EC6C84D14A0480867981E2B8220FEC6D3BFCF0874A03AA9B97F8C2A5
SHA-512:	34AFE7164AF85D8BFD12DDDACE86D4BDED614A79E98E6AA7942F3CE1017D4652451F88A2C9D7FEB6F0B19F59D7B312E4510C671F43167B783824FDA8CB4DE3F3
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	25672
Entropy (8bit):	1.3149000527612524
Encrypted:	false
SSDEEP:	48:KI+mq5LLOpEO5J/Kn7UF8eSxfvv3TS4+RPu/yLSI0qekLLOpEO5J/Kn7Ur8:H+mcNwWnQLRPKUSTMNwk
MD5:	42BE930D04F9F24F1672B77513D6B8CB
SHA1:	1E72256701D6740C5BBB28120A392255E30C3153
SHA-256:	795E8A021BCA87320D0DA724E5187981BB4F7B4C002211C01FAAD3D88A55A66E
SHA-512:	74C14A5E9414C943E116012B0C8385FFE5D50AC791839F05FF9B1C200F7322F56FAAB82A9EB6DD349039E2DF8C5FC9245388B43C7FA5FF0EF81BE817F9218D35
Malicious:	false
Reputation:	low
Preview:	.....4.x..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	136384
Entropy (8bit):	2.97169755269141
Encrypted:	false
SSDEEP:	768:3DYLT/Bd/A8/AM/Au9pWnGmw4O6mmI4OT/Asxm9mb:3D+/b///v/zKS4zS4O/nt
MD5:	918EEB30E6F50DCC3BBBFADBFF6D6F6F
SHA1:	6CB3C2F856CF6382F0941F758879169CA4C27671
SHA-256:	CFA12DAC39E65ACF78396350DACA3A6B351165D6E43EEB06B22E97270FB155AD
SHA-512:	61B7A76521316C88925E534DD2122192B6168E5A89D9B86ECD977BED73D5C1681D1973FFDFE34DC071BF92E50C05BB4795BADA07B2CD14C0F9270FED2CD09DA
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...d4f530e5_e0ae_4e85_92aa_55a2b469342f.....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....U...https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1.....h.....`.....X.....p.....U...h.t.t.p.s.:././.w.w.w...p.a.p.e.r.t.u.r.n.-.v.i.e.w...c.o.m./.u.s./.p.a.p.t.e.r.t.u.r.n.f.i.l.e.s./.s.h.a.r.e.p.o.i.n.t.-.f.i.l.e.?.p.i.d.=.M.T.c.1.7.5.0.3.6.&.v.=.1...1.....8.....0.....8.....U...https://www.paperturn-view.com/u

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.221935049153129
Encrypted:	false
SSDEEP:	6:mfXYUq2P923iKKdK8aPrqIFUtpUXYuZmwPUXY5PkwO923iKKdK8amLJ:9Uv45KkL3FUtpNu/PNd5L5KkQJ
MD5:	1C68BB0146DCC1D1A7D39A0A018FC728
SHA1:	0F101845CDEC9D7AF8A55A70411C96494AA126DB
SHA-256:	0F77156A18ACA5EB4CA88CB0A73171935533D5B6EA0CBCE3EC1F81DC78889BC6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
SHA-512:	8897F4817CBE742850F3C2F49E642240D6C74F0505E880393C619C42E5A6563BFC0E7F96E991B1F7ED21EBE6FC7880D18B3917F273EB1FDDEE43F89DF722104A
Malicious:	false
Reputation:	low
Preview:	2021/07/22-19:00:28.164 17b4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/07/22-19:00:28.165 17b4 Recovering log #3.2021/07/22-19:00:28.166 17b4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D951
Malicious:	false
Reputation:	low
Preview:	.f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Preview:

{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 19:00:32.214699984 CEST	192.168.2.5	8.8.8.8	0xfed3	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.222985983 CEST	192.168.2.5	8.8.8.8	0xe6a6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.227921009 CEST	192.168.2.5	8.8.8.8	0xa626	Standard query (0)	www.paperturn-view.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.122229099 CEST	192.168.2.5	8.8.8.8	0xe213	Standard query (0)	d3euuwqpqlzvic.cloudfront.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.129268885 CEST	192.168.2.5	8.8.8.8	0x7160	Standard query (0)	www.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.424011946 CEST	192.168.2.5	8.8.8.8	0xd015	Standard query (0)	assets.paperturn-view.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.048899889 CEST	192.168.2.5	8.8.8.8	0x6a09	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.552658081 CEST	192.168.2.5	8.8.8.8	0x1a81	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.553356886 CEST	192.168.2.5	8.8.8.8	0xe424	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:35.528513908 CEST	192.168.2.5	8.8.8.8	0xa89d	Standard query (0)	translations.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:36.364301920 CEST	192.168.2.5	8.8.8.8	0x4fc3	Standard query (0)	www.paperturn-view.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.047708988 CEST	192.168.2.5	8.8.8.8	0x8999	Standard query (0)	assets.paperturn-view.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.064929962 CEST	192.168.2.5	8.8.8.8	0x143a	Standard query (0)	d3euuwqpqlzvic.cloudfront.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:39.988229036 CEST	192.168.2.5	8.8.8.8	0x10bd	Standard query (0)	consent.cookiebot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:39.991869926 CEST	192.168.2.5	8.8.8.8	0x813a	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.172305107 CEST	192.168.2.5	8.8.8.8	0x924d	Standard query (0)	images.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.258683920 CEST	192.168.2.5	8.8.8.8	0x713a	Standard query (0)	assets.calendly.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 19:00:40.479422092 CEST	192.168.2.5	8.8.8.8	0x9e5e	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.678127050 CEST	192.168.2.5	8.8.8.8	0x7830	Standard query (0)	acsbapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:41.340328932 CEST	192.168.2.5	8.8.8.8	0x1f76	Standard query (0)	consentcdn.cookiebot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:43.577816963 CEST	192.168.2.5	8.8.8.8	0xc884	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:45.723614931 CEST	192.168.2.5	8.8.8.8	0x22b0	Standard query (0)	cdn.acsbapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.029556036 CEST	192.168.2.5	8.8.8.8	0x1876	Standard query (0)	images.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.996655941 CEST	192.168.2.5	8.8.8.8	0xeaef	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:48.725361109 CEST	192.168.2.5	8.8.8.8	0xe253	Standard query (0)	v2.zopim.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:55.238342047 CEST	192.168.2.5	8.8.8.8	0x57ab	Standard query (0)	www.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:56.993319988 CEST	192.168.2.5	8.8.8.8	0x92c9	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.573523998 CEST	192.168.2.5	8.8.8.8	0xbf22	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.575089931 CEST	192.168.2.5	8.8.8.8	0xeeb1	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:58.973692894 CEST	192.168.2.5	8.8.8.8	0xa72	Standard query (0)	xpans.in	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:59.344590902 CEST	192.168.2.5	8.8.8.8	0x90bd	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:59.362659931 CEST	192.168.2.5	8.8.8.8	0x7139	Standard query (0)	static.sharepointonline.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:01.375731945 CEST	192.168.2.5	8.8.8.8	0x16b	Standard query (0)	xpans.in	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:01.461642027 CEST	192.168.2.5	8.8.8.8	0x1758	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:02.183159113 CEST	192.168.2.5	8.8.8.8	0xb949	Standard query (0)	static.zdassets.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:02.561655998 CEST	192.168.2.5	8.8.8.8	0x173f	Standard query (0)	ekr.zdassets.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.903520107 CEST	192.168.2.5	8.8.8.8	0xe5ff	Standard query (0)	widget-mediator.zopim.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:04.591250896 CEST	192.168.2.5	8.8.8.8	0xc775	Standard query (0)	v2assets.zopim.io	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.516477108 CEST	192.168.2.5	8.8.8.8	0x71f7	Standard query (0)	images.paperturn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.517483950 CEST	192.168.2.5	8.8.8.8	0xbb05	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:18.282258034 CEST	192.168.2.5	8.8.8.8	0x1b08	Standard query (0)	consent.cookiebot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.299048901 CEST	192.168.2.5	8.8.8.8	0xf042	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.548439980 CEST	192.168.2.5	8.8.8.8	0x972f	Standard query (0)	consentcdn.cookiebot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.352044106 CEST	192.168.2.5	8.8.8.8	0x1ef	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.360992908 CEST	192.168.2.5	8.8.8.8	0x4223	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.929851055 CEST	192.168.2.5	8.8.8.8	0xc23f	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.937478065 CEST	192.168.2.5	8.8.8.8	0x33b3	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:32.754302025 CEST	192.168.2.5	8.8.8.8	0x64fe	Standard query (0)	d8n9fts9ic943.cloudfront.net	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:33.986771107 CEST	192.168.2.5	8.8.8.8	0xfb96	Standard query (0)	d3euuwqpqlzvic.cloudfront.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:00:32.280525923 CEST	8.8.8.8	192.168.2.5	0xfed3	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:00:32.280525923 CEST	8.8.8.8	192.168.2.5	0xfed3	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.288146973 CEST	8.8.8.8	192.168.2.5	0xe6a6	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.291388988 CEST	8.8.8.8	192.168.2.5	0xa626	No error (0)	www.paperturn-view.com		143.204.225.123	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.291388988 CEST	8.8.8.8	192.168.2.5	0xa626	No error (0)	www.paperturn-view.com		143.204.225.125	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.291388988 CEST	8.8.8.8	192.168.2.5	0xa626	No error (0)	www.paperturn-view.com		143.204.225.71	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:32.291388988 CEST	8.8.8.8	192.168.2.5	0xa626	No error (0)	www.paperturn-view.com		143.204.225.42	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.181731939 CEST	8.8.8.8	192.168.2.5	0x6f8	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.181889057 CEST	8.8.8.8	192.168.2.5	0xe213	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.76	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.181889057 CEST	8.8.8.8	192.168.2.5	0xe213	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.13	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.181889057 CEST	8.8.8.8	192.168.2.5	0xe213	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.224	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.181889057 CEST	8.8.8.8	192.168.2.5	0xe213	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.40	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.186906099 CEST	8.8.8.8	192.168.2.5	0xbdf4	No error (0)	www-googletagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.218102932 CEST	8.8.8.8	192.168.2.5	0x7160	No error (0)	www.paperturn.com		148.251.96.155	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.483755112 CEST	8.8.8.8	192.168.2.5	0xd015	No error (0)	assets.paperturn-view.com		143.204.225.93	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.483755112 CEST	8.8.8.8	192.168.2.5	0xd015	No error (0)	assets.paperturn-view.com		143.204.225.76	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.483755112 CEST	8.8.8.8	192.168.2.5	0xd015	No error (0)	assets.paperturn-view.com		143.204.225.82	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.483755112 CEST	8.8.8.8	192.168.2.5	0xd015	No error (0)	assets.paperturn-view.com		143.204.225.60	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:33.606247902 CEST	8.8.8.8	192.168.2.5	0x5659	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.101423979 CEST	8.8.8.8	192.168.2.5	0x6a09	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:34.101423979 CEST	8.8.8.8	192.168.2.5	0x6a09	No error (0)	stats.l.doubleclick.net		64.233.167.157	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.101423979 CEST	8.8.8.8	192.168.2.5	0x6a09	No error (0)	stats.l.doubleclick.net		64.233.167.155	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.101423979 CEST	8.8.8.8	192.168.2.5	0x6a09	No error (0)	stats.l.doubleclick.net		64.233.167.154	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.101423979 CEST	8.8.8.8	192.168.2.5	0x6a09	No error (0)	stats.l.doubleclick.net		64.233.167.156	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.610393047 CEST	8.8.8.8	192.168.2.5	0xe424	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:34.617379904 CEST	8.8.8.8	192.168.2.5	0x1a81	No error (0)	www.google.de		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:35.587951899 CEST	8.8.8.8	192.168.2.5	0xa89d	No error (0)	translations.papertu rn.com		143.204.225.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:00:35.587951899 CEST	8.8.8.8	192.168.2.5	0xa89d	No error (0)	translations.papertrn.com		143.204.225.62	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:35.587951899 CEST	8.8.8.8	192.168.2.5	0xa89d	No error (0)	translations.papertrn.com		143.204.225.123	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:35.587951899 CEST	8.8.8.8	192.168.2.5	0xa89d	No error (0)	translations.papertrn.com		143.204.225.84	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:36.438906908 CEST	8.8.8.8	192.168.2.5	0x4fc3	No error (0)	www.paperturn-view.com		143.204.225.123	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:36.438906908 CEST	8.8.8.8	192.168.2.5	0x4fc3	No error (0)	www.paperturn-view.com		143.204.225.125	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:36.438906908 CEST	8.8.8.8	192.168.2.5	0x4fc3	No error (0)	www.paperturn-view.com		143.204.225.71	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:36.438906908 CEST	8.8.8.8	192.168.2.5	0x4fc3	No error (0)	www.paperturn-view.com		143.204.225.42	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.109952927 CEST	8.8.8.8	192.168.2.5	0x8999	No error (0)	assets.paperturn-view.com		143.204.225.93	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.109952927 CEST	8.8.8.8	192.168.2.5	0x8999	No error (0)	assets.paperturn-view.com		143.204.225.60	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.109952927 CEST	8.8.8.8	192.168.2.5	0x8999	No error (0)	assets.paperturn-view.com		143.204.225.82	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.109952927 CEST	8.8.8.8	192.168.2.5	0x8999	No error (0)	assets.paperturn-view.com		143.204.225.76	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.128928900 CEST	8.8.8.8	192.168.2.5	0x143a	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.224	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.128928900 CEST	8.8.8.8	192.168.2.5	0x143a	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.13	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.128928900 CEST	8.8.8.8	192.168.2.5	0x143a	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.40	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:37.128928900 CEST	8.8.8.8	192.168.2.5	0x143a	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.76	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.053800106 CEST	8.8.8.8	192.168.2.5	0x813a	No error (0)	use.fontawesome.com	use.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:40.053864002 CEST	8.8.8.8	192.168.2.5	0x10bd	No error (0)	consent.cookiebot.com	consent.cookiebot.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:40.239497900 CEST	8.8.8.8	192.168.2.5	0x924d	No error (0)	images.paperturn.com	d3jodor2jgify2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:40.239497900 CEST	8.8.8.8	192.168.2.5	0x924d	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.4	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.239497900 CEST	8.8.8.8	192.168.2.5	0x924d	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.25	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.239497900 CEST	8.8.8.8	192.168.2.5	0x924d	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.16	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.239497900 CEST	8.8.8.8	192.168.2.5	0x924d	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.106	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.321464062 CEST	8.8.8.8	192.168.2.5	0x713a	No error (0)	assets.calendly.com	d2mvl3dkxvehny.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:40.321464062 CEST	8.8.8.8	192.168.2.5	0x713a	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.225.47	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.321464062 CEST	8.8.8.8	192.168.2.5	0x713a	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.225.8	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.321464062 CEST	8.8.8.8	192.168.2.5	0x713a	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.225.113	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:00:40.321464062 CEST	8.8.8.8	192.168.2.5	0x713a	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.225.79	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.537102938 CEST	8.8.8.8	192.168.2.5	0x9e5e	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:40.537102938 CEST	8.8.8.8	192.168.2.5	0x9e5e	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.738614082 CEST	8.8.8.8	192.168.2.5	0x7830	No error (0)	acsbapp.com		206.189.187.108	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.738614082 CEST	8.8.8.8	192.168.2.5	0x7830	No error (0)	acsbapp.com		161.35.15.77	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.738614082 CEST	8.8.8.8	192.168.2.5	0x7830	No error (0)	acsbapp.com		208.68.39.149	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:40.738614082 CEST	8.8.8.8	192.168.2.5	0x7830	No error (0)	acsbapp.com		206.189.191.180	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:41.401802063 CEST	8.8.8.8	192.168.2.5	0x1f76	No error (0)	consentcdn.cookiebot.com	consentcdn.cookiebot.com-v1.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:43.627810001 CEST	8.8.8.8	192.168.2.5	0xc884	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:43.627810001 CEST	8.8.8.8	192.168.2.5	0xc884	No error (0)	star-mini.c10r.facebook.com		157.240.16.35	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:45.784218073 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	cdn.acsbapp.com	acsbapp.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:45.784218073 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	acsbapp.com		206.189.191.180	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:45.784218073 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	acsbapp.com		206.189.187.108	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:45.784218073 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	acsbapp.com		161.35.15.77	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:45.784218073 CEST	8.8.8.8	192.168.2.5	0x22b0	No error (0)	acsbapp.com		208.68.39.149	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.111012936 CEST	8.8.8.8	192.168.2.5	0x1876	No error (0)	images.paperturn.com	d3jodor2jgify2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:46.111012936 CEST	8.8.8.8	192.168.2.5	0x1876	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.25	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.111012936 CEST	8.8.8.8	192.168.2.5	0x1876	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.16	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.111012936 CEST	8.8.8.8	192.168.2.5	0x1876	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.106	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:46.111012936 CEST	8.8.8.8	192.168.2.5	0x1876	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.4	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:47.053620100 CEST	8.8.8.8	192.168.2.5	0xeaef	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:47.053620100 CEST	8.8.8.8	192.168.2.5	0xeaef	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:48.789084911 CEST	8.8.8.8	192.168.2.5	0xe253	No error (0)	v2.zopim.com		104.16.106.139	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:48.789084911 CEST	8.8.8.8	192.168.2.5	0xe253	No error (0)	v2.zopim.com		104.16.103.139	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:48.789084911 CEST	8.8.8.8	192.168.2.5	0xe253	No error (0)	v2.zopim.com		104.16.105.139	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:48.789084911 CEST	8.8.8.8	192.168.2.5	0xe253	No error (0)	v2.zopim.com		104.16.107.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:00:48.789084911 CEST	8.8.8.8	192.168.2.5	0xe253	No error (0)	v2.zopim.com		104.16.104.139	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:55.298424959 CEST	8.8.8.8	192.168.2.5	0x57ab	No error (0)	www.papert urn.com		148.251.96.155	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:56.070926905 CEST	8.8.8.8	192.168.2.5	0xdb9d	No error (0)	gstaticads sl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.042562008 CEST	8.8.8.8	192.168.2.5	0x92c9	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:57.042562008 CEST	8.8.8.8	192.168.2.5	0x92c9	No error (0)	stats.l.do ubleclick.net		66.102.1.156	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.042562008 CEST	8.8.8.8	192.168.2.5	0x92c9	No error (0)	stats.l.do ubleclick.net		66.102.1.154	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.042562008 CEST	8.8.8.8	192.168.2.5	0x92c9	No error (0)	stats.l.do ubleclick.net		66.102.1.155	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.042562008 CEST	8.8.8.8	192.168.2.5	0x92c9	No error (0)	stats.l.do ubleclick.net		66.102.1.157	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.625771046 CEST	8.8.8.8	192.168.2.5	0xbf22	No error (0)	www.google .com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:57.640732050 CEST	8.8.8.8	192.168.2.5	0xeeb1	No error (0)	www.google.de		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:59.038078070 CEST	8.8.8.8	192.168.2.5	0xa72	No error (0)	xpans.in		144.91.89.225	A (IP address)	IN (0x0001)
Jul 22, 2021 19:00:59.401336908 CEST	8.8.8.8	192.168.2.5	0x90bd	No error (0)	spoprod-a. akamaihd.net	spoprod-a.akamaihd.net.edgesuite .net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:00:59.425767899 CEST	8.8.8.8	192.168.2.5	0x7139	No error (0)	static.sha repointonl ine.com	static.sharepointonline.co m-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:01.434077978 CEST	8.8.8.8	192.168.2.5	0x16b	No error (0)	xpans.in		144.91.89.225	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:01.523473978 CEST	8.8.8.8	192.168.2.5	0x1758	No error (0)	spoprod-a. akamaihd.net	spoprod-a.akamaihd.net.edgesuite .net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:02.233021975 CEST	8.8.8.8	192.168.2.5	0xb949	No error (0)	static.zda ssets.com		104.18.70.113	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:02.233021975 CEST	8.8.8.8	192.168.2.5	0xb949	No error (0)	static.zda ssets.com		104.18.72.113	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:02.614084959 CEST	8.8.8.8	192.168.2.5	0x173f	No error (0)	ekr.zdasse ts.com		104.18.70.113	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:02.614084959 CEST	8.8.8.8	192.168.2.5	0x173f	No error (0)	ekr.zdasse ts.com		104.18.72.113	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		52.29.88.9	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		35.158.37.218	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		52.29.74.145	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		3.65.187.24	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		35.157.204.138	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		52.59.52.172	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-med iator.zopim.com		52.57.125.117	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:01:03.966042995 CEST	8.8.8.8	192.168.2.5	0xe5ff	No error (0)	widget-mediator.zopim.com		18.198.99.212	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:04.657028913 CEST	8.8.8.8	192.168.2.5	0xc775	No error (0)	v2assets.zopim.io		104.18.204.90	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:04.657028913 CEST	8.8.8.8	192.168.2.5	0xc775	No error (0)	v2assets.zopim.io		104.16.152.37	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.573379040 CEST	8.8.8.8	192.168.2.5	0x71f7	No error (0)	images.paperturn.com	d3jodor2jgify2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:17.573379040 CEST	8.8.8.8	192.168.2.5	0x71f7	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.25	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.573379040 CEST	8.8.8.8	192.168.2.5	0x71f7	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.16	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.573379040 CEST	8.8.8.8	192.168.2.5	0x71f7	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.106	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.573379040 CEST	8.8.8.8	192.168.2.5	0x71f7	No error (0)	d3jodor2jgify2.cloudfront.net		143.204.225.4	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:17.574305058 CEST	8.8.8.8	192.168.2.5	0xbb05	No error (0)	use.fontawesome.com	use.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:18.341384888 CEST	8.8.8.8	192.168.2.5	0x1b08	No error (0)	consent.cookiebot.com	consent.cookiebot.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	youtube-ui.l.google.com		172.217.168.14	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	youtube-ui.l.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	youtube-ui.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	youtube-ui.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.351037979 CEST	8.8.8.8	192.168.2.5	0xf042	No error (0)	youtube-ui.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:19.607424021 CEST	8.8.8.8	192.168.2.5	0x972f	No error (0)	consentcdn.cookiebot.com	consentcdn.cookiebot.com-v1.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:20.408777952 CEST	8.8.8.8	192.168.2.5	0x1ef	No error (0)	googleads.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.427203894 CEST	8.8.8.8	192.168.2.5	0x4223	No error (0)	static.doubleclick.net	static-doubleclick-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 19:01:20.427203894 CEST	8.8.8.8	192.168.2.5	0x4223	No error (0)	static-doubleclick-net.l.google.com		172.217.168.70	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.994856119 CEST	8.8.8.8	192.168.2.5	0x33b3	No error (0)	i.ytimg.com		216.58.215.246	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.994856119 CEST	8.8.8.8	192.168.2.5	0x33b3	No error (0)	i.ytimg.com		172.217.168.22	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.994856119 CEST	8.8.8.8	192.168.2.5	0x33b3	No error (0)	i.ytimg.com		172.217.168.54	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.994856119 CEST	8.8.8.8	192.168.2.5	0x33b3	No error (0)	i.ytimg.com		172.217.168.86	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.994856119 CEST	8.8.8.8	192.168.2.5	0x33b3	No error (0)	i.ytimg.com		142.250.203.118	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:20.998456001 CEST	8.8.8.8	192.168.2.5	0xc23f	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 19:01:20.998456001 CEST	8.8.8.8	192.168.2.5	0xc23f	No error (0)	photos-ugc.l.googleusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:34.044720888 CEST	8.8.8.8	192.168.2.5	0xd618	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:34.050635099 CEST	8.8.8.8	192.168.2.5	0xfb96	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.13	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:34.050635099 CEST	8.8.8.8	192.168.2.5	0xfb96	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.224	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:34.050635099 CEST	8.8.8.8	192.168.2.5	0xfb96	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.40	A (IP address)	IN (0x0001)
Jul 22, 2021 19:01:34.050635099 CEST	8.8.8.8	192.168.2.5	0xfb96	No error (0)	d3euuwqpqlzvic.cloudfront.net		13.225.29.76	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 19:00:33.361386061 CEST	148.251.96.155	443	192.168.2.5	49726	CN=paperturn.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jun 02 12:37:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Aug 31 12:37:18 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 22, 2021 19:00:35.573985100 CEST	148.251.96.155	443	192.168.2.5	49740	CN=paperturn.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jun 02 12:37:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Aug 31 12:37:18 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

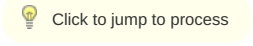
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 19:00:36.601207972 CEST	143.204.225.123	443	192.168.2.5	49748	CN=paperturn-view.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Oct 07 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Nov 06 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 22, 2021 19:00:37.229034901 CEST	143.204.225.93	443	192.168.2.5	49750	CN=paperturn-view.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Oct 07 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Nov 06 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 19:00:39.585961103 CEST	148.251.96.155	443	192.168.2.5	49757	CN=paperturn.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jun 02 12:37:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Aug 31 12:37:18 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 22, 2021 19:00:40.316572905 CEST	148.251.96.155	443	192.168.2.5	49760	CN=paperturn.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jun 02 12:37:18 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Aug 31 12:37:18 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3500 Parent PID: 4672

General

Start time:	19:00:26
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.paperturn-view.com/us/papterturnfiles/sharepoint-file?pid=MTc175036&v=1.1'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 4588 Parent PID: 3500

General

Start time:	19:00:28
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1708 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 6532 Parent PID: 3500

General

Start time:	19:00:34
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=4612 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: chrome.exe PID: 3708 Parent PID: 3500

General

Start time:	19:01:23
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1572,7917042391378505505,9881702941299426833,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=3848 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Copyright Joe Security LLC

Copyright Joe Security LLC 2021