ID: 448253
Cookbook: browseurl.jbs
Time: 20:49:59
Date: 13/07/2021
Version: 33.0.0 White Diamond

Table of Contents

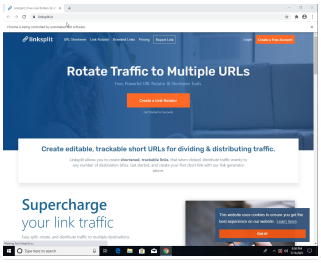
Windows Analysis Report https://linksplit.io/

Overview

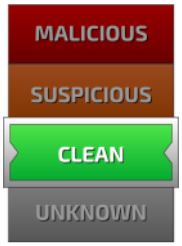
General Information

Sample URL:	http://https://linksplit.io/
Analysis ID:	448253
Infos:	

Most interesting Screenshot:



Detection

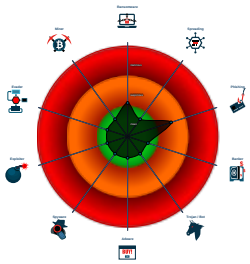


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Form action URLs do not match mai…
- Found iframes
- HTML title does not match URL
- Unusual large HTML page

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6448 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://linksplit.io/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6696 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6188 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=7588 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5484 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=7336 /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

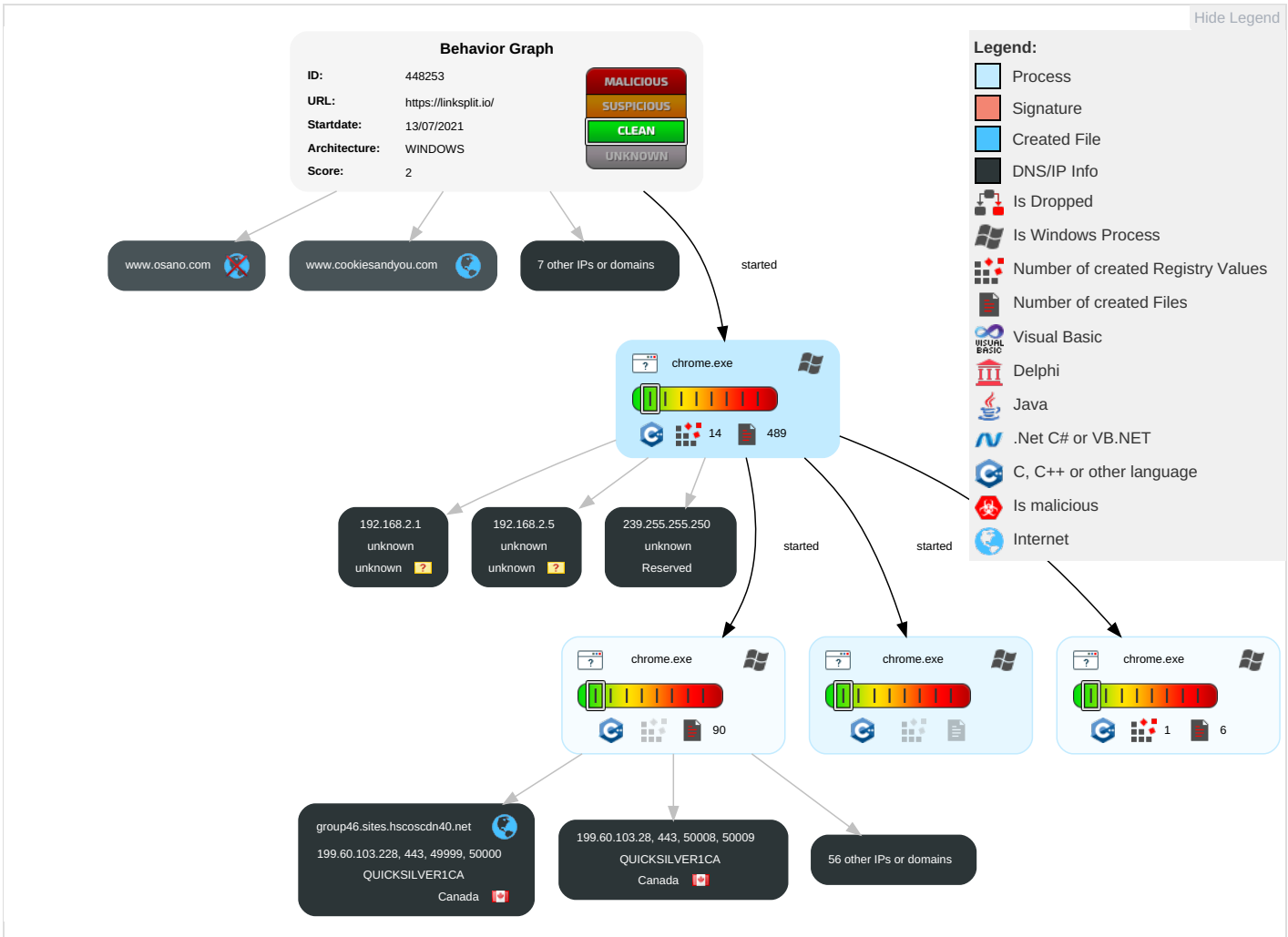
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	I
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	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	M S F
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	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	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	D D D

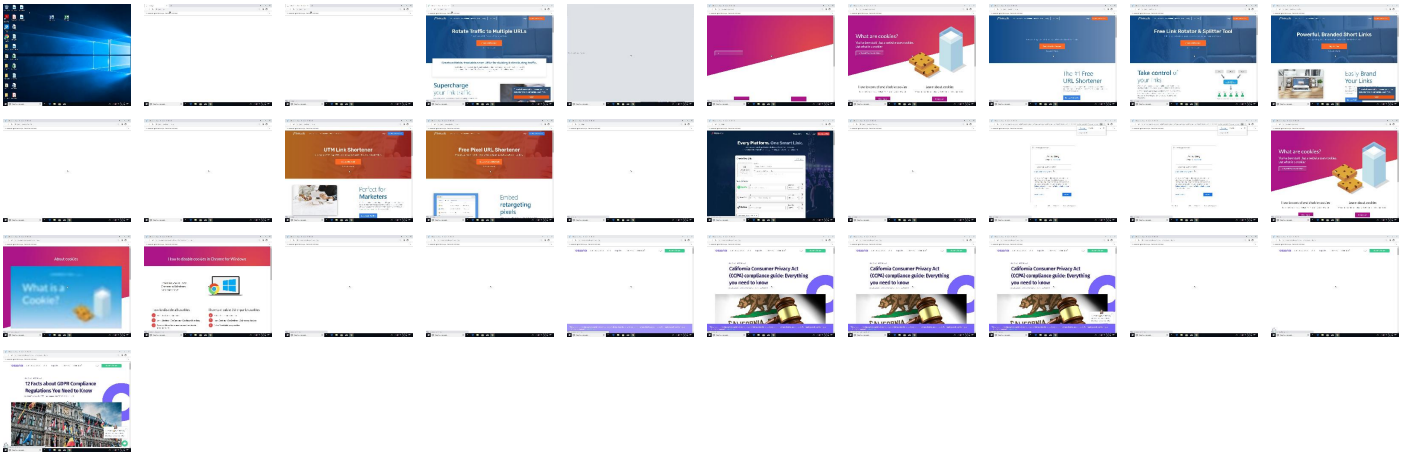
Behavior Graph

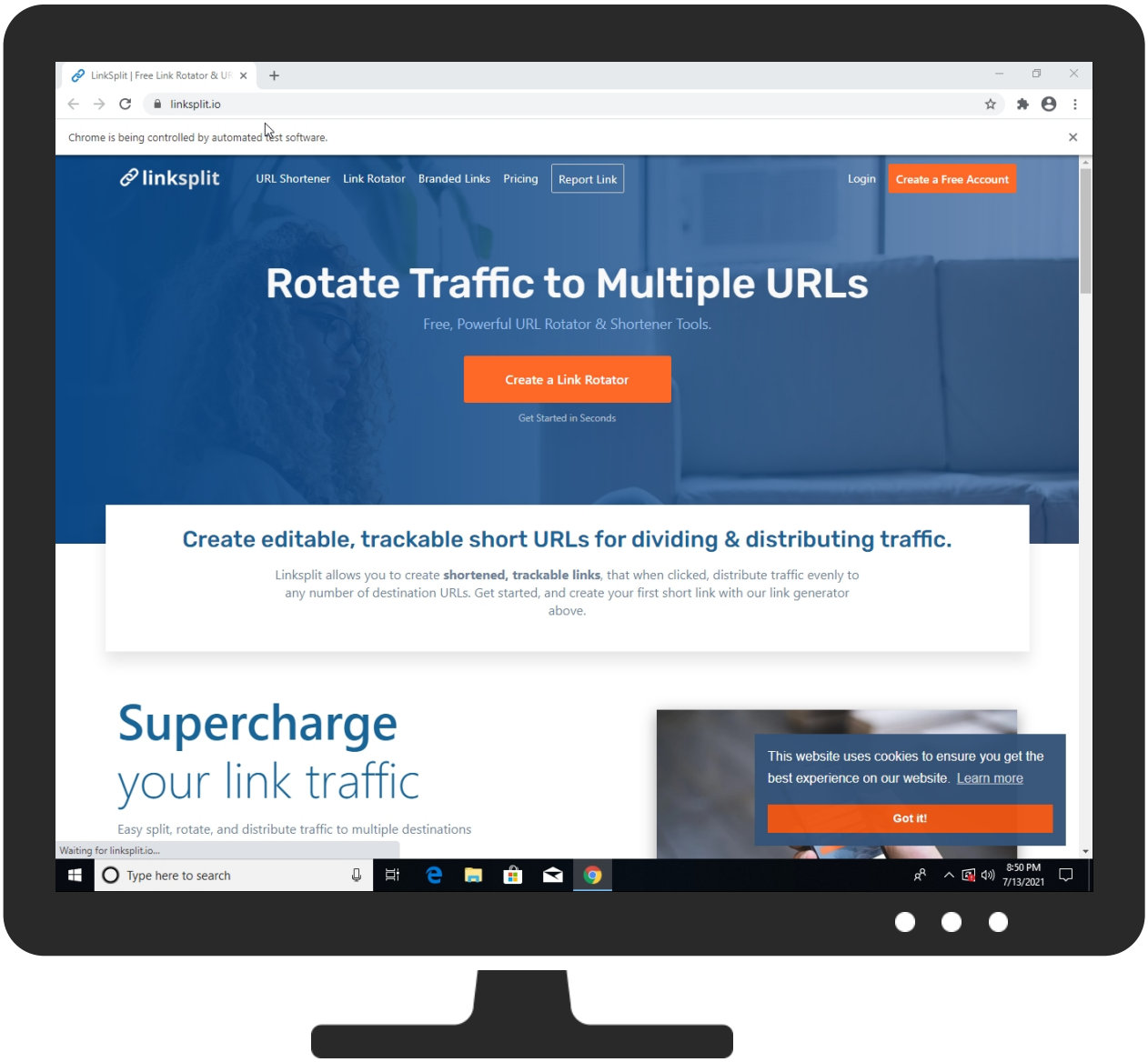


Screenshots

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://linksplit.io/	0%	Virustotal		Browse
http://https://linksplit.io/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://js.hs-analytics.net/analytics/1626202200000/4785246.jsaD	0%	Avira URL Cloud	safe	
http://https://www.osano.com/articles/gdpr-compliance-regulations	0%	Virustotal		Browse
http://https://linksplit.io/users/registerCreate	0%	Avira URL Cloud	safe	
http://https://li.sten.to/js/dist/index.min.js?v=112	0%	Avira URL Cloud	safe	
http://https://js.usemessages.com/conversations-embed.js	0%	URL Reputation	safe	
http://https://js.usemessages.com/conversations-embed.js	0%	URL Reputation	safe	
http://https://js.usemessages.com/conversations-embed.js	0%	URL Reputation	safe	
http://https://js.usemessages.com/conversations-embed.js	0%	URL Reputation	safe	
http://https://linksplit.io/users/googleAnmelden	0%	Avira URL Cloud	safe	
http://https://js.usemessages.com/conversations-embed.jsaD	0%	Avira URL Cloud	safe	
http://https://www.osano.com/features/consent-management	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hs/cta/cta/current.js	0%	Avira URL Cloud	safe	
http://https://cmp.osano.com/2sUBzx7wRdAfu6J2kkS/8e547744-886f-4a9b-a90f-7e96a47aa604/osano.jsaD	0%	Avira URL Cloud	safe	
http://https://linksplit.io/branded-linksLinkSplit	0%	Avira URL Cloud	safe	
http://https://linksplit.io/link-rotatorFree	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hubfs/v2/js/blog_single.jsa	0%	Avira URL Cloud	safe	
http://https://linksplit.io/utm-shortenerPFree	0%	Avira URL Cloud	safe	
http://https://linksplit.io/js/url-shortener.jsa	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/head-dlb/static-1.149/bundle.production.js	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hubfs/v2/js/common.js	0%	Avira URL Cloud	safe	
http://https://js.hubspotfeedback.com/feedbackweb-new.js	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hubfs/v2/js/blog_single.jsaD	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hs/cta/cta/current.jsaD	0%	Avira URL Cloud	safe	
http://https://li.sten.to/Create	0%	Avira URL Cloud	safe	
http://https://linksplit.io/js/system.jsaD	0%	Avira URL Cloud	safe	
http://https://js.hs-banner.com/cookie-banner	0%	URL Reputation	safe	
http://https://js.hs-banner.com/cookie-banner	0%	URL Reputation	safe	
http://https://js.hs-banner.com/cookie-banner	0%	URL Reputation	safe	
http://https://static.hsappstatic.net/conversations-visitor-ui/static-1.11495/bundles/visitor.js	0%	Avira URL Cloud	safe	
http://https://linksplit.io/images/favicon.ico4/	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/hubspot-dlb/static-1.129/bundle.production.js	0%	Avira URL Cloud	safe	
http://https://linksplit.io/link-rotator#	0%	Avira URL Cloud	safe	
http://https://li.sten.to	0%	Avira URL Cloud	safe	
http://https://sten.to/2	0%	Avira URL Cloud	safe	
http://https://sten.to/9	0%	Avira URL Cloud	safe	
http://https://li.sten.to/users/register	0%	Avira URL Cloud	safe	
http://https://js.hs-banner.com/4785246.js	0%	Avira URL Cloud	safe	
http://https://www.osano.com/articles/gdpr-compliance-regulationsC12	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hubfs/v2/icons/favicon/favicon-32x32.png	0%	Avira URL Cloud	safe	
http://https://linksplit.io/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hs/hsstatic/HubspotToolsMenu/static-1.103/js/index.js	0%	Avira URL Cloud	safe	
http://https://linksplit.io/users/google6	0%	Avira URL Cloud	safe	
http://https://www.osano.comh	0%	Avira URL Cloud	safe	
http://https://js.hubspotfeedback.com/feedbackweb-new.jsaD	0%	Avira URL Cloud	safe	
http://https://linksplit.io/users/register1Create	0%	Avira URL Cloud	safe	
http://https://linksplit.io/js/bootstrap.bundle.min.js	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://linksplit.io/js/system.js	0%	Avira URL Cloud	safe	
http://https://cmp.osano.com/	0%	Avira URL Cloud	safe	
http://https://js.hs-analytics.net/analytics/1626202200000/4785246.js	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/5.1.1/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://cmp.osano.com/2sUBzx7wRdAfu6J2kkS/8e547744-886f-4a9b-a90f-7e96a47aa604/osano.js	0%	Avira URL Cloud	safe	
http://https://static.hsappstatic.net/feedback-web-renderer-ui/static-1.6417/bundles/fetcher.js	0%	Avira URL Cloud	safe	
http://https://browser.sentry-cdn.com/6.8.0/bundle.min.js	0%	Avira URL Cloud	safe	
http://https://linksplit.io/A?6	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hs/hsstatic/HubspotToolsMenu/static-1.103/js/index.jsaD	0%	Avira URL Cloud	safe	
http://https://www.osano.com/hubfs/v2/icons/favicon/favicon-32x32.png&	0%	Avira URL Cloud	safe	
http://https://sten.to/u	0%	Avira URL Cloud	safe	
http://https://osano.com/o	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=OPT-PPQPK94aD	0%	Avira URL Cloud	safe	
http://https://linksplit.io/users/google	0%	Avira URL Cloud	safe	
http://https://sten.to/x	0%	Avira URL Cloud	safe	
http://https://linksplit.io/pixel-url-shortenerm	0%	Avira URL Cloud	safe	
http://https://www.osano.com/_hcms/forms//embed/v3/form/4785246/162149ed-dd87-457a-9bc7-d18001586306?callba	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=OPT-PPQPK94	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cookiesandyou.com	143.204.98.55	true	false		high
browser.sentry-cdn.com	151.101.2.217	true	false		unknown
forms.hubspot.com	104.19.154.83	true	false		high
static.cloudflareinsights.com	104.16.94.65	true	false		unknown
pop-eda6.mix.linkedin.com	108.174.11.69	true	false		high
li.sten.to	104.26.0.226	true	false		unknown
js.hs-analytics.net	104.17.70.176	true	false		unknown
ajax.cloudflare.com	104.16.168.35	true	false		high
track.hubspot.com	104.19.154.83	true	false		high
fresnel.vimeocdn.com	34.120.202.204	true	false		high
no-cache.hubspot.com	104.19.155.83	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
group46.sites.hscoscdn40.net	199.60.103.228	true	false		unknown
perf.hsforms.com	104.16.85.5	true	false		unknown
js.usemessages.com	104.17.235.204	true	false		unknown
js.hubspotfeedback.com	104.17.113.162	true	false		unknown
star-mini.c10r.facebook.com	157.240.196.35	true	false		high
js.hs-banner.com	104.18.20.191	true	false		unknown
client.relay.crisp.chat	134.209.238.18	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
static.hsappstatic.net	104.17.9.210	true	false		unknown
f.hubspotusercontent40.net	104.16.183.114	true	false		unknown
app.hubspot.com	104.19.154.83	true	false		high
feedback.hubapi.com	104.17.202.204	true	false		high
linksplit.io	104.21.2.221	true	false		unknown
client.crisp.chat	104.18.28.91	true	false		high
vimeo.com	151.101.192.217	true	false		high
www.googleoptimize.com	216.58.215.238	true	false		unknown
vimeo.map.fastly.net	151.101.0.217	true	false		unknown
s.osano.com	52.45.97.212	true	false		unknown
js.hsleadflows.net	104.17.234.204	true	false		unknown
api.hubspot.com	104.19.154.83	true	false		high
googleads.g.doubleclick.net	172.217.168.34	true	false		high
tattle.api.osano.com	107.20.89.168	true	false		unknown
d2gt2ux04o03l1.cloudfront.net	143.204.98.25	true	false		high
consent.api.osano.com	143.204.98.90	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cookiesandyou.com	143.204.98.44	true	false		high
unpkg.com	104.16.122.175	true	false		high
www.google.ch	172.217.168.3	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
vimeo-video.map.fastly.net	151.101.114.109	true	false		unknown
i.vimeocdn.com	unknown	unknown	false		high
www.osano.com	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
use.fontawesome.com	unknown	unknown	false		high
f.vimeocdn.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
cdn.osano.com	unknown	unknown	false		unknown
cmp.osano.com	unknown	unknown	false		unknown
accounts.youtube.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
player.vimeo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.osano.com/articles/gdpr-compliance-regulations	false	• 0%, Virustotal, Browse	unknown
http://https://linksplit.io/link-rotator	false		unknown
http://https://li.sten.to/	false		unknown
http://https://api.hubspot.com/cors-preflight-iframe/	false		high
http://https://www.cookiesandyou.com/disable-cookies/windows/chrome/	false		high
http://https://linksplit.io/pricinghttps://linksplit.io/users/login	false		unknown
http://https://app.hubspot.com/conversations-visitor/4785246/threads/utk/771df7ec49e349bcabe954647659ea25?uuid=fa5a06b31d3c408c8b4137e44cfb2a3a&mobile=false&mobileSafari=false&hideWelcomeMessage=false&hstc=106899676.fb78b4cfb86ad3bcbc24353d8af15f34.1626202312268.1626202312268.1626202312268.1&domain=osano.com&inApp53=false&messagesUtk=771df7ec49e349bcabe954647659ea25&url=https%3A%2F%2Fwww.osano.com%2Farticles%2Fgdpr-compliance-regulations&inline=false&isFullscreen=false&globalCookieOptOut=null&isFirstVisitorSession=true&isAttachmentDisabled=false&enableWidgetCookieBanner=false&isInCMS=true&hubspotUtk=fb78b4cfb86ad3bcbc24353d8af15f34	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	no-cache.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.16.122.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
104.18.20.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
151.101.0.217	vimeo.map.fastly.net	United States		54113	FASTLYUS	false
143.204.98.90	consent.api.osano.com	United States		16509	AMAZON-02US	false
52.45.97.212	s.osano.com	United States		14618	AMAZON-AESUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
143.204.98.55	cookiesandyou.com	United States		16509	AMAZON-02US	false
104.16.168.35	ajax.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.19.154.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
151.101.192.217	vimeo.com	United States		54113	FASTLYUS	false
134.209.238.18	client.relay.crisp.chat	United States		14061	DIGITALOCEAN-ASNUS	false
199.60.103.228	group46.sites.hscoscdn40.net	Canada		23181	QUICKSILVER1CA	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
199.60.103.28	unknown	Canada		23181	QUICKSILVER1CA	false
104.26.0.226	li.sten.to	United States		13335	CLOUDFLARENETUS	false
157.240.196.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
104.17.70.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.98.25	d2gt2ux04o03l1.cloudfront.net	United States		16509	AMAZON-02US	false
104.16.94.65	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false
104.17.235.204	js.usemessages.com	United States		13335	CLOUDFLARENETUS	false
104.16.183.114	f.hubspotusercontent40.net	United States		13335	CLOUDFLARENETUS	false
104.17.9.210	static.hsappstatic.net	United States		13335	CLOUDFLARENETUS	false
172.217.168.3	www.google.ch	United States		15169	GOOGLEUS	false
104.17.113.162	js.hubspotfeedback.com	United States		13335	CLOUDFLARENETUS	false
108.174.11.69	pop-eda6.mix.linkedin.com	United States		14413	LINKEDINUS	false
104.21.2.221	linksplit.io	United States		13335	CLOUDFLARENETUS	false
151.101.114.109	vimeo-video.map.fastly.net	United States		54113	FASTLYUS	false
34.120.202.204	fresnel.vimeocdn.com	United States		15169	GOOGLEUS	false
104.17.202.204	feedback.hubapi.com	United States		13335	CLOUDFLARENETUS	false
104.17.234.204	js.hsleadflows.net	United States		13335	CLOUDFLARENETUS	false
172.217.168.34	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.2.217	browser.sentry-cdn.com	United States		54113	FASTLYUS	false
104.16.85.5	perf.hsforms.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
143.204.98.44	www.cookiesandyou.com	United States		16509	AMAZON-02US	false
104.18.28.91	client.crisp.chat	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	448253
Start date:	13.07.2021
Start time:	20:49:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://linksplit.io/
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:	13
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@58/271@61/41

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://cookiesandyou.com/ • Browse: https://linksplit.io/url-shortener • Browse: https://linksplit.io/link-rotator • Browse: https://linksplit.io/branded-links • Browse: https://linksplit.io/pricing • Browse: https://linksplit.io/users/login • Browse: https://linksplit.io/users/register • Browse: https://linksplit.io/utm-shortener • Browse: https://linksplit.io/pixel-url-shortener • Browse: https://li.sten.to/ • Browse: https://linksplit.io/users/google • Browse: https://www.cookiesandyou.com/ • Browse: https://www.cookiesandyou.com/about-cookies/ • Browse: https://www.cookiesandyou.com/disable-cookies/ • Browse: https://www.osano.com/articles/ccpa-guide • Browse: https://www.osano.com/articles/gdpr-compliance-regulations
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:51:25	API Interceptor	1x 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:\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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2A0
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\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.145340414441777
Encrypted:	false
SSDEEP:	6:kKYl8doW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:H5kPlE99SNxAhUe0et
MD5:	5E96B5A1EA72C3CE17DF63DD971C22BA
SHA1:	FF44A365C2E3D6B54C24090EBFC8239A8D15E62C
SHA-256:	D4B17EC2AD356DE94C000C967D1C7DAEBE10C075FE3B49614E1955E1811ED6EB
SHA-512:	360AB56B7285BB3AFDC67E5E2FD10C16E1D1E878BA41D5CC5026669B4D10022F6408400B02A1E42F1F834E32CF8108BCB6C3D3841E7F7B22308DD54D2673FFA
Malicious:	false
Reputation:	low
Preview:	p..... .....x..(..... .....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\Local\Google\Chrome\User Data\1941c3e5-24e0-4f79-974c-0acd803e74dd.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7507436335483275
Encrypted:	false
SSDEEP:	384:LzN+K0rxwIXKhN2rjvKC3ZicdHY1G90r/cu8xxgskfr36mb4vsO6yBOoMCNz1+3Z:/a1RCchFMers+cE/3G+KcqeBu9
MD5:	1F4AC3898A3B4D448FBEC3BD9CD4F704
SHA1:	B564AC7A3D3CABDC3F9CBE558C1EF2F561A1578A
SHA-256:	9BBB85BC72B376031E24DE62A3A929F0DC9F542C979A186E4A01DCABB7915FB9
SHA-512:	A6A50D06C5CDC07910CBBBF2740F7E3533333F7E4CBC64CD985B1F34F5B9FB84F9757614A06257F57078FEECE3979652574446335E6F9C2F0E71A048E27D227A
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....?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\31613d4a-5d5d-42ae-a374-6f1caf09c952.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751265916000241
Encrypted:	false
SSDEEP:	384:1zN+K0rxsbIGVjFKhN2rjvKC3ZicdHY1G90r/cu8xxgskfr36mbvBvsO6yBOoMC4:FWa1RCcAFMers+cE/3G+KcqeBC
MD5:	4971C3020C0D723BED26F4FB4C184C62
SHA1:	F2613E596E662FDF41687CD1F9D20EF719BCEA45
SHA-256:	3A48F2064D8C193B6AFB456AC017328BCE30D6A1BE15BA78764E26D763088647
SHA-512:	05937CA99D4D527BB349E44215FF55912DEFBE648C16DDFFECFBADCFBBA7FD4F6EE85DDFF6746FE110F0B3C004D2D9B57A9921513FEAC994411438C2947573
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\31613d4a-5d5d-42ae-a374-6f1caf09c952.tmp	
Preview:	.t.....*...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....?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\4c6363e9-f723-4383-ae27-2de825938355.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):	165309
Entropy (8bit):	6.050232095083586
Encrypted:	false
SSDEEP:	3072:PwHgiNHZgSY7jMeK2oD7SbACkNibl3nzhFHYLmxFcbXafIB0u1GOJmA3iuRT:oHgK/sjMz2oD7SEnM4CfaqfIlUOoSiuJ
MD5:	BC818AAACDA38B4777FCD876E98E2F01
SHA1:	6AF350792245363E9167FAC28CFBF2D13FEBE421
SHA-256:	C47164465854657E09CF3385F51C488470A09202AB0482E9C0DDF10F8F4DDA1E
SHA-512:	12FC39AA76E6767028A66FA9D7BE9F3F4DFA73719CF154738D0051523E6FB8BFAFBDBF8BFDA726A4AB1073F28966A267835E15C678F4E88749D6809DDAC8ACC 6
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62620225317884e+12,"network":1.626202254e+12,"ticks":5380357873.0,"uncertainty":2439650.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715518094"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\62e717b9-a522-4be1-a0d1-95e8bcd4669d.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):	173767
Entropy (8bit):	6.079565185826315
Encrypted:	false
SSDEEP:	3072:PIpKHgiNHZgSY7jMeK2oD7SbACkNibl3nzhFHYLmxFcbXafIB0u1GOJmA3iuRT:Q4HgK/sjMz2oD7SEnM4CfaqfIlUOoSiu
MD5:	F68ACE66F10D587866435B6257F258F0
SHA1:	40813C8C30C56F02D1508C76248A575279E0366C
SHA-256:	FEA432330E1B6154422C85687804B7435D281EE4E7056AA5874233456E79FB9D
SHA-512:	E34B9CB9FD6E4928E3FB9B1ACCE980D010628260C0CC47ACF72CC01D4E1BF2DFAB6278E984D8808B46021DC2E6B54D09DFB51EDFE0F5C30F555E3C5A7A2DD 5E5
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62620225317884e+12,"network":1.626202254e+12,"ticks":5380357873.0,"uncertainty":2439650.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715518094"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\7549e725-e65c-4482-a7da-0aa3d7dbe661.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):	173765
Entropy (8bit):	6.079564521590724
Encrypted:	false
SSDEEP:	3072:2hptHgiNHZgSY7jMeK2oD7SbACkNibl3nzhFHYLmxFcbXafIB0u1GOJmA3iuRT:afHgK/sjMz2oD7SEnM4CfaqfIlUOoSiu
MD5:	42E70725FC8FFC3A49382BAEF85BB85B
SHA1:	F23E6237685CB51D56855959B534B90F2EE62593
SHA-256:	D0D3D01E4AFA776207C090A00AB4F875177B7B40D3765CA545DA2CD70142CD2F
SHA-512:	A05167FD590FCABCB89B19B3B695F1AC4D706B1A2FE9B474923156C9B6E9CE8620448B91080CCC999A3382927EBE838C4B8A15559A60F3D3412DC464F0B5EBE E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\7549e725-e65c-4482-a7da-0aa3d7dbe661.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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62620225317884e+12,"network":1.626202254e+12,"ticks":5380357873.0,"uncertainty":2439650.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\99c90fc5-674e-40d7-80d6-a1d673242fde.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):	173765
Entropy (8bit):	6.07956357700997
Encrypted:	false
SSDEEP:	3072:2up1HgiNHZgSY7jMeK2oD7SbACkNibl3nzhFHYLmxFcbXafIB0u1GOJmA3iuRT:d/HgK/sjMz2oD7SEnM4CfaqfIlUOoSiu
MD5:	EBE8BE6D5054F69F3BBAF61DB5226F84
SHA1:	EA3EC0C6B919323F1941DF3793DF3116CFA12959
SHA-256:	2084A0DC84117E02E93EE1CFD2485EF191137B08D7C9BE0B05BBBD2D2EDF4D79
SHA-512:	9FDEDAF8723F0FE5CF609B104F16A1BBC7F93DC24974313F98F25F5A7DA0B88AB2CADE6DA7837284FE15663210BA4D9AC538475BAE64E9F9D2BD29013B304A37
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62620225317884e+12,"network":1.626202254e+12,"ticks":5380357873.0,"uncertainty":2439650.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

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:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
Malicious:	false
Reputation:	low
Preview:	sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\352fabad-778a-4709-94f0-93586ca015e5.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):	2542
Entropy (8bit):	5.593903621827216
Encrypted:	false
SSDEEP:	48:YV1UvVwUXieUU6UUhZZhUCNUpUIh7KUlcU5RzHUfqPeUekUeC4cUNDwUAUeP:k1UeUXieUtUU/ZhUCNUpUkKUlcU5RzHy
MD5:	5595074BABFC27F377E9C9BD98FCEC67
SHA1:	32E64D0061CD010509FF5D3D7C5E2D7C9EE1AEC9
SHA-256:	DB8217B90238C8FE12D2BF9DE2D569107CCD84B720F12FF3C2B4FD67BFD97065
SHA-512:	3B30145921CF97B8ED661013F426E887869C2C6A6E8D1F9EC0798424E4A75485F9DBDB22E76DD8E0F3E6ED08558FBEC38DD4F9A66C6C57FD2D65B9EBC07EEF4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\352fabad-778a-4709-94f0-93586ca015e5.tmp

Preview:

{"expect_ct":[],"sts":[{"expiry":1657738255.073706,"host":"CZU0ovCjWSlHcoYuG0ZSGiph68/Tvd43RsTejedDQms=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626202255.073712},{"expiry":1641982255.29997,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626202255.299976},{"expiry":1657738255.105937,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626202255.105943},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1657738262.930357,"host":"YkShQ/gtROgeLN+DIPuXqOKZPnlNzRZ2CaurTbeKmUQ=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626202262.930362},{"expiry":1657738255.492334,"host":"e3SziuwfuO2UvuBno+qkR1ObHAzZmSUoJhrc7dbP1Uo=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4aa72155-39fb-457b-aafc-0842be7fb5fb.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low

Preview:

{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7656b8ff-8b74-49b2-a544-0d9f065a9342.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):	5855
Entropy (8bit):	5.169159293314827
Encrypted:	false
SSDEEP:	96:nELVHyMFfF512VNGNgIKIKY5k0JCKL8EkZ81ZPbOTztVuHn:nELEMFfLczQgIwYh4KTkZ8YM
MD5:	9699651E2A7B4815387511FDC4E67B30
SHA1:	D232250FD918463FCB19F972180A16CD6D474349
SHA-256:	84355F6C6379B1F195E099F8EDA3943AE0C4062DA00B6E6BB45B6B096A25F146
SHA-512:	8589189025D0567D4EB2C711FDDC70CB57EA0D535F6F1F1EE3B3653D05CE2DF6C66404271724D44141C7BB7ADCB9A1003E6D65E762616CB7EB7BD0F6223EFC6
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13270675849817000","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7793c590-986c-47ca-b67d-7973781f8885.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):	5176
Entropy (8bit):	4.959688293186276
Encrypted:	false
SSDEEP:	96:nELxtMpIKIKW5k0JCKL8EkZ81VbOTlVuHn:nELrMpIwWh4KTkZ8d
MD5:	017F1C5A17279E8E50B67EE014C215D7
SHA1:	9CAEE5D2C65A420394C3846997682568E9F70F83
SHA-256:	7D545C4AD37A8EB3205E17C1AB5A5A50CFD379465A6F7A976AA9DD442D007A59
SHA-512:	EFFA119385263A8DC085560F754E1A67179B0311B926F1822AE18A0FB2BDE7FC7607190436F7C0B84FFFBA2A63BC9265F2047C48ECB9AFE31B352B732C8F932B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7793c590-986c-47ca-b67d-7973781f8885.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270675849817000","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8ba6e14f-329d-4f19-be85-c5e1b47b90a3.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):	5882
Entropy (8bit):	5.171237255570547
Encrypted:	false
SSDEEP:	96:nELJ0yMFfF512VNGNgIKIKV5k0JCKL8EkZ81ZPbOTztVuHn:nELRMFfLczQgIwVh4KTkZ8YM
MD5:	842CD27DFE7CBD822070A332E587B740
SHA1:	56B486EBA8CB3FF995C1AE9ACA48325EABDCCFD2
SHA-256:	4AFB7D110F82CA289D399C091E691F856F43B8C8AE91B2CCDFD21EE43C9465FF
SHA-512:	58A0659D0522918FDCFABE5562AB57BD625332CF150C8F7DA9DBEA6DBB59B252650C521E5BC558E45123B6D7D2299A8E8ABCA5BE152B1C9CF16A862B9FF9A4 66
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270675849817000","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","2042016"],"daily_recei

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):	334
Entropy (8bit):	5.23056994676006
Encrypted:	false
SSDEEP:	6:mjRLa0Q+q2Pwkn23iKKdK9RXXTZIFUtpyRLupdWZmwPyRLupQVkwOwkn23iKKdKT:SLa0Q+vYf5Kk7XT2FUtpCLcdW/PCLcQh
MD5:	3FE5CC52B65EEBC6919720E560A19F76
SHA1:	765AD2D31B8CE028BA803710F76EDBDC35A6D075
SHA-256:	9BD9296F997B7C8E17C402BD9EC1B7AF961CF897AFD2D5C0793090F7DDEF829C
SHA-512:	71384DEEE28D3B9E83FC64C47E405D2B80828F044EADE1ADA94B865443FEFBDEADB252B53AF17CE1C2AFC6FCAB027DEFA499AB3BF2A077880935F1337100E1 39
Malicious:	false
Reputation:	low
Preview:	2021/07/13-20:51:04.588 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/13-20:51:04.590 19cc Recovering log #3.2021/07/13-20:51:04.590 19cc 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):	318
Entropy (8bit):	5.226208706903218
Encrypted:	false
SSDEEP:	6:mjRL5ZQ+q2Pwkn23iKKdKyDZIFUtpyRLI0dWZmwPyRLMQVkwOwkn23iKKdKyJLJ:SL5ZQ+vYf5Kk02FUtpCLFdW/PCLMQV5E
MD5:	09FEDC86E41FFD7A90BB92D419DC6BF6
SHA1:	53E80190DD680FAD9A2FEA7F87E9EE36486DC9FF
SHA-256:	E7B748A750D1FD7E05BF5D57E75E6F53CC74540C8CC28E7F3EB701D80A48D126
SHA-512:	8F0AE050C1B6DE77933355E50415BE59C23AFF4EC5A5BA67F79A7C7E9B44709F15072878B880D67CAE2C5CF49800756694EA2DC54A5486A5C03E592D83C9D07
Malicious:	false
Reputation:	low
Preview:	2021/07/13-20:51:04.580 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/13-20:51:04.582 19cc Recovering log #3.2021/07/13-20:51:04.583 19cc 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\0063b110928a54f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	30055
Entropy (8bit):	5.742681711788744
Encrypted:	false
SSDEEP:	768:RVibDlZAt6cjzQ7A4qPYuSoity+lhgfkf:ulZAgNAMuRit0fa
MD5:	ECE8B0490937A3769E126C1CBB84C3BC
SHA1:	A86203BA0EDB7C200ABA065A4DB3BBD853EB3494
SHA-256:	EFFD180094626F2BFB98978A0DB1D8EF3FC0993BF4BD21A1FDE4D8A73F3447C4
SHA-512:	999C777B1F0D469C91800ED8E35EF3DB44C342C372A9AB692490E96B83459CD9A3A53E1D76A7A01A8F3F1571F1FDC52DB280CA84D589C75AD3CFB60E1A2688
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....X5...._keyhttps://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js .https://linksplit.io/..B..%/.....]...P..L..@...Q...7.@...+^..A ..Eo.....%l.....A..Eo.....'.HQ....O....9....D.....@.....(S.@..`8.....L`.....(S....`.....L`t....@Rc.....Qb.]+....e.....Qb...g....t.....S. b$.....I`....Da....Z.....Qe.N3.....hasInitialised.....aB.....QdV..t....escapeRegExpC..Qcj.a.....hasClassC..Qc._{.....addClassC..Qd.....removeClass.C. Qf.n.+....interp olateString...C..Qd..,....getCookie...C..Qd.=.....setCookie...C..Qdn[.....deepExtend..C..Qc.P.....throttleC..Qbj.v\....hashC..Qd.Y.?....normaliseHexC..Qd..4.....getCon trast.C..Qd.Y.....getLuminanceC..Qc...U....isMobileC..Qe.....isPlainObject...C..Qe.....traverseDOMPath.C.(S.<.`.....L`.....Qc.A....replace..0Qj.c."...[\-\[\]\/\{\}\(\)*\+\? \.\\\^\$|]....Qb...L....\$&...K`....Di .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\025bff122fc1bcb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.893358264169726
Encrypted:	false
SSDEEP:	6:m3YGL+MIwJJWrs6a10qlm4sRK6t8dN0gc3LPrroqlm4:aIwvWrsy7ras1PI
MD5:	2A28BD84CD6856F51A9CC02CCBC3DDBD
SHA1:	C775EA622913AF0CF414C551A87C0FB2C9015A28
SHA-256:	5B7AB4A946784CEE8D6A26C1A6EB3F678D6E6F8A87F12981365EB5D4906E1ACA
SHA-512:	5BC97B448ED2FBCCE86EC7EA18BD7FCD3469EF53B588F3A21C0C094643D0C7E10BE114786EEDA48C454FC9D04C692A4A5F4C46C19663A2F83ABE2CE6B3932 0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H.....E...._keyhttps://www.google-analytics.com/analytics.js .https://linksplit.io/..H..%/.....X.m0...;..`.x.X.....9....A..Eo.....A..Eo..... ..H..%/../..74B519361B5D42C980B6BC6F993B15473720D473C79D62EFA554799582A16992.....X.m0...;..`.x.X.....9....A..Eo.....(8.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\077962262e85ed64_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.412600733185162
Encrypted:	false
SSDEEP:	6:m3PY0OCZlXZ5yaXGb3/wdqdCK/48Qq34K4HZK6t:GnlXZ5/GrQmD/iB
MD5:	3D6CFDE7182DDF30BB2CCDD94062931D
SHA1:	F4640798BA2E4D2B60F0F40A17B06E0D67E2BB69
SHA-256:	E19612D43F10B07D1CAC377C5041BC94EB113FBD73093F6A6F9D6094CDCE26A3
SHA-512:	652BE854BDC1ACF38E658ABE30A9A782D555E60894E5E931EF42C69BD728E3AC0BC779834ED9FC6E4D4415C75D0351C58FE70414DFBF07E1BDF23E19969B27 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....._keyhttps://unpkg.com/ionicons@5.2.3/dist/ionicons/p-206e6cb0.entry.js .https://sten.to/x....%/.....h.....FY.Tk..1.8^.#.n.;...).c..'"....A..Eo.....^_... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a145b60b66c4d9d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	398
Entropy (8bit):	5.888850707898078
Encrypted:	false
SSDEEP:	12:XEm80vbm4dXmrlfMMZXlazLYh3J5P1+jAE9l1:XfnvbTnMZXlanYpJ5P1i9r
MD5:	E65B288498F368F7FDA4F4A1F901FF10

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a145b60b66c4d9d_0	
SHA1:	6E7CF525EFED9F77D8DEA3775815168498294A9E
SHA-256:	A092B49EFCAD58A6A3DCFC8B7B5A385D9E5669925FFBC86C9ED28314A5353866
SHA-512:	338D95E58156F448714F562BF95FB2A527C123E4C6F83DAE28867CE4382100CD9D7EDE517624470015386A77DD1501679A6638B4807A103CDDE74FC24CD43E62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.de.nfC-qpizUn4.O/am=B8BxhwlIGCABAEAOAAAAAAAAAHA0CCgHczzDJw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax2rlQXvBiM_NlHa1QKxh9v2Yn_xOw/m=sy7y,sy7z,sy80,sy82,sy83,sya0,pwd_view .https://accounts.google.com/..+..%/.....C.....nzD...d./.1...!..y.t.IO.....N..A..Eo.....A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ea68543a07da8e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.499731026405878
Encrypted:	false
SSDEEP:	3:m+lof/a8RzY8ciAnGY2IFPWFvDH4R3eelHCCPg//CjIuVvRj00MxRoyg4mCXpK5M:mv/XYWAnN1cq3IMgqUIJgh2CZK6t
MD5:	FFEC1C70B30FCFB9FE28D2350AF94E2B
SHA1:	1A000B4169757859761C3E343DB9B64F19D9D6DE
SHA-256:	1FC173589E5970D8E982A398957712CF5BB91B40DFF8A40422F63E5F6AE59101
SHA-512:	EA77214AB0B75AC4AAD3385625242453709C3DDAA7DD13E98D2EB5B9D5AE55083247D118D21829E60A671965F28075B3F7B546903CF001830B224702CB99B547
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...$b.k...._keyhttps://browser.sentry-cdn.com/6.8.0/bundle.min.js .https://sten.to/9....%/.....*.....[g.J..z.R..q@7....`...N..A..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1022efe5884231f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93760
Entropy (8bit):	5.773444970841206
Encrypted:	false
SSDEEP:	1536:ieztFvM4y768B0Y7Cm7xiCY7Na9Ph1pJjWHSnZoGeOi6:pztVMY8rB7LY7NSDzP/7
MD5:	27C8B521426AEBDB1A375379BDCC5A51
SHA1:	0E66343332A0C3345186F8186A4DABC47A829FD3
SHA-256:	AC8C1E6ECCC115DD089F603C3C581562A78C2A17E46A8E12FFBA9EAC64AB44E1
SHA-512:	A3E16F7D77CEF8C96B986353FA0EB3AE9132BFD0872EF0A37DE09C2DD86ABF28928E2CA4162122C009993B9B3F359BE98516CF0F4D0833A12D51F008721CF9A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....(....86775C4A5DE804838120F9125AB3C5CA751CE492315DD83C535DB2705F1ADEF8.....'..I....O ....l..+.....".....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....L.....Q.@..r.....module....Qc.Z.!....exports...Qc..l.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.... ...I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.jsa.....D`....D`....D`.....`d...&...&..!.&....&.(S...".`.C.....Q.L`.....q.Rc4.....M...Qb."{.....d.....Qb.]+....e.....Qb.?.....f.....Qb.....h.....S.....Qb.w.....j.....Qb. 0s....k.....Qb.VM.....l.....QbB..<....n.....QbJ..o....o.....Qb>.....p.....Qb..z.....q.....Qb./.....r.....Qb..{.....s.....R....Qbzd3.....v.....Qb...J....w.....Qb.A.....x.....Qb.*Fx....y.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\12157c5daace4a72_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.4087221409868675
Encrypted:	false
SSDEEP:	6:m7zVYUyALfPAtPdTaHqXv6eg4EWKuao4aK6t:Mz9TLWdTSc5cm
MD5:	7EF5AE25C6650BF12B0EF784F2657A61
SHA1:	23EAC357F304619E7FE3388D4160BAAE4AB02B5A
SHA-256:	D42376F607720FC60FB9A96A9795AAFDD430C554C9FBCC807B92E2866E72DC2E
SHA-512:	C102F0B4E6E9613EF1C8C63B187F8F7A74FB746BE41FAF49D5CE485AEAAA2C108193086F3D239942EAFBB566559B5CF6B3CD451D9E3A9E083B0B51209233737
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.../)U...._keyhttps://li.sten.to/js/dist/index.min.js?v=112 .https://sten.to/.c...%/.....-.....}d-.....N.u.....*.y.....A..Eo.....w7S&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1817f6a17d4fee61_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1817f6a17d4fee61_0	
File Type:	data
Category:	dropped
Size (bytes):	481
Entropy (8bit):	5.840455829609872
Encrypted:	false
SSDEEP:	12:msVtrWyIOkyhwlp7uAbHUIOkyY+lfXdgxB8F8s2IOkyx:mUWyILyhwzUILyY+FtgxB8mJILy
MD5:	8D5A67882A988BDF16718A60CCD39A96
SHA1:	3CDEE6DE3B7FDF64A894D96D6786EBAF47C3B09E
SHA-256:	9A91ADBC5EACAD2C4F4C3BCFBBEAD9A6BA110372CA81967054AD661D3419455E
SHA-512:	F2215A7659D16663DAD0A304191C70A122A842DF12314E019245B130641B674B084F998F151C90AD0DBE10B3EB4C2BA56CEC615CE5E16CDA656C0E910A63085
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...Su....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-157457758-3 .https://linksplit.io/..E..%/.....[-."V.S.#8.e.sc....%...`.U".O|/.A..Eo.....? SN[.....A..Eo.....E..%/.8-..980221479666CE22D890A9047E86279F6953222EA87CF275429383A4EB83A99E.[-."V.S.#8.e.sc....%...`.U".O|/.A..Eo.....;5L .....E..%/.8-..28C2D8A60D2835B4B713C908A532C818A686FBD5856121E93AFC6C1D0CB50347.[-."V.S.#8.e.sc....%...`.U".O|/.A..Eo.....F.Z{L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18caefcf534d85fa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.488034059919971
Encrypted:	false
SSDEEP:	3:m+lUjyv8RzYM4hGWh4MGK8T/GYZA4BV2VN4RvFlHCMIgXBvutKuJU9ANVqmSyz1X:mPyEYM47at4qyKQtvJUiVdB1K6t
MD5:	71C6BB38F5360BE3C321150ECA5DAD29
SHA1:	4CA766920E9424FACE5B4EE2BF901BC689C9FC15
SHA-256:	9F3583709E8DCAC0B1DF1E84AD1573CC5AF73A4FD2ED959E465C69778A488A69
SHA-512:	FE7C03B709A78D327B09BD35325B34038A28BA455CE620312E781683E4F566F6F0BEB6F9287DBFF2AD68375B06DB0FD00B1B7F19B13602F78288BEBEBF351CCI
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...([g\...._keyhttps://client.crisp.chat/static/javascripts/client.js?6450942 .https://sten.to/.....%/.....-.....P...O^~D..A..,...e.A..Eo.....Y.W.....A..Eo.... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c5b580f843a2f86_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4112
Entropy (8bit):	6.109077645989583
Encrypted:	false
SSDEEP:	96:N4dSIx4wfRrE6RlM6Rc/d2FeqL6RhAIFYYHqIyE:KdkMBl9cCqhA4cE
MD5:	078A5F78C5535A1646E1E3A0DA5021A2
SHA1:	874086D3513758CD4FA48F54B9501CEB1717927A
SHA-256:	6BE43808BB6E16B1C8F309F7FB7DCDA80FC654198CE0561A5DD851845F81E753
SHA-512:	FE2AB49F546E057326F5B1DA1D899D67A7A23FFFC974F4786C6F1EA11C99A01A658FEC04FCD720E587571832D36E6B7BE386C80DF55627B41DAD04BC67430DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...<."o...._keyhttps://www.osano.com/hs/scriptloader/4785246.js .https://osano.com/.8K..%/.....M.....[..A..| ....."_..U.R.....y..A..Eo.....^.....A..Eo..... .....8K..%/.....'.....O....._..... .....(S....`b....TL`&....L`.....Qb...n...._hsp.(S..`^....@L`.....Qcz..?....document..Qe..e*....getElementById....Qez >$.....createElement....9..@Qn...\1...https://js.usemessages.com/conversations-embed.js.....Qb2.v.....src...Q.`.....text/javascript.....Qb.3f.....id....Qe.,[W....hasOwnProperty ....QdRg.....setAttribute. QfR.....getElementsByTagName..Qdv.....parentNode....Qd._&f....insertBefore..K`....D...h... .....&.(...&.Y.....&.(...&...&.Y....&...-.....-...%.-... %..Cw.....&....4.....&&.&.(...&.Y.....(...&.%.*..&.Z.....&.4....&.(...&...&.Y....&..*..&.(..!&.(..#&.Z....%.....(Rc.....I`....Da....<....(..h'.....@...@.@.....@.-....<P..... .0...https://w

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20072f99538be5cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	297
Entropy (8bit):	5.686715495253723
Encrypted:	false
SSDEEP:	6:monYM4qmODAZppaVWfd2RAXtoqTICNmiwnDRK6t:tL1mOYpBsRAXuypNPWr
MD5:	F6486EA78D9805522FE9F92BDC72137E
SHA1:	C919F5239803F2239D27F3FB456157B9F8CE7F22

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20072f99538be5cc_0	
SHA-256:	008EAE9113E39E3F48D784EEF4CF67A0B28B854807D7B5494026EDD92C58B1A3
SHA-512:	513ACCF37A2BA62EC76D47919BB9F123F05CFDD8ECA0FF18ECBF99DEFB177A3E04D53E30E79720CAF4766FCCE2F6569B7B8C87916BA226B0182578C2D5114A31
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....._keyhttps://client.crisp.chat/settings/website/7d36feaf-0b0c-49ef-a1f4-a2ea71a33f04/?callback=window.%24crisp.__spool.website_handler&16 14843734463 .https://sten.to/...%/.....c....."0y."C.X.8.....?E..\^.....xu.A..Eo.....@6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2296ffdb1de47d8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77944
Entropy (8bit):	6.079174674682629
Encrypted:	false
SSDEEP:	1536:1aFqpDxtvrVHCkOLLBALLMtifc02CwWA8B1pEzS/IwkTqiF9dzvMJ:cFqvtvpHCGLL7fc02CJJB3MDZ+iF9c
MD5:	44FFE48FFE1B1DC05A1AC2F2AAA519A1
SHA1:	936794327BAEA7EFE5E52F92E2F1114BF901857F
SHA-256:	A9DB91D7F804B7AA1BF520952C601F1F89B5D9EBE77EA75A21D83085C0F975BE
SHA-512:	B37AE5960AF1D1FB5C06CA33994ED08ACB02C3A1A727FB22EC6F12F27C9E8A04F21A58945F053C4027916522E93AA03F747C15409B162A33B9409089D90F2EAE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....UJ.....74B519361B5D42C980B6BC6F993B15473720D473C79D62EFA554799582A16992.....'.....O....8/..).P.....8.....`.....D.....(.....I.....@.....x.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qbvl.+....n.....Qb..nd....q.....Qb.$z.....r.....Qb...x....t.....Qb.wC.....v.....Qb.Jj.....x.....Qb..5.....y.....Qbn.....z.....Qb..M.....A.....Qb..[.....B.....Qbn44.....C.....Qb..I....F.....Qb.....E.....Qb:T.....D.....Qb.c.....G.....Qb~.....H.....Qb.%.....J.....Qbf.....I.....Qb...S....K.....Qb.....aa....Qb.....L.....Qb.].....N.....Qb&.].....O.....Qb.f)....P.....Qb.Y."....M.....Qb..2e....da....Qb.....ea....Qb..6p....Q.....Qb.+.....S.....Qb...@....R.....Qb.!(.....ia....Qbn.~Z....U.....QbFJ".....ha....Qb.;.....T.....Qb...S....V.....Qb>.....W.....Qb.dk.....Z.....QbJn9.....Y.....Qb.....X.....Qb.....ba....Qb:X6<....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26efd76df850a2b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77280
Entropy (8bit):	5.763828727976226
Encrypted:	false
SSDEEP:	768:fmpESuLJr56vVJRbSevOilZ1frMN64iv8WCB+VGVKofpgGnK7xrpmQ6:e+LVERbGRZ1TMN64i2VJfpgGK7xVo
MD5:	03BB919D43CABE6AB31F5D54B4961A38
SHA1:	C946D10514135B42BA5A8313C6EA0225288E0B72
SHA-256:	1EEB0273901C9D5C15B0D1F9B35543187AA40DC0DF5DC87EEE71B953E6BC7D15
SHA-512:	F551761899D32147B6C9905CF6F6ED7E3B54131BB121087191DA2419052771B933F72A784CC23EA5484BD3BF7883596713C9BC274BDC1AF3191FBC705AB71EB6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...<..F....28C2D8A60D2835B4B713C908A532C818A686FBD5856121E93AFC6C1D0CB50347.....'.j....O.....,..}.....D&..8..... .....(S.0..`.....L`.....(S...E&.`>L.....9.L`.....Rc.....Qb.^.e....data..Qb..U6....ba....Qb...v....ea....Qb.....la....Qb.._T....pa....Qb..8.....qa. .....Qb.....ra....Qb.....sa....Qb.&i.....ta....Qbfr."....ua....Qb.v.....va....Qb.c.....wa....Qb.....xa....Qb6.X.....za....Qb.....Aa....Qb>*@.....Ba....Qb.....Ea....Qb..N.....Ia....Qb~.....Ja....Qb.....Ka....Qb.ZAT....La....Qb...h....Ma....Qb...e....Na....Qb.z.a....Oa....Qb..e....Pa.....Qb.....Ha....Qb.T.B....Ra....Qb.....Ta....Qbj.<.....Ua....Qb.4.....Va....Qb .....Wa....QbZ.....Xa....Qb. .....Za....QbbQ6$....$a....Qb.z.....ab....Qb>.....bb....Qb.....eb....Qb..]....cb....Qb..(.....fb....Qb..d.....gb....Qb*..e....kb....Qbv.....mb....Qb..U.....n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2702a4b400b22c7e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.592124648686421
Encrypted:	false
SSDEEP:	6:meitVYGLfjsVgWPWlvnRHqhA14N93PAT9bANbK6t:bwD1nRHuAeNdI5I
MD5:	22DA094055D21133A8BE12E135384B38
SHA1:	F1F5D13D4C9AB8E346037430AD34A409F5050A46
SHA-256:	5B46A5B8DC054CE5B48EC255F5E04C7CAE0AB4F1F825FE0B47C3907461C1F2CF
SHA-512:	AC2AD67413F6C5EE7D94E9137067930B3B489A1AB0E0E56C4664B4F70AF4331DF0509910E497429D4A7A341CAA7B20A46BB742BFB6048A6FDC0DD62FEADA589A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...4Z....._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-M3NKS7J .https://sten.to/]....%/.....+.....g>2.D.@.B),?3.X.7...+u..A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a396d8271332b0d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	62435
Entropy (8bit):	5.8582651625570925
Encrypted:	false
SSDEEP:	768:fgIeIjbIlUgSwzLCMOPCgoeTg+D1pzfoVfvA1Q9b7ApAtR6eE:fg7FbIlUmvCp2eU2py3A147Dc
MD5:	6EB3559755F3468B16EC103C39F62739
SHA1:	BF60154D4624C6D9F9C54E07B0F914DB00D1D7A9
SHA-256:	19223C12AE5AF0B549FF736CEC470487CF2DEF4BCCD3F3767C2C745F8417456E
SHA-512:	5391E60605FCD88ED219ECFFD891342BE9888725FFBE4AE3420DE16C42ABDD09E355E77E211E4B26964574680A13E74B79C1C26DBC3AEB8D1382F2D3E78801FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....5.A...._keyhttps://static.hsappstatic.net/head-dlb/static-1.149/bundle.production.js .https://hubspot.com/e2...%/.....I.....J.K..a.;.R...+$.....<L..O...A..Eo.....A..Eo.....'.....O.....$r.....(S....`.....LL`"....(S..`H....dL`.....PRc$.....Qb.I.....e.....Qbv.,C....t.....Qb&O."....r.....Qb..j.....n.....Qb..c.....o...d$.....I`....Da.....(S...`.....L`.....Qc.-.....exports..$..a.....S.C..Qb.|a.....I...H.....a.....Qb.. .....call..q...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....DaH...@.....e..... P.....@....@.-....XP.Q.....I...https://static.hsappstatic.net/head-dlb/static-1.149/bundle.production.js...a.....D`....D`....D`.....`>...&...&...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c14c7421096824d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	91064
Entropy (8bit):	5.8590535945016775
Encrypted:	false
SSDEEP:	1536:XIHDYG9lLq8A0J3boba3NUQJn+ITGlUTfJ:4L3Lq8DAa3NbB
MD5:	1B02E4C81C9016907A29750457DE9A33
SHA1:	9E44390BDD7ED5289EF480C71D69242A65C917A1
SHA-256:	36ECB2F397C6D1EA233EF22202E8F76448DF29C20E57F66E9B5DDFE57C18F3C7
SHA-512:	CCD5BD0E7A1EFE7D47690AEA18699107FABB4288AC9FF638630F82901389B82914F9E52CD8602BBDE265D8FA5D8C58396FB7E2FBD4A3452BCF73DF5FE70D076
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....[(....DE912632EBA008F7F9EE5F5C321606967B87C560ECD0F34650B745A628C7918A.....'.HC....O ...hb....@m.....D.....(.....(S.....`.....L`.....(S...`&....XL`(....HRc .....Qb.....e.....Qb.~.....t....Qbn{.....n.....S.c$.....I`....Da.....(S..`.....L`.....Q.@.....exports..$..a.....C..Qb.Pe....I...H..A(...a.....Qb.[).....call..!)..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....$`....Da@...8....!#....e..... P.....@....@.-....@P.....1...https://js.usemessages.com/conversations-embed.js...a.....D`....D`H...D`.....y....`....&...&..A.&...%&.(S.....Pc.....n.dlbpr.a.....I....+d.....&.(S.....Pb.....n.d.a.....I..!#.d.....&.(S.....Pb.....n.r.a.....I..d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d8ad63145050845_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	610
Entropy (8bit):	5.708124394511786
Encrypted:	false
SSDEEP:	12:GolHAg5BUoN7UHKMVWWPifnnIzeKqUHK9BlTWhpXuPy/h:G+Ag5BU2EBVWWPmY2EilTWhp/p
MD5:	DAEC90A69C0EC05765642B25B9136557
SHA1:	10723B82F7CC6429AFC44B5EC5E0D07F0A971022
SHA-256:	7A9BE3FF9271732C1AD8162648A5599B640D9E5B08D6D3A9C5834615C7C9124E
SHA-512:	91F82E9593096B65B512945AA0BBD8C52E12788FEE3B6733C577DE41C498E7D1F7ECEE829D1431DD070A808E5D48C975EBA0FCE292F5179D742D1C0FA9C3CB0
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.osano.com/hs/cta/ctas/v2/public/cs/loader-v2.js?cos=1&__hsfp=2200529148&__hssc=106899676.1.1626202312269&__hstc=106899676.fb78b4cfb86ad3bcbc24353d8af15f34.1626202312268.1626202312268.1626202312268.1&canon=https%3A%2F%2Fwww.osano.com%2Farticles%2Fccpa-guide&hsutk=fb78b4cfb86ad3bcbc24353d8af15f34&pageId=27824911813&contentType=blog-post&pg=bad56632-e79c-4b99-b5ce-24fce148c450&pid=4785246&sv=cta-embed-js-static-1.43&lag=1877&rdy=1&cos=1&df=a .https://osano.com/E'...%/.....H%....).....[.....H?...1.<N|..u.A..Eo....."9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e312ec1caeaaeb8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4086

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e312ec1caeaaeb8_0	
Entropy (8bit):	5.714537252930491
Encrypted:	false
SSDEEP:	48:OEiiF+YI7TEipjcwFlFVvfNOKlYzMjv6/wtsf6ZLJLzkdenfsVT5nJsn0TC2:Hy7IGzHNOKC66IWCZL5kdenfIAt2
MD5:	A215ABD68C67C9C257EEE7A854FA2BF8
SHA1:	A78FF6CBFD24940AFAB08A88F132A0242FE20F01
SHA-256:	D9F5CF2C0E05560421D6B7F9BEC4233028C023E01B2E15152A3F16B2947DA324
SHA-512:	232866FAFF42BD038979324F2B396649C6ABB36ADE717B9DF4F916C69362D2522B4C69B2086A69BAE3776148728E583BF45C65F7B119B1ECE79E8F4EF72A69A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....'...._keyhttps://linksplit.io/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js .https://linksplit.io/..7..%/.....N!4..>mJDh.t...~.5.[...(.-lWM.A..Eo.....n.B.....A..Eo.....7..%/.....'.....O....x.....G.....h.....(S.0..`.....L`.....(S...`.....HL` .....Rc@.....Qb.....e.....Qb.8.....t.....Qbz\.8....r.....Qb^.N.....n.....Qb.....c.....Qb6D.....o.....M....S...Qb...U....l....R....Qb.A.....f.....QbFea=....d...k.....I`....Da.....(S.....Ia#.....@.-....`P.q.....S...https://linksplit.io/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js.a.....D`....D`....D`....4...`....&...&....&....&.(S.t..`.....0L`.....Qd6..e........Qd.Yj.....innerHTML.....Qdz.....childNodes....Qd.-.....getAttribute..rT.I..K`....Dw0.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2f2fe2aaead4ce0d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.351772008411576
Encrypted:	false
SSDEEP:	6:mP8PYGL+MIwJJ6qwD6AgXOEy2Wo0+Y7RK6t:M8LIwv6vDRglW5r
MD5:	C7CEC3C6D0E8BF610DA2A411A5CE0963
SHA1:	4D3228AC58BEB063573AF9F3330E8F4D8190D5F8
SHA-256:	E3EE11055EA9074933AC390F982293711319BD4EAC033C6FB23018425035CA32
SHA-512:	8993EB78A26FC64E65137C61985783168E73372D7CA19D4F6407DFBAB175087E8ED6191FCEA67F6490267CE8D7F76F0E61B16CC1C2E25E68755FE589C2A3111D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....B'...._keyhttps://www.google-analytics.com/analytics.js .https://sten.to/..H..%/.....-.....d...."N...j}T.B..}.....S..A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3121e888bcde1488_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8054
Entropy (8bit):	6.053375932169858
Encrypted:	false
SSDEEP:	192:RNbDRITIJXjHW8OLMk47sa3cqxtorIM0Gh0fyXHg3Z:RB9B1FOLO7QUorIiheyXgJ
MD5:	2F6731A4B7F5CEF2A371AF07CD0A18E0
SHA1:	4315FF8FCAA4658A223B91463F2DF1241B842022
SHA-256:	772DEE0DD0F71483BCF7E10F97BCAE02F19F4BC4D82BB1A54FE657A267C65E2E
SHA-512:	5097659CFD233BF31F04569D1BD8D4D5A3BA104196BCD2CED53BF4AF9B4A630C98ACFEAA70E52B8069F037657A4F253C3BC29850262DC304F912F54CE359AEI 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...p....._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://osano.com/^.M..%/.....c.....8..-..C-0.C.q.Q...J...A..Eo.....K.....A..Eo.....'.....O.....Rw.S.....(S.0..`.....L`.....(S....`.....L`J.....Rc`.....(.....Qb.....c.....Qb.Pe.....l.....Qb".....r.....Qb..P....s.....Qb.....o.....Qb R..0...._.....Qb.[.....v.....Qb...-....p.....Qb..q.....f.....Qb.....l.....Qb.....w.....Qb..q.....k.....Qb^.....A.....QbN..J....R.....Qb.:mw....U.....Qb..<!....L.....Qb.H.....O.....Qb.....N.....Qb.....y...s.....I`....Da....D%...(S.<.`.....L`.....Y...Qc.....getTime...K`....Di.....&.e....&.(...&.X.....,Rc.....Qbn{.....n...`....DaF.....a.....c.....P.....@.-....DQ....PTU6...https://snap.licdn.com/li.lms-analytics/insight.min.js..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\34f494fab9275322_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.695999454862974
Encrypted:	false
SSDEEP:	12:8ok5BUoN7UHKMVWWPifnnIzhQJaWzqUHKDn8V8TWkt/3Q1+t:8V5BU2EBVWWPmYhQzuEN8TWiI1G
MD5:	1BA9BF346F1CC850508162375766E3BF
SHA1:	3827D9B009B4C6DAFBC5EEC4AF02FE279D035C6E
SHA-256:	66E3E9C0E03F2DC1CB236FE04AF663874FA378B3377FF3D7E6124CA66FBEDDF8
SHA-512:	EB612B4E9EF9C7D672D4B660BBD67C7E0A970ADD52A2941B644D42504EB53232EAAD3D5292BE60F80BF065725FAD6373D3BB83EBE626AAEA9431DBDCE2A93 B1D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\34f494fab9275322_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....ic....._keyhttps://www.osano.com/hs/cta/ctas/v2/public/cs/loader-v2.js?cos=1&__hssc=106899676.1.1626202312269&__hstc=106899676.fb78b4cfb86ad3bcbc24353d8af15f34.1626202312268.1626202312268.1626202312268.1&canon=https%3A%2F%2Fwww.osano.com%2Farticles%2Fgdpr-compliance-regulations&hsutk=fb78b4cfb86ad3bcbc24353d8af15f34&pageId=13134249950&pg=d59a2ac5-70b9-46eb-a4f4-73fd4e790db2&pid=4785246&sv=cta-embed-js-static-1.43&lag=319&rdy=1&cos=1&df=d .https://osano.com/.V...%/.....t.(T...'v.c....._.!....$.xl...A..Eo.....34.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\351791750d52ea5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38378
Entropy (8bit):	5.7139099598466165
Encrypted:	false
SSDEEP:	768:fLZobdxVM/4yEGlb991Avlw4VKFXmBXVPpz:fLZonO/4yEGlNU64VKFWJVPpz
MD5:	3C7BB93C6B1669922F51DDB06677706D
SHA1:	64F55E8BDB239B053FC8C5C6B5C9BBFFC8841002
SHA-256:	E9759C7A65A595D3CC95586D23FA0EEAFCA188ABD9B11B7DDE0B0283FD53CB8E
SHA-512:	540B2076570A0FF99492E77952D7C54801A315D5D8F7A27BADA1CF1AA84CF24F78D755196DD13CF18004C109D8DD4C2ABC0D637A53ED535084E6832BAFBE818
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r....._keyhttps://static.hsappstatic.net/feedback-web-renderer-ui/static-1.6417/bundles/fetcher.js .https://hubspot.com/*1...%/.....W.4.|..yK..21.b.. ...ZS.A..Eo.....i.....A..Eo.....'.\E....O....0....lz.....<.....(S.Y...`h....\L`*....(S....`.....L`.....Rc<.....Qb&O."... .r.....Qb..c.....o.....R....Qb.K. ....c.....M...Qb.7.....f.....Qb..A.....s.....Qb.|a.....l.....Qb~=.....d.....Qb..@O....p.....O...Qb.e.....v.....Qbfl$1....y.....Qb>P-.....h.....Qb.....j.... .Qb.h.....O.....QbN..S....m.....Qb.K.....w.....Qb...B....S.....QbV..;....E.....Qb...f....I.....Qb.....T.....QbR.*e....P.....Qb.....k.....Qb..:f....x.....Qb..`.....`.....Qb.....C.....Qb..Y.. ...N.....Qb.....R.....Qb..\i....M.....Qb.27.....F.....Qb.....D.....Qb2.....U.....Qb...f....W.....Qbj$.....G.....Qb.....B.....Qb: .....K.....Qb.K.....X.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\37947cc29278bdb5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93760
Entropy (8bit):	5.773031047279213
Encrypted:	false
SSDEEP:	1536:MsAdiq1v488p180tlm7li0TD+1BoJWF4jt8JAMZPnZoGeOil:JA038882T7hTD+1BoivnP/2
MD5:	BC7CE548A6167C0BE6AC91A8B4546438
SHA1:	04FF740FD550ADFDEA7DF0E74B1927EC612A7739
SHA-256:	144F2A2FE1965B37254EB54549F97CD939F0D91A9B37C645658E3043A526F308
SHA-512:	7CA4636B9A17F6F3BACEC537810853E46149BFEA3F9198A82CB19D460EC2AECD04F55BA1E8459E6238C73E8968C52D39C12B98C8272204B546E1DB5120DB782
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....."....C746762D9A282B5C6A0CCB3CB815CCF52E354BD1A801AD023D8AF26445FF9466.....'..I....O ....I....'....."..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....L.....Q.@.....module....Qc..#....exports...QcR..M....document. (S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.... ...I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.jsa..... .D`....D`....D`.....`d...&...&..!.&....&.(S...."..`.C.....Q.L`.....q.Rc4.....M...Qbv.dg....d.....Qb.....e.....Qb>up.....f.....Qb.P3.....h.....S.....Qbv.....j.....Qb.b.....k.....Qb.. !_....l.....Qb.ph.....n.....Qb..(....o.....Qb.TK.....p.....Qbz.....q.....Qb.....r.....Qb.=.....s.....R....Qb..}#....v.....Qb.....w.....Qb6.....x.....Qb.|.....y.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3903e821dc37d9e2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.39453381940583
Encrypted:	false
SSDEEP:	6:m9CogEYk+6KHHcqjF/X6m1a8bkI4s2k4jlhK6t:KCoN+hnc45b4kGl7
MD5:	4201304041AC4F25970CAEAE799AEF66
SHA1:	AD2DC71D24F637EDC6DEF6F07DD99FE04779D674
SHA-256:	CACA34CCEE37752C93FA584E72D50E7D521B9D239170FB404682F3A48F8B97D1
SHA-512:	D78457E13A6581593DCD2A10C7D22F33D3C0745A01326125080F54B0F4FC5B068F0E2A10A1914AFE6750C378C6B315C7D986FD69C69AFD662A9F4800A024FD9D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....-`...._keyhttps://static.cloudflareinsights.com/beacon.min.js .https://sten.to/.....%/.....-.....?@&..l}..."..g.....X.b...k.El..A..Eo.....Jl.K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a59899a21d99bb0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a59899a21d99bb0_0	
File Type:	data
Category:	dropped
Size (bytes):	50019
Entropy (8bit):	6.164569846521312
Encrypted:	false
SSDEEP:	384:zzgKsO1l1nO4stcG5BrMdt3iAL56sPjpqeZ+saiE5dreaFPz1hb6DXTVL/QaAVsk:z8AHKclTUgfOvH0cnyYSjg9zFrl88LGq
MD5:	6D61F80FAD8BF9B8BF4810EDB22AEF49
SHA1:	FE078BFAEA206374DE1C1884E88C6773FA64F267
SHA-256:	592F4F96B4EAB1EAE2AC05B079ACE669013D30F5D6A33F3DB4592FC78C91C583
SHA-512:	D58BEDF0036B91ED5CEDA3E32E39A0DFFDCB310E7B2B2FBB0644C8DF3F18A3B2DC651E608EA2B6E35C4C1C2B3B488149A2C79FB6860EBEFA1B67F6EEF4FEFA42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;.....@...._keyhttps://js.hs-banner.com/4785246.js .https://osano.com/./k..%/.....O<m...+.g.pD...sQ...o;.....E....A..Eo.....e4.....A..Eo.....'.....O.....l<f.....d.....0.....\.....(S.A...`8....PL`$.....L`.....Qb...n...._hsp..Q.@.%CK....window.....Qb~,.....push....`.....L`.....Qe .!8w....setCookiePolicy....`.....L`.....aF.....Qc.l{.....portalId`.....Qb.3f.....id..`.!....Qc.....domain....Qe..D....docs.osano.com....Qb"A{.....pathF..Qc:.....label....$Qg...9 ....Documentation & Helpdesk..QcR.>:....enabled.G..Qe..."....privacyPolicy...`..... Qf.S.....privacyHideDecline..H..Qe.}.C....privacyDefault..H. Qf...[....privacyPolicyWordingF. Qf.....privacyAcceptWordingF.$Qgb.i.....privacyDismissWording...F.$Qg.1.....privacyDisclaimerWordingF.$Qg.d.....privacyBannerAccentColor..Qcf..N....#00bda5.. Qf.I.K....privacyBannerType.....Qbj.....TOP.. Qf:~.t.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3badedbad50d82cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	184
Entropy (8bit):	5.278378464349013
Encrypted:	false
SSDEEP:	3:m+l487la8RzYM4hGWWoH4RTX1lHCUt2o8Go4rOKbn9Ndg1mNe/pK5kt:m07VYM4rqTX6c2bw6KbSsNehK6t
MD5:	E5FE3D1239B7324CB30FAF5DDD651CF3
SHA1:	61190B7B742BA6048A43D4EC667D6F785C3BCE9E
SHA-256:	81D288732C396A6D84A0095C5D8E3CA86D09EEBA8D3FED3C7A6438FB6BDA9F09
SHA-512:	49E1587A770FE2D2BE26706CE33FE6D67C931980AD98962090016DDB80A65D6AC059596B34737C951B242F1033232D8B301CE8E12F1F1235DD710C2BC200C580
Malicious:	false
Reputation:	low
Preview:	0\r..m.....4...,....._keyhttps://client.crisp.chat/l.js .https://sten.to/.....%/.....G-.....N.[..M.NC[CrpoTx..N.76K....?\.A..Eo.....!..e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4250e464f91d41f0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.590011419041093
Encrypted:	false
SSDEEP:	6:mhdVYGLSmXZCrTSRRNq2Vyg1JXWKoH7raK6t:qDRNH7HX8I
MD5:	A036BE9B0916B15D57D0344492E6858E
SHA1:	98BBDC02F30E8388BD42259842DF7853C248BCF6
SHA-256:	64B3FE6E5AEBC40240D7DA5342693BBCE6C3B971CE1B876133740B80693A4824
SHA-512:	0243FA6109AC701E9B002BA454C5F961BF0601B0B6DA3DE149553D8D0BCC5FE9D3148CFD0BE10CF6C6E2684DDBF1037FF73362E58CA1616CB37D3A1431C3F0F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P.....J....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-157457758-1 .https://sten.to/.....%/.....k-.....7..]l...N..V]S..aF..u..q5..L..A..Eo.....9.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\425b48b83c530999_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20615
Entropy (8bit):	5.71176928011959
Encrypted:	false
SSDEEP:	384:2h7IJHBQwIs5kTKpzL8o2wTTCQ6IcRKOi71FZkDFI2mJiJoRfjW2v:2YBt5kTKpzLWw/uRKF+y2haXv
MD5:	0DB43D3DF78F0A70F6E538C9F681ABD5
SHA1:	32D7210083F652475B09EE66CBC446C3535935DA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\425b48b83c530999_0	
SHA-256:	50C0829255E32DC9AA0485DA81DCC0EA0117753AB37DCA3207B4918A7C5B5011
SHA-512:	C1A4E838929CE543835A0E3747B2084CAB296FC3180CE016C4854C210075E4E49B475BDBEBD5134C21528E763D3316DC4F38241920D84E4327967E944A8EFEC5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|.;...._keyhttps://static.hsappstatic.net/conversations-visitor-ui/static-1.11456/conversations-visitor-ui-lang-en-gb.js .https://hubspot.com/N....%/.....S.....r.. ....NH`.:..-.C.....B..A..Eo.....|/.....A..Eo.....'..3....O.....N...,e.....(S.l..`.....$L`.....Qc...%....window....Q.P..J.....webpa ckJsonp..Qb>..[....push.....`.....L`.....`.....M`.....0Qj...'#...conversations-visitor-ui-lang-en-gb.`.....a.....Qb.;....tSS8C.(S..`l....XL`(....(S.H.`L.....L`.....a.....Q.@..3.... .en-gb.....a.....Qe..^.....sanitizedEmail...4.a.....QdJ.....imageError...0Qj../.#...This image is too large to display...$Qgv.....expandEmailButtonText.....Qc..g.... .Expand...$Qg.....collapseEmailButtonText...QcJ?g'....Collapse.(Qh...I....hideEmailRepliesButtonText... Qf.!.m....Hide trimmed content.(QhnK.D....showEmailRepliesButto nText... QfjUN.....View trimmed con

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c3bb1d769cb3b44_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.8503341810352385
Encrypted:	false
SSDEEP:	6:mq3NnYeWE0ZT6T5DFV/l/wct0aGYBnK6tZmvfw4PtSyeoyNVUt0aGY5:PNKEqkVlomVWw4Ptlye
MD5:	8AFAAB55EFD5ABAC354EF300E072BF52
SHA1:	64E2D93C1681846F3024A05800CB6E56C24041C7
SHA-256:	8848F21CAB4A33DE61F6437874F56E7AA9EC690A4D9B94B2A54BADA06AF5FC16
SHA-512:	5CC88A45FBA2AD6445FF24B313938FC6F76107500B9C6839967A31C6B64F4686F2C5062932F0210C81D6407055B4E2730684036CCE5C2D899F7750D4CB21D28C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...3....._keyhttps://cmp.osano.com/2sUBzx7wRdAfu6J2kkS/8e547744-886f-4a9b-a90f-7e96a47aa604/osano.js .https://osano.com/6.U..%/.....X.....Bu!..4.3 Q...?h....i{.L.....f.A..Eo.....A..Eo.....6.U..%/..A..0F2058A2C309897BEA5F29FDAC11CF1825C9DC08D7D755BE7ABADC46241425D0Bu!..4.3Q...? h....i{.L.....f.A..Eo.....:..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d4a1d895d05a729_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	610
Entropy (8bit):	5.720372281511365
Encrypted:	false
SSDEEP:	12:eolHAg5BUoN7UHKMVWWPifnnIzeKqUHK9Bln8V8TWYpYG:e+Ag5BU2EBVWWPmY2EiG8TWYpYG
MD5:	27263391994558C2A8A740DF9095245B
SHA1:	E55EC30A0A8334DE41472D3AB20D3254A24A4426
SHA-256:	C861A62C05BD1F7FDB21D383AB6DED30412B7ACAF00EC05A74DC5C9BD171D21E
SHA-512:	EE8F2D4071D28CB81F49B13CE187121186C4E84CD4E9769967FD2C01EFA848BE2C692DAFC0ABEE6BD80466647CF5BAD0ACA71B4766ED359A5C588B5B20430D 65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....)9....._keyhttps://www.osano.com/hs/cta/ctas/v2/public/cs/loader-v2.js?cos=1&__hsfp=2200529148&__hssc=106899676.1.16262023122269&__hst c=106899676.fb78b4cfb86ad3bcbc24353d8af15f34.1626202312268.1626202312268.1626202312268.1&canon=https%3A%2F%2Fwww.osano.com%2Farticles%2Fccpa -guide&hsutk=fb78b4cfb86ad3bcbc24353d8af15f34&pageId=27824911813&contentType=blog-post&pg=d59a2ac5-70b9-46eb-a4f4-73fd4e790db2&pid=4785246&sv=cta- embed-js-static-1.43&lag=1931&rdy=1&cos=1&df=a .https://osano.com/;.~..%/.....G..D."....E.q.....9.oC..A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4edbab3cf137776a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11708
Entropy (8bit):	5.568374008057817
Encrypted:	false
SSDEEP:	192:KJreai1dmb8xFFDbtglpIIDRUZgiQjrpJ9DgGDla59i3nNg6:KsRmbKaxdUZgVhgQlqSNg6
MD5:	FD68977EF0A022DE1DD64FD783E721E1
SHA1:	B83837E12D7433BFB8D42FEAB1F5DF1548F10CBC
SHA-256:	17BC49159CC35D51ED47CD5E5A0742F441204FF063248A298DDD34CF738DB0E4
SHA-512:	76D1DF1F9C1586BDD2C0BDCD14B9E65093C2B57562159872EEB39DAD95A64674F0D7B90BD097CC4E67D8BAD6E26EB40462844354EE07076411DCDFDF263AFA 0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4edbab3cf137776a_0	
Preview:	0\r..m.....d...O.n\...._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://linksplit.io/.9..%/.....h....b>$..EI[.1...p]g.1.vG..B.9.A..Eo.....C.....A..Eo.....'.J....O....(,..U.Z.....(S.<..`2....L`.....(S.I.`.....L`.....Q.@.Z.!....exports...Q.@..r.....module....Q.@..C.....define....Qb:V.a....amd...Q.@nQ.....Popper....K`....Du.....s.....s.....&.\..&.-...%..*...s.....&.(.....&.]....\..&.-...%....(Rc.....l`....Da"...8.....e.....`...p...@.....@.-....XP.Q.....I...https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js...a.....D`....D` ...D`.....`....&...&....&.(S.U..`b.....L`.....Rc.....v.....Qb.]+....e.. ...Qb...g....t.....QbJ..o....o.....QbB..<....n.....Qb./.....r.....Qb>.....p.....Qb..{.....s.....Qb."{.....d.....M...Qb.VM.....l.....Qb.?.....f.....Qb.?.....m.....Qb.....h.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58fc5f4da155621d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	390
Entropy (8bit):	5.446689520580092
Encrypted:	false
SSDEEP:	6:mpaEYLXrdWb/j/UYfExQE/bUEVbK6tWpaEYLXrdWb/j9AbYgXGYfExQE/bUTbK6t:K8bUjcYyQ+7j08bUjdgWYyQ+q
MD5:	5003740B7B8A4135CC317260F1106F03
SHA1:	358E61A4B78DCF43A3896281F21B13556395B65D
SHA-256:	489115890E56C573F774449B286361B6AC3A98ED440FD87588872A8B7322F47F
SHA-512:	2149BCB1460A1999516E41AC933352223A42BE9DC63DB8B5C73DB38A4127ABB01E8541DF8032CBA0C9CA50EAF6D07BCB1893E13EA7346E5EFB082203CB303AAB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?..........._keyhttps://js.hsleadflows.net/leadflows.js .https://osano.com/..c..%/....._.....^...=LE...4.....z.\..O.A..Eo.....4.....A..Eo.....0\r..m.. ....?..........._keyhttps://js.hsleadflows.net/leadflows.js .https://osano.com/[*...%/.....^...=LE...4.....z.\..O.A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5af0b50463c83ef2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	586
Entropy (8bit):	5.740144908652123
Encrypted:	false
SSDEEP:	12:Bok5BUoN7UHKMVWWPifnnIzhQJaWzqUHKPTWYtyKqs/mN:BV5BU2EBVWWPmYhQzuEqTW2y5N
MD5:	15425E6BF075A8762E6FDA23D02E99D6
SHA1:	E965D6B839CC29DEC83A941F6169562237C1EBB2
SHA-256:	4E926E2EE73C002AF8385814B8C5B79D3D72D5EE8904B93805615724143E407F
SHA-512:	943FE2045602401E4C10B45355EA189B8A3D4E961BFFE746479F5ACBF1FAA046A68B5BD39C0FAB86E75E1B4E0F594C12D5BBB0DF1A3ED1BBF89618E27CCE9F3F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://www.osano.com/hs/cta/ctas/v2/public/cs/loader-v2.js?cos=1&__hssc=106899676.1.1626202312269&__hstc=106899676.fb78b4cfb86ad3bcbc24353d8af15f34.1626202312268.1626202312268.1626202312268.1&canon=https%3A%2F%2Fwww.osano.com%2Farticles%2Fgdpr-compliance-regulations&hsutk=fb78b4cfb86ad3bcbc24353d8af15f34&pageId=13134249950&pg=bad56632-e79c-4b99-b5ce-24fce148c450&pid=4785246&sv=cta-embed-js-static-1.43&lag=412&rdy=1&cos=1&df=d .https://osano.com/.....%/.....6....T....X....R.@X..Z....c.G..*.A..Eo.....@.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5c1ff057fef9c98d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16883
Entropy (8bit):	5.597692026936458
Encrypted:	false
SSDEEP:	384:5Y1ED1/qOCZSF8vBniLyvhy4ewSNh8YkxYVzzqWN+G996NtCzW7air:5Y1qiOmAykXVz3XmNtCCD
MD5:	BBC8642F9792D6346929AD97666F5A24
SHA1:	AAB9732FBCA969EAF6C2B8E57B4153A3F1F63B13
SHA-256:	87B576F592B9D2C702892636F77FCC89C97612ED7CDAD94DAB6944F7449425D0
SHA-512:	0E05C10BA5E01342B69C5050891DDF83152E7BCDC4C327C6F8D7751361EFB5C259C1600294E3C2A5818E0CB1BF19380174351DCFE3B73E94BA9B55CF0CD4006
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...N./....._keyhttps://www.osano.com/hs/cta/cta/current.js .https://osano.com/3.6..%/.....u...n..^.....Ra....5nY.G.z.A..Eo.....z1.....A..Eo.....'.]:....O.....@.....|.....(S.a...`z.....L`b.....Qc.$.+....window....Qb.[....._hsq..Q.@Z.G.....hbspt.....Qbji~.....cta..%...a.....Qc.,%....__hstc..I..Qc..8...__hssc..I..Qcr(c....__hsfp..I..Qc>..*...__utk...I..Qe:<....__generated_utk.I..Qc~.-M....email...I. Qf.....__analyticsPageId...I..Qc:=,a...__path..I..Qe. .....__referrerPath..I.$QgJ.....TRACKING_CODE_TIMEOUT...`.....Qe.&*.....placementsData.....a..... Qf.....placementsLoadQueue....a.....Qdv.....loadedQueue.H..Qe.....loadQueueSuccessH..Qd.r.....canonicalURLI. Qf.....queryStringToForward.....`.....$M`.....QdF.....tc_country... Qf.ZGw....tc_deviceCategory.....QeF..;....tc_visitSource....Qe.H._....tc_drillDownRule..Qd..E;....tc_language...Qd.[

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\667c08e332de2811_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19678
Entropy (8bit):	5.602812585461819
Encrypted:	false
SSDEEP:	192:uspFtPEhajTJOsyUy2bKy+l9URkKIyhJc2Kg9ejylpO9y6zKr24OkreyBZBawDsX:usNXTILv0RIIIHhuwDsT+lR4A/+h
MD5:	6C68CB6BB90B5EE2338E85686358D43A
SHA1:	B079A67F615F589CBAE2869F0C83A48B12A1E052
SHA-256:	FDC651099D6CD77C74FC6DD2E1A2FF23722D92BE8C206F77B01243C327122033
SHA-512:	6985F062ED57E08807317FA68188E9D5CB2C231E00B8939DFFF5102CFB78CFABCF4AF4724DE397CF7960738F078EB3F782D8784E203C65DE0F81EF20AB376B24
Malicious:	false
Reputation:	low
Preview:	0\r..m.....v...\..L...._keyhttps://ajax.cloudflare.com/cdn-cgi/scripts/7d0fa10a/cloudflare-static/rocket-loader.min.js .https://linksplit.io/..8..%/.....8.O..v...;..... ...do..8...?.A..Eo.....U.....A..Eo.....'.,0....O....0K...w.....t.....(S.0..`.....L`.....(S...`.....L`f....q.Rc.....R.....Qb.8.....t.....Qb.. .....e.....Qb^.N.....n.....Qbz\.8....r.....Qb6D.....o.....S....M...Qb.....c.....QbJ/F.....s.....R....Qb.qn.....p.....Qb...U....l.....QbFea=....d.....Qb.A.....f.....Qb..k....h.....QbNd.<....v... ..QbZwT.....y.....Qb.....m.....O.....Qb.ip.....S.....Qb.....w.....Qbf.Z.....x.....Qb.'N....P.....Qb^qv.....A.....Qb.5.....E.....QbZ.kj....k.....Qb.....I.....Qb2.Ix....L.....Qb..... ..QbZ.....H.....Qb.0.....N.....QbN.uQ....O.....Qb.X;7....C.....Qb6*....j.....Qb2.....M.....QbZ1^.....W.....QbB.P.....R.....Qb.N$.....T.....QbN.ol....B.....Qb..3y....U...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68c4a69f1a2a6b8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.426931545407397
Encrypted:	false
SSDEEP:	6:m8VY0OCZlXZ5yaXGbuygqcqLvEDinm1rqAJbK6t:/nIXZ5/GCfyUASqgN
MD5:	10D24DB8A323E0AFA5360DDBE915194B
SHA1:	C1E5D70449710ED8EB436747D350B9778EE4E0C9
SHA-256:	ED3D6ED1D1443CE91C2CD8C4464075383B7239A99D52EE25628F99FC49168425
SHA-512:	AFF1B25203843F71732EF571885D22B7F61FF1E827BAEC9E1F396160C2C5F94006AA3002083C2D3EF3DB796D13D4737968BE828881C5EAEF79837F7A66552086
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://unpkg.com/ionicons@5.2.3/dist/ionicons/p-6f4eae92.js .https://sten.to/u....%/.....r.O..i`.....7...c.....y..o.A..Eo.....97.5..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c3607d5a4c1b394_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	344
Entropy (8bit):	5.7604225885607505
Encrypted:	false
SSDEEP:	6:mgLnYGLSmXZC23gSS//AoCpvP7m45JhK6tODkT5p0TeKS+f6pvP7m4c/:jXzwSm/+vD7Qg8EXv
MD5:	50189D105079870F8D986E78F7E86021
SHA1:	8C7787A7F0EFD6A86E4A11A393849F6069E6F4DC
SHA-256:	89F4BDC6A1D0FDDC71B922245DD87B43B0C92789228744C85B87980A03412605
SHA-512:	9D630E91CFC9658F92798480A22B5C2AAC9EFBDE3D59339F2974A091D97D4958F057CEA2E2125E1B3A391EE07C9C20CA48EDEA90913DA49BCD6DB6EBFA2B3 BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...:....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-739694307 .https://osano.com/.bL..%/.....G.....n3@8...._g .+.L.YL.p.3J..(.a...A..Eo. .....r..A.....A..Eo.....bL..%/..1..F26F57D4203B361967CAC9C23A940E7E9271A6247698D635EB7561319367F4A9.n3@8...._g .+.L.YL.p.3J..(.a...A..Eo..... ...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\734100cf3f350dd0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	309
Entropy (8bit):	5.70252680004367
Encrypted:	false
SSDEEP:	6:m3eYGLMQXrXrABrYGTXW+3QI1Kl/Q9+D9uMn7AHKnpiFAK6FM4+wS7MrGl3K6t:TrXYrfTKlY4pumUHKpiFAKuM4+wlq6
MD5:	351C7F3C8C352EF5EBFDB7A5D21CAC1F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\734100cf3f350dd0_0	
SHA1:	3F48F3EC6E406BD5D4ED7D07EC0059683F3A6D03
SHA-256:	4FA6DBB6CFB3D1F86843CFFF56BC64B52C7B31B63376FB876256A3E674EA1E26
SHA-512:	16658C23EC957A961977BD793B680545007D5C207CA9E232B1C448FE232D174BF2778B6FF04D63C1A3FCF6DCF7B61E7A38E0BF8550EFFE82AFEA85C7F0979B0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7.W...._keyhttps://www.osano.com/_hcms/forms//embed/v3/form/4785246/162149ed-dd87-457a-9bc7-d18001586306?callback=hs_reqwest_0&hutk=fb78b4cfb86ad3bcbc24353d8af15f34 .https://osano.com/....%/.....]..]...4....7*...5.....2]N...:Z.A..Eo.....yr.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\75f1fcd730ba1190_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6944
Entropy (8bit):	5.300399987189359
Encrypted:	false
SSDEEP:	192:yWTtahFqrcO6zfgUGlEP4wV6X/GnY5lmFwFJN:yoa+fefgUKEP4wV6vGnY5lcqj
MD5:	2326E329695C484D41CCA6E815CEC29D
SHA1:	23EEBAAC2DB3D03ED89588E2182C89DE6D2CF7FC
SHA-256:	0A36BC9B542853CE0B9F1E7000747B64B7B9A8D6C5DCBD4697A717DC1F5128E7
SHA-512:	78B0ED10D17CF70FAF66DC1752EE1776EB13CB3B2A16C4E9AA1088898B329608D7E91177A5DE3B4DA97ACBF967571439D6581882EA80E5F471829C9003A386D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....o=...._keyhttps://www.osano.com/hubfs/v2/js/blog_single.js .https://osano.com/..7..%/.....Rku^._.h....!.....X..F..U.A..Eo.....A..Eo.....'.....O.....J.....(S.=...`.....PL`$....(S.)..`.....pL`4....`Rc,.....Qb.....e.....Qbn{.....n.....Qb.~.....t.....S...Qb.....o.....Qb..P....s.....M.f$.....I`....Da.....(S.M..`P....(L`.....M.....Qe.,[W....hasOwnProperty....Qb.[).....call..Qb~,.....push..Qc.A.....shift.....K`....D...x.....*..&...*..&...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&...&.Z.....)..&.%.*....(...&...&.%.*..&..*..&.Y.....&..0.. %.L"&..i.%..Qw.....#.&...B....#.4&....&.(...&.(..$&.(..&&.Z....(....&.%.*.*&.0..,%..&..B.....&.]...(..0..(..2&.X..4&.\.6.....&.(...&.(..8&...&.%...|:&.Z....;..&.\.=....,Rc.....Qb".....r...`....Da....P.....8..I?..... .....P..... .....(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c0277fc49638798_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8888
Entropy (8bit):	5.660156392656196
Encrypted:	false
SSDEEP:	192:xbb+H/IMurUaZGxM+OECCbF8a/m7zrUai1OM+ODPqr:h6H/IOUA6a/mYb1qr
MD5:	B1EA792DEDB9ACD978521DE38D4BF6BB
SHA1:	14A184C23AAAACCE55C4BDB16C73C65D671747EE
SHA-256:	B24E7AEFDED86611264D81C18BDB4A0B3537156386DC1FC26E9FBCF37CC29E12
SHA-512:	CE426CE55A6524C2C51A11ED7AC0EF4FBD826EC16BB88AF75169F6E10474D4D496CB58DDF20C148014E686B22C700E5B521ED300B4BCFD083A02A6CCD3682F7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.....x...._keyhttps://unpkg.com/ionicons@4.1.2/dist/ionicons.js .https://linksplit.io/m.E..%/.....(.....z.I..hKy>.-...L.2....s.O6...]...A..Eo.....4!:.....A..Eo.....'.e.....O....P.....c.....(S.`..`x.... L`.....(S.E..`B.....L`N.....Q.@&vKm....ionicons..Qd.....components....Qc.$K.....filter...(S.(.`....]..K`....Dd.....*....(Rc.....I`....Da"...B.....b.....@.-....@P.....1...https://unpkg.com/ionicons@4.1.2/dist/ionicons.js...a.....D`....D`(...D`.....,...`....&...&....&....&.(S.(.`...]..K`....Dd.....*.....(Rc.....I`....Da^...~.....b.....!.d.....&.(S.L.`T.....L`.....@Rc.....Qbvl.+....n.....Qb.....e.....Qb.$z.....r...b$...$.....I`....Da.....Qb.+.....$r....Qe.....componentOnReady.(S.....5.a.....Qb...x....t.....a.....A.a....Q.....d.....I..A..d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c07533499897e7c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	65414
Entropy (8bit):	5.7274850761014395
Encrypted:	false
SSDEEP:	768:a8uxAONpdYxap/Pt7Mr/uTjFoi4dufyylvzMoSCRFImu8ZcKFj05:52ex2Pt8Ai5ufy2zMDCRzuscb
MD5:	3A29BF1FD44419E200213A7360F64D69
SHA1:	3C2D99D6A69661FA20FADF097B51979B8188731A
SHA-256:	0DCCCF509C6D0B0B2512F52049B381338B67D5082C8DDC8924A26C890D6732EF
SHA-512:	8BEEDEBBA6930D50723C1E23CA8BD0E94C5812A29E96663E2707353D30D0EC6D200FC1C2C3E8A0AF9BD70E48D0001EF9C38717B297607FF842A457CFF070EA9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c07533499897e7c_0	
Preview:	0\r..m.....V....._keyhttps://js.hs-analytics.net/analytics/1626202200000/4785246.js .https://osano.com/..k..%/..... .....)..E.....a(....3.c....a.3P.A..Eo.....9..... ...A..Eo.....'.....O.....H.....(S.5...` ....tL`6.....L`.....Qbvv.0...._hsq..Qb>>."...._paq.. .....Qb~,.....push....`.....M`.....Qd...F....setPortalId.`.....`.....M`.....Qe.`.....trackPageView.....`.....L`.....Qd.E.....trackClick.....Q....J.....div#annually.tab-pane.show.activ e > div.row > div.col-lg-4 > div.js-aos-fade-in > section.pricing-plan.rounded.c-mt-6 > div.pricing-plan__content-wrapper.rounded.c-pt-5.c-px-5.c-pb-6 > a.js-annually-single- pricing-plan-trigger.js-pricing-plan-button.pricing-plan__button.crunch-button.crunch-button__full-background.crunch-button__full-background--secondary-color.crunch-b utton__full-background--large.text-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\812bbda565fa10e6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.7553235753016665
Encrypted:	false
SSDEEP:	6:mTYPXUIYfKPD6ByFQMrOlft716lbK6tkV0NTCI2h/dr8Qkm+nAs5rOlft713:5SfKy3filNRgIE/dgelf
MD5:	24F2A0826752AA45CA693007E4FB0B78
SHA1:	36737C23538DC319312F8808FF7C0DCCF156CE6C
SHA-256:	0D1904640EBB9BB12F4D8DABEFC4A306DE44C3FC9D79E8C0AF90FD9FDA585EF0
SHA-512:	1F7F30EF16ADF7034D2683FFAC6AC83C7E3B55CBCFF309911B9682230F593C976F69C2E782DAF29C58FFD9FA1D5FCA6FA50CA7DB21CAEF9F0D882A7108D610 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...E.m....._keyhttps://f.vimeocdn.com/p/3.36.12/js/player.js .https://vimeo.com/b....%/.....n.....e@..5.A.....n.....Nb....h.\.A..Eo...../1.....A..Eo..... .....b....%/..!..4289B1939DEE4EF087B01552955EADF64B7762D978C90353F70F05F6FFB4CFF6e@..5.A.....n.....Nb....h.\.A..Eo.....~Q..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\869fde940426a7c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.921688327609047
Encrypted:	false
SSDEEP:	6:mWYGLfjsVgWPWZ1Nrxhcx0wzp7Ar5K6t+8dOVuPL+gTrexTZ9wzp7Ar:XDZ1NrnQ0wzp7Ee8za3cp7
MD5:	01B001D78538F386B71A7AEF64478E21
SHA1:	AF2EFD33C82041CD6212408E0F6E0F3603CE100C
SHA-256:	101E3AD7D19E4A417F0DE5EFD30853A1769FFDA057F3933DAB53597A1F4C702B
SHA-512:	E0587136D6FA628A6E6A7E8908223C26DE4880C3D0B631EC281478CCAF50FFD360FCA05D203A280FDD2DC4BFFB449F8A668BE7C9ECFBFA37F0E694FE5A8A37 89
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....bA...._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-PPQPK94 .https://linksplit.io/..F..%/.....-??.+.+...mt_..Y.$..A..Eo.....;2.....A.. Eo.....F..%/..{..B2D10AC120DCC1525D629F631316DE81C5E95207E6B67097101735E197816562.....-??.+.+...mt_..Y.$..A..Eo.....O2..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c453bdbb818e924_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.464226742759177
Encrypted:	false
SSDEEP:	6:mNb/yEYSHT8NWQAlKPUQyTrQjqucTzrK9dK6t:M/yCz8NWQCUUhrM1cTzo
MD5:	3E168E429969E94A2EC2B22C66900B7E
SHA1:	849CFCB1966FCB2A25787B17D81E4D6348103C3F
SHA-256:	2A3289D4CD9B804C73715E842744EEF9A567A2B1BB9DBE82D5A1482D8B3EBA0E
SHA-512:	C251A8EAC8D328FC1EE763E15333F2D0E3D28F165BC1B4EC92B94DB635E09A94CE94501303268D1A81BF300B5186F6BFF9F112A8813D38469020E21BD3600BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[....n.~...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://linksplit.io/fNE..%/.....6.%p.}.v|..k....|Z.]]b...`..f.A..Eo.....g.Q... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cc3917569a6375c_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\8cc3917569a6375c_0	
Size (bytes):	337
Entropy (8bit):	5.835975353001486
Encrypted:	false
SSDEEP:	6:mHYYEQyMF9ypy2lEAaIHx/kK6tjKJ3VNdBKVQenEurlUaIHxfdD:a99yRE/lp2l/KHEelDIv
MD5:	4ED23CA22FACEC1FE1383FB3B1AFCBD0
SHA1:	94F3B337F464EAC2A512F65149160937CBDAE8AD
SHA-256:	0086F2DAE82D296C7CFECB6D9111D17B4EA850B0C3CFAD8B021985EDB9843340
SHA-512:	B0F66D6BB892F485230234BDE2544E14367E1ACFB876AF230B29D3B0FF2B494A7B3CF3D698EC7CDAE64FCF07A67F796E6491835D59CBCF154BB91A918001300
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....o)...._keyhttps://js.usemessages.com/conversations-embed.js .https://osano.com/.Nj..%/.....i...9...7....#p.._.W...=.....A..Eo.....B0.g.....A..Eo.....Nj..%/..c..DE912632EBA008F7F9EE5F5C321606967B87C560ECD0F34650B745A628C7918Ai...9...7....#p.._.W...=.....A..Eo.....+..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91b5e499bdac1afd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78496
Entropy (8bit):	5.774670933832611
Encrypted:	false
SSDEEP:	1536:WvrqbZrNK5Kysv3zfjfesSnDDaUvq2cD+SzvJtUYABGkE2xnOh9INIP:WTqbHK5Kysv3zf9SPNqv9htEGSIP
MD5:	0AD3D6502868428DE419FF01F7080D5C
SHA1:	C6EAD8EFF85C62C4D6E121C3A30502084B96FCD1
SHA-256:	0F3B374F305D75BB37FEFB0CCB73792430F932419A3D9CF4AA9B7C5544DEA3B6
SHA-512:	9D8F1AF78762F59FA4197F422574FF7E7D920B70CAFD5A55462A9CA01A74349CD4F889FDD20FD039F52C2B44462D4DBC3FBB57CEB572FE33F4B36A0EBC52299E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....].....F26F57D4203B361967CAC9C23A940E7E9271A6247698D635EB7561319367F4A9.....'..b....O....`1.....*.....T.....(S.0..`.....L`.....(S....*.`\U.....L`.....Rc.....Qb>".(....data..Qb.y5.....ba....Qb.....ea.....Qb.L.....la....Qb.....pa....Qb".....qa....Qb>?X.....ra....Qb^.....sa....Qb.....ta....Qb.....ua....Qb.....va....Qb.....wa....QbVWE.....xa....Qb.....za....Qb.}S.....Aa....Qb..7,....Ba....Qb..~.....Ea....Qb..c.....Ia....Qbf.;.....Ja....Qb.....Ka....Qb~.....La....Qb./D.....Na....QbV.'.....Oa....Qb.....Pa.....Qb6`./....Ha....Qb.C.....Ra....Qb.....Ta....Qb*.....Ua....Qb^.S.....Va....Qb.$.....Wa....Qb..o....Xa....Qb.....Za....Qb*..\....$a....Qb".....ab....QbV..V....bb....Qb.QdA....eb....Qbb%.....cb....Qb.....fb....Qb~^p.....gb....Qb:.....kb....Qb.|.|....mb....Qb.b.....nb....Qb..-.....I

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9309777715d6e7e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.893890688336983
Encrypted:	false
SSDEEP:	6:muVYk+t/1SvE1RoBKXMQsv2xn/iqgrvcOTrmfK6tD0Kouw+NkTrvcOTm:3+td8EboBKYv2xnaq+3Ih0KoANkB
MD5:	70F661FD72C02D95AFC5065517D84ECD
SHA1:	149E5350530E1A3BAC6254A6A4D79BC5CCAB8148
SHA-256:	E906409BD190F8BCC2DD3FEDF0CB38B47F23F0794CD0A8F9D02C8BAB5C663C6F
SHA-512:	1F71D9C0B4258882E7D5BA9132946FB362019F84CB24A51C877753717CE077AB0F2B2000D5FB774BA6830C42CE6FE990CFC70962A0D31A9834C4AEA9B25C6368
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....]. ...._keyhttps://static.hsappstatic.net/hubspot-dlb/static-1.140/bundle.production.js .https://hubspot.com/.-...%/.....e.....X.:.Z..s.g.kW.].x.J.....$.#kq.A..Eo.....A..Eo.....-...%/.x!..F6E41ED76CF40DCEE5BF9E649BBEC4639D10BA921B0C7AC83FDFD197FEF04EA1X.:.Z..s.g.kW.].x.J.....$.#kq.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\939fa2eb7e32fb7e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.465084802586745
Encrypted:	false
SSDEEP:	6:mwegEY0OCZIXZ5yaXGbXGh+sdqsIL2LXTdGH4jc5RK6t:OnIXZ5/GrQvYgjsylr
MD5:	0249426503782D3D8B37D63AC72632AE
SHA1:	73AE14FAB3DFBEA22E126BB82089C0E1EAF5F258
SHA-256:	5D2108C2C6E2DD728E2A7099B192D90F2A4F7FD045E95339D8779D5836D570B6
SHA-512:	A867F0A949F1BA5F34A175A8BED86EF88587BFFEB30B4BC26D92AFCB7DE0E9954FBE2D2FA614E464831912B68F0AB20D48BB555E33B5ABA057AD9020FD461F93

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\939fa2eb7e32fb7e_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....[B...._keyhttps://unpkg.com/ionicons@5.2.3/dist/ionicons/p-4372c4bc.js .https://sten.to/.....%/.....c..$.2w...|\...b.....x.A..Eo.....4.1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\95e14a1397d711f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	571
Entropy (8bit):	6.011294726646117
Encrypted:	false
SSDEEP:	12:3z8NWQf0rHfD38MdokrAeqWXeRV58MdoQVaD38MdoB/Q/Nv6RsSp8MdoY:D8diHfrpokrAFjpoQ0rpopQx6RsSppoY
MD5:	685DB7EC3CF4BE0EF7AB9794C96A2251
SHA1:	DFB9E1BD6320C2ED9D5EAA36C14E26B6AE23F588
SHA-256:	38C44DBF28BC64A18BDAAEB23383363F0ACBE1678A604DE6E565573D79779D3B
SHA-512:	3209437E50CBEAA828BA669842763925680BDD6185DE34C93E669FBCF2DC8D1787E8E116EDA6045651DD3FEF9307F735101E87BEE7D0966D0FA2C440036DF4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...9..S...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js .https://linksplit.io/W.#..%/.....V.....g..fR:v.....{.I.orM..|..5...A..Eo.....g].....A..Eo.....W.#..%/..m..86775C4A5DE804838120F9125AB3C5CA751CE492315DD83C535DB2705F1ADEF8..g..fR:v.....{.I.orM..|..5...A..Eo.....(..6L.....W.#..%/.....e.....g..fR:v.....{.I.orM..|..5...A..Eo.....w.....W.#..%/..m..C746762D9A282B5C6A0CCB3CB815CCF52E354BD1A801AD023D8AF26445FF9466..g..fR:v.....{.I.orM..|..5...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\96d9db8af29d1e89_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.9799669917001825
Encrypted:	false
SSDEEP:	12:0Em80vbm4dXmrlfMMZXlazLg+eIR3K+w1G2zagc/N:0fnvbTnMZXlangTi3KxM2f4
MD5:	CD90C49E0663B3319C4416D8BC667DC7
SHA1:	81983F4E9A503398C1EF9415680B6ABA0638678A
SHA-256:	DD5F60A5B4CA3736F74286D6C72E2491A40784C2B3EFD9E905E1B9486DD82CBD
SHA-512:	8156D205800DBF035C4B73C4F47871753EA5C13838F76E568FB78F21F7D78E4EC2632DE0B068A76D05D6E2ABFAAC3771584052A7FF17E5A19B1400B20DFBB5FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....&....S...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.de.nfC-qpizUn4.O/am=B8BxhwlIGCABAEAOAAAAAAAAAHA0CCgHczzDJw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax2rIQXvBiM_NlHa1QKxh9v2Yn_xOw/m=sy7a,sy79,i5dxUd,m9oV,RAnnUd,sy73,sy74,sy75,uu7UOe,sy76,sy77,soHxf .https://accounts.google.com/..*..%/.....C.....l.QZ8....o...8/.zc....~..E....A..Eo.....".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b6319f5c3ad72ad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2971
Entropy (8bit):	5.835732558425046
Encrypted:	false
SSDEEP:	48:eWOaQDshVb66tKxKnMudvlWmFbfsVSjV1huq4hefmHx0WllEWvH+WOO3Rt/sEqgw:eWRj6YKc9IbpMiWnvH+W5t/k
MD5:	C0A127DF3AF8554C1AAE5074BA51E6DF
SHA1:	9965AC45EBECCD8A71EA671220D88C238374F2A6
SHA-256:	19BE095C2B5E47E77DE21FD08C695A715509A1E9DD1646EA729DB159CC106CB3
SHA-512:	31813922A65E639C8D77550EE4984A40F3B0FB4D657FDC5632A93EE2149EBF15E8D586FB02E552604162530DDA70F5677AD0F0C7BB5147697202D77ACCF2D99E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....kh...._keyhttps://static.hsappstatic.net/conversations-visitor-ui/static-1.11456/I18n-lang-en-gb.js .https://hubspot.com/V...%/.....V.....!E6.....1.....Q.gH...A..Eo.....A..Eo.....V...%/.`.....'.h.....O.... ...b.}.....(S.I..`.....$L`.....Qc...%....window....Q.P..J.....webpackJsonp..Qb>..[....push...`.....L`.....`.....M`.....Qe.-gG....I18n-lang-en-gb.`.....a.....QbZ.....znPIC.(S.0.`.....L`.....(S.H.`L.....L`.....a.....Q.@..3.....en-gb.....a.....Qb..[K....i18n.$.a.....Qc.....duration.<.a.....Qcn'.....seconds.. Qfv.oL....{{ seconds }} sec.....Qc..=.....minutes.. Qf.>.....{{ minutes }} min.....Qc^0.....hours.....Qe.#=.....{{ hours }} hr....Qe.....hoursAndMinutes..,Qi"..} ...{{ hours }} hr {{ minutes }} min..Qbr.s.....days..Qe...#....{{ days }} days...Qd.V.0....shortForm....4.a.....a...Qe>g.....{{ seconds }}s....1...Qe.C.....{{ m

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b8b2ce4badd6f17_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b8b2ce4badd6f17_0	
File Type:	data
Category:	dropped
Size (bytes):	205472
Entropy (8bit):	5.9922082784624315
Encrypted:	false
SSDEEP:	3072:6qkv0MSBbujeqXRe3VnYKQ5suE8K04gEFK9hArSnzg:pksMCueqBe3VYY04gE8WOg
MD5:	A4FED89D228DBCC813C3C0EFE8A3C709
SHA1:	B4FC7FE6A624EFB0C5D1C9410D1D19D6577290D0
SHA-256:	7A1822FD918F151D8AB4FD9E81C3B4C8ABCC89880FD08BE594163633AFA0E7BC
SHA-512:	14C2A5316EDC17648BF90DCEAAC2742208EF7B0643096A4B13E0E04811041C578F497D6B8C5EF8A9B4B497AC561B08E537DD849C5988CF5A05A82AFF9C1337F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@..._*.....4834E1DEAFA5F1ACF80C2846894240E7903345B96FD17F8698947A4EC038BE1B.....'.....OA.... ..R`.....|.....(....$.....,..... .....h....$.....X.....(S.e...`.....i.L`.....L`.....Qb..... ..._paq.(S.p.`.....L`.....0Rc.....Qb..J.....t...`....I`....Da".....Q.@.....module....Q.@N.h.....exports...Qc...a....document.(S.....5.a.....a.....a.....a....a.... .....a.....Pc.....exportsa.....I.....@.-....LP.!.....=...https://www.cookiesandyou.com/assets/js/scripts_6876243bd9.js...a.....D`....D`....D`.....`....&...&..A.&....&... (S....$..`.I.....L`.....Rcl.....Qb.lmm....e.....S...Qb~].e....o.....Qb...+....r.....Qb.bOh....s.....M...Qb.B.X....l.....R....Qbn@8.....c.....QbZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9bb0043db3f0be22_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	795248
Entropy (8bit):	5.972544696079979
Encrypted:	false
SSDEEP:	12288:KYrPek/bmj6u43dM3/o/rsLoOELYIvs/msBx:FrWkDfr94
MD5:	A48E00C5B779A04187170C926A752CE6
SHA1:	CA0E6BAA1FC75BD136179EAC29591020D7D9A5FA
SHA-256:	E7BE4DB34F9FED02A2C38C001171ADC4386DCBFE27C852B4FD1EDD03FF664071
SHA-512:	F50C7091CEC73F61EA296A417677E85E8C31F758415783C12724C0BA188CD4C70E8BB23EEF5D279C4C1CC5A40A9D12C03921EA3101C022EF7D3AE4CF9E9EAC D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...q3%.....4289B1939DEE4EF087B01552955EADF64B7762D978C90353F70F05F6FFB4CFF6.....'.....O.....:.....hk.....hH..... .....l.....d.....\.....t..... .....t..... .....t.....p.....p.....@...h.....\..... .....0.....l.....h.....d.....p.....<..... .@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e127b6126039886_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18507
Entropy (8bit):	5.505071741645981
Encrypted:	false
SSDEEP:	384:kf28fA6NaZytjlm8YmStBW48vULYdJojGqwmPlNp0l220O0GKQrUE9re2aikr0e7:kf2LRcLdJuJEPfGOLq
MD5:	B029BA2C207F43DC44CB0739CFCC9EC6
SHA1:	81C3BEC024CCE633147BAEA4018FFB94D2A8B64C
SHA-256:	AECA3418D3625380EDA67062E23B1F9BD4CAF098ED5700263F900F3F4A72588B
SHA-512:	56CA9782A365F8600766AD3F1C4EAF7B57A393FBD4FB2721DB41BB73EF7A0AB81B3791F32CC4527DDFDCF88A593B578151F8B1D60B5DA510B2600A90B5E957E 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....zw....._keyhttps://www.osano.com/hubfs/v2/js/common.js .https://osano.com/.+7..%/.....kY.y....F...T..:A.=.p.E.;.A....A..Eo.....z .....A..Eo..... .....'..s....O.....F..9f.....(S.=...`0.....L`.....Qc.%CK....window....Q.PV..(....webpackJsonp..Qb~,.....push....`.....L`.....`.....Ma.....`.... ...`.....A.La.....Eb.....E`....Ei.....E`.....E`.....Ed.....Ec.....Ea.....Ec.....Ee.....Ef.....Ee..... .....E`....Eg.....Ec.....E.....(S.....laA.....d.....IE.@.- ....8Q..>..E+...https://www.osano.com/hubfs/v2/js/common.js.a.....D`....D`....D`.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a00c3f9a15359b14_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114678
Entropy (8bit):	5.894960783995012

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a00c3f9a15359b14_0	
Encrypted:	false
SSDEEP:	3072:HxZblCyTamDSe7zVoDiDiRrS1BO8HW6OVoDiDR:HnbMLU0iDiR440iDR
MD5:	E5E8728C3EB611500B47EC4E6E385A21
SHA1:	BEA681E50D868459435BE0B7FA879E728B70B140
SHA-256:	E76A906F67E1433E0B4E28DC61C7A8D25844BEE417D703C88A8B898BA978C31F
SHA-512:	3FB5D17713FA8294689A4AA5EB59167C2EB62FC7B4DA6DBAA3DCC7F7C9DAB4F7BA8B4FFAC4841D43519C37F13918445958A236945062F38492B3A56F243A86D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J...n....._keyhttps://linksplit.io/js/bootstrap.bundle.min.js .https://linksplit.io/..E..%/.....q...%u..m{Skr`.....E@@.A..Eo.....B.A_.....A..Eo.....'.+3....O.....!!.....L.....(S.<..`4.....L`.....(S...`.....0L`.....Q.@.....exports...Q.@.k.....module....Qc:.....require...QcN;0.....jquery....Q.@~!d0....define....Qb^..s....amd.....`.....M`.....Qb..9.....self..Q.P.....bootstrap.....Q.@*..[....jQuery....K`....D. .....s..$...s.....&....&...&.]...&.^.....G...s.....&.(.....&.z..%&.^.....#%.'.....&.~&.-...'..(...&.^.....(Rc.....I`....Da....t.... ..f.....`...@...P.....@.-....<P...../...https://linksplit.io/js/bootstrap.bundle.min.js.a.....D`....D`....D`.....`L...&...&....&.(S.....`.3.....L`<.....Rc.....Qb.@g.....p.....S...Qb.....s.....Qb&.0G....l

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a0481ad5bef4dece_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	390
Entropy (8bit):	5.324769180761773
Encrypted:	false
SSDEEP:	6:mMl9YGLMQXrXMGVVB1U6BPB9kom4JOhK6tWMl9YGLMQXrXMGVl1ISl/S6BPB9koD:HxrXMGVnvBFIRxrXMGVlltzBF8W
MD5:	C7C2C72C6B14B54C4FB01CA7CD615B5E
SHA1:	1B8F9C81B4E1514C22AB427620959E6163A5501D
SHA-256:	8DE282B36B7C348D82B98DD62C7CF5D7833C352874CB4CA4157B8D46C03CCF6A
SHA-512:	D93744AEBD6F0189B51A9157C9FADD12F82A3DFFF74D23CBC5FA390C601C697DBB412E911BDF8F5833C22BBFFF753E41933583968700B26EB431194219208DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://www.osano.com/_hcms/forms/v2.js .https://osano.com/..1..%/.....m.....L... ....Z.N...ZJ.5.I'..zw...A..Eo.....).....A..Eo.....0\r..m.....?....._keyhttps://www.osano.com/_hcms/forms/v2.js .https://osano.com/....%/.....~.....L... ....Z.N...ZJ.5.I'..zw...A..Eo.....JkX.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a05311590db82634_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.873896217385963
Encrypted:	false
SSDEEP:	6:moCYGLMQE9ixO2mYMHqOQAiV/4ey+4ShK6tW5AmQdzTkxSXEPpQAiV/4ey+4c:yxOBhKOV8weyK7cb6FExV8weyk
MD5:	45EE471CFEFA53475DD6049016D5CB04
SHA1:	EED80714080EF0704E565166CCFBEBDA7820047E
SHA-256:	74021343E1303EE6E6B59B602625D9DBA45171150B3C254ADE205BD82B6FF585
SHA-512:	5194EC4814AF091BC592E06D0DA99F9B40D07105A6668EC15FAADF85F7935E74AAF93D1A5B30363A7C048EBFEBCCB132114FC852522CD0E664FA0AE143BA46F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....2.*...._keyhttps://www.osano.com/hubfs/v2/vendors/jquery-3.5.1.min.js .https://osano.com/..2..%/.....D.....]"O..Z..I.%....._q.%uX.....A..Eo.....N.*.....A..Eo.....2..%/..}..BD748424BF2E93A9D9E0E2E103F32D01AA8A46C6BFB072B1ACFA6221F3CF418F]"O..Z..I.%....._q.%uX.....A..Eo.....u.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a16337e915d4d6a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.482855151055106
Encrypted:	false
SSDEEP:	3:m+l7rtLA8RzYM4hGWh4MGK8T/GYJsKE5RQV2VN4RpnNlHCUGgBjwoEYc+gPSUtwN:m8rnYM47atJrSR1qpyIucc+p9/bK6t
MD5:	4CD644FD553B0798AF4FCB057901ABD1
SHA1:	A2C69E17D15B3D66C5957FBAC4DDBA02D1B42372
SHA-256:	56C7B6746DB411D3196D531D7E4FB322F7F47FF0FAE8FA5BE1D8D1D3D1A34738
SHA-512:	F4D56E2C71D34EA1B1F617AB77A85C60D427C9C8402A5463D68C2D5EBC515B66B8E2EAA3691AF5844D4C3867FFBC5FBB3EE8D998FAF5A3533C70652E128A8DD6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a16337e915d4d6a2_0	
Preview:	0\r..m.....X.....(....._keyhttps://client.crisp.chat/static/javascripts/locales/en.js?6450942 .https://sten.to/2 ...%/.....1c.....>..l.....h...Y...w.....G].A..Eo.....e.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a3c696d80a473cda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	876344
Entropy (8bit):	6.027049757477237
Encrypted:	false
SSDEEP:	12288:VFAnWFCqHgzBlSihh3uVkAmhazd5E185Qb:VuWETeVlku52OW
MD5:	E70FC0E787AB560630424AEEB0D73D06
SHA1:	BA9E2B910EF20BECB18B79B242122038E5FAF118
SHA-256:	3F1EA62C88CD244D10A23C0599BF7D63407EA7D7CDBFADE33BA0BAE8EE734193
SHA-512:	BA5FE10A36C660577D0ED75282A5F21A788CB1AB1131C19FA47EA7CF1DF54EF0690174EDE5854854D3F434F76C753ECDA7D23DC7135DD4B414981C3BDB0678 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...'.....A7A3690B36A93C8B43CD2AB6D046375233A70A4A91C16905CD6DC3E39189D653.....'..L....O.....Z..`cL.....(...$$.....X...H>..... .....X.....,.....<.....h..... .....x.....<.....p...d.....T.....`..... .....H.....\...x.....X..... .....8.....8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a749d5b3abc314c4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	379
Entropy (8bit):	5.794414682253021
Encrypted:	false
SSDEEP:	6:mzPYk+t/1ZyM1MBYwBOu2Av2LbgeMsZLthK6topMhGOuMthiESeMstZ:e+tdZNMBTBO9Av2hDPgfMtpbpZ
MD5:	C524BF757E55618FBF88B2EDAAA0D736
SHA1:	7C0464868AA1246AA9439B3830F4FB0FCD3EFA4E
SHA-256:	8B488D3501E86B1217563C8B7F543A289F4B42521F3EAF430A24582BD28BF7C0
SHA-512:	0B2DC959121B4503CAF86A2CC941A8F1C0468931BF482B2F89F19CFC239EF7AD1011F7397C10C8DDA8AC30E4D6FBE9B0B311D12106EEB5B8BAF3738FB4D6F3 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....i.O...._keyhttps://static.hsappstatic.net/conversations-visitor-ui/static-1.11495/bundles/visitor.js .https://hubspot.com/./...%/.....1.S3g.t]..c....'vb.=.rb? |..H..A..Eo.....pk.....A..Eo...../...%/..^..A7A3690B36A93C8B43CD2AB6D046375233A70A4A91C16905CD6DC3E39189D653.1.S3g.t]..c....'vb.=.rb?|..H.. A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8ee338ad3b8379b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	277
Entropy (8bit):	5.742594887000934
Encrypted:	false
SSDEEP:	6:mh2YGLMQXrXrABrYGTXW+3QI1Kl/Q9+D9oV3P2zDGaqMV11rdK6t:2crXYrfTKlY4p+PyDV1t
MD5:	90D0A4C488914B16401ED8193E5280E9
SHA1:	D78C7DA2535966EE9883FDFB078BDC5E9D153569
SHA-256:	D450EB3B186A3155A5C0771CBCB9AE2F4BBBC1C024FA91B9D470A3BEF6D3910A
SHA-512:	E59421565570969B87C14AB7309AD26A4FC2C8A14034C9D704F09BD63892C21400CBE2F2832CD97B83DB48DB0D784DBD56A5B23F38D8D27C73C2527FA8A7326
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w{....._keyhttps://www.osano.com/_hcms/forms//embed/v3/form/4785246/162149ed-dd87-457a-9bc7-d18001586306?callback=hs_reqwest_0&hutk= .https://o sano.com/`.f..%/.....C.....s.*.....2a....n..g'~N..A..Eo.....qW.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1f24eeb74b7be7f_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\b1f24eeb74b7be7f_0	
Size (bytes):	1009
Entropy (8bit):	5.440646042321344
Encrypted:	false
SSDEEP:	24:yzo//OtD1+Ftq76dzo+V1xRmWlwlyYgBfKzl50sTR/r:yzAOR1+fzdV1xRmWy8YOfKD0sTRT
MD5:	04B51A3CE090E5450E45B7CE939ACB00
SHA1:	7A1FA6BB65EC4217487880D7B8D1C0C2C16E64AD
SHA-256:	D645232516BE2600EB652D9DA38890E291784B9CAA51DB6DA1121212107FC8E2
SHA-512:	D17C405DFEEDA38AA54D40493A80B3AC56635F25FDB150F114EA28FB658ECC64AF737C68E227FBDF1CE5307F489E096152C923F959EB8AF6EA48E3499A64E49D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a..._.c....._keyhttps://www.osano.com/hs/hsstatic/cos-i18n/static-1.37/bundles/project.js .https://osano.com/..1..%/.....Z}...nZ...|..Jvr....*6...W...$ O.A..Eo.....#+2.....A..Eo.....1..%/.....'.....O.....".q.....(S.4..`"....L`.....(L`.....(S.....Ia+...R.....Qd.....hs_i18n_log.E.@.-....XP.Q.....I...https://www.osano.com/hs/hsstatic/cos-i18n/static-1.37/bundles/project.js...a.....D`....D`,...D`.....`....&...&..Q.&.(S...Iat.....(Qh.}.....hs_i18n_substituteStrings...E....d...."...@.....&.(S...Ia.....(Qh.....hs_i18n_insertPlaceholders..E.d....#...@.....&.(S...Ia..... Qf>^I.....hs_i18n_getMessage..E.d.....@.....`....DI]d.....@.....`.....a.`.....`.....a.`.....Qc.7.....use es6...K`....Dg.....&.'..a9.....&....$Rc....`.....Ib.....a.....d.....@..P.....Z}...nZ...\|..Jvr....*6...W...$O.A..Eo.....C.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b27ebd90995caa18_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	748
Entropy (8bit):	5.363517365539443
Encrypted:	false
SSDEEP:	12:8RKeTsBk01qRK//wLBkeqRKPk6LBk7qRK62LBkK:OsSgl4LSe9k6LS7ZLSK
MD5:	1CDA4E04810C4441B7B41FC53EDA3FB0
SHA1:	B0BF6A3DAF4EBACA9E43CB22AED465A2CD07F72B
SHA-256:	AEF6AE0B24426734459E6122B716B8E20DE2F0E7F38D10DEA1EB0D5FB44113E1
SHA-512:	F87EE53628A077FB4F1EDF981FDC06AB67A363311710A5C7DB16928A4F829F08C0FB5D9148C2D5FF083BA4F54E24C25502453B1890877B9542C78BFB1035A502
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7....=v....._keyhttps://s.osano.com/js/ .https://cookiesandyou.com/.n...%/.....;....{}.%2..ua..+S}.A#..r.A..Eo.....>..-.....A..Eo.....0\r..m.....7....=v....._keyhttps://s.osano.com/js/ .https://cookiesandyou.com/.{...%/.....;j.....;....{}.%2..ua..+S}.A#..r.A..Eo.....9L.+.....A..Eo.....0\r..m.....7....=v....._keyhttps://s.osano.com/js/ .https://cookiesandyou.com/|G...%/....._q.....;....{}.%2..ua..+S}.A#..r.A..Eo.....A..Eo.....0\r..m.....7....=v....._keyhttps://s.osano.com/js/ .https://cookiesandyou.com/|....%/.....&z.....;....{}.%2..ua..+S}.A#..r.A..Eo.....7.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b34387ef0f1d4348_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29534
Entropy (8bit):	5.910290450039124
Encrypted:	false
SSDEEP:	768:rXdmgsP8drEIQhIH0KrQNd5itzJ2950CZQ/l0zgx5qa:rtjduIUhNdMtM6C+/Kgua
MD5:	5B1B0E4AEEE29DA5390EC4F4A56912F9
SHA1:	0690293783E287FCBC137E53801C0F5C20FB4220
SHA-256:	4E53B1AD2DCCED574342B3F0A3905EA401927AC2A635D5FAB0F03014BC88F99D
SHA-512:	86C375E24450C64100F6DAF38F0E7CB54850DB359D6339EA23A0210CE3F719D3685D8C5A107B088A60C0B32A134C9A3B36FB11F02497CBC1F5BC03BA57E71A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f.....5....._keyhttps://static.hsappstatic.net/hubspot-dlb/static-1.129/bundle.production.js .https://hubspot.com/.?...%/.....z..~b.T.....h.?.LZg..+.&ht..s..A..Eo.....7.....A..Eo.....'..u....O.....q..2R.....(S.....`.....Q.L`.....(S...`"....`L`,....PRc$.....Qb.I.....e.....Qbv.,C....t.....Qb..j.....n.....Qb&O."....r.....S.d$.....l`....Da.....(S.....Ia$.....@.-....XP.Q.....L...https://static.hsappstatic.net/hubspot-dlb/static-1.129/bundle.production.jsa.....D`....D`....D`.....`....&...&....&....&...(S.....Pd.....i.linkDlb...a.....I.....d.....&.(S.....Pc.....i.dlbcr.a.....I..d.....&.(S.....Pb.....i.d.a.....I..d.....&.(S.....Pb.....i.r.a.....I..d.....&.(S.....Pb.....i.t.a.....d.....0@..I.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b48e7af8fbcc485d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	181
Entropy (8bit):	5.246852423963295
Encrypted:	false
SSDEEP:	3:m+lLhla8RzYW147CVRH4Rpua11lHCRXwzveZPQYN/8cfJTMme6otlllpK5kt:mClXYW+wdqp16RXwzveRQYJFlnlotlhD
MD5:	AEE2537EDE5E875DA886D818A0222C06
SHA1:	461C55EA61E8C3F700067186427A435CA61D6234

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b48e7af8fbcc485d_0	
SHA-256:	BC9AE7694014E945E280C25DD5E3C75E12E3029B2B513DB6A05769815EC4AC17
SHA-512:	4E436EEBE32CC61016549D3C05ABB39B21A8C18861EC9D9E8EBE8901FE93C98E6CE441726FD8475D98E28870C6740DCCCB0579353651B6E4D1ED4DDBB0AD8 98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.....y....._keyhttps://bat.bing.com/bat.js .https://sten.to/.....%/.....H-.....U.\T...<.kD..5&..I..aR....AzI.33.A..Eo.....f_.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4a366eda40b65cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	61635
Entropy (8bit):	5.856595969492661
Encrypted:	false
SSDEEP:	768:05KshiMuLl2SiwjIXRCIzU0xGq3aL+8ICjgxajxMp3QYVveD4djM1I:gwVRSCSUtR+8ICjtap3lmc
MD5:	96DDDCE160071013C085B3DC583AA14D
SHA1:	DF3A3E684FF81D7E96EED55A94DED7859602ACA5
SHA-256:	23D9E591726691EF762A1311CAC3D0789BCB963EEF897C01A524BFAE2348DC30
SHA-512:	FBCDBFB994351A498A08F05E2867974962A298F249B393438963DA7BAB15C3785A253729473D3C66F8B115D6E3DA25B97C9BEF1E16096286BEBFAAE45FF6BDF4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c...S....._keyhttps://www.osano.com/hs/hsstatic/HubspotToolsMenu/static-1.103/js/index.js .https://osano.com/,.1..%/.....6Y;...3G.$.(.s.d@`y.X.K{un..X0 ..A..Eo.....T..L.....A..Eo.....'.....O.....U.....$.....8.....(S...`.....(L`.....(S...`.....LL`'....@Rc..... .....Qb.~.....t.....Qb.....e.....Qbn{.....n...b$.....I`....Da.....(S...`.....L`.....Q.@.....exports..$..a.....S.C..Qb.Pe.....l...H.....a.....Qb.[).....call.....K`....D}8.....&. %.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....!.`....Da@...8.....e..... P.....@....@.-....XP.Q.....K...https: //www.osano.com/hs/hsstatic/HubspotToolsMenu/static-1.103/js/index.js.a.....D`....D`....D`.....E....`....&...&..A.&..a.&.(S.X..`l.....L`.....Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be3f4d1cb271a8f3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5128
Entropy (8bit):	5.3404675412534655
Encrypted:	false
SSDEEP:	96:uGTwIrmuAnhlJFA53KTEyKVphYZUnJdA532:LwoAhlJe6E9/YZUnJWQ
MD5:	432321246C928F415B67CD9B8D523D79
SHA1:	08A7216A06CBDDFB8AC0C6396FAA73B1205278C6
SHA-256:	46CCB785ED7F03139BCF6DF5C82424399D12F3B63B2FEE0B115974A2EDBD7482
SHA-512:	82761F6AB534DB1492158057E2533F1BCE8DA430B55BE66167F9F0BFED5D460BB7FA32C8A98C7017DFEC58C5E42F36002E3EB2B2D71F6D4F3B6A335AB5D28FD D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<.....Q....._keyhttps://linksplit.io/js/system.js .https://linksplit.io/..E..%/.....o#Kr...P2.H1.Yh\,{.B<1.U.....A..Eo.....z.....A..Eo.....E..%/.`..... .....'.....O.... .....,.....(S....`.....4L`.....L`J....(S....Ia.....Qe...`....copyToClipboard.E.@.-....0P.....!...https://linksplit.io/js/system.js...a.....D`....D`$...D `.....x...`8...&...&....&.(S...Ia..... Qf.::Z....loadingSpinnerAdd...E..A.d.....&.(S...Ia....?.... Qf.<)6....loadingSpinnerRemoveE.d.....&.(S....Ia.....d..... .....QdJ.....escapeHTML..E.d.....D&.(S...Ia2.....Qd.....ensureURL...E.d.....&.(S...Ia....$.....QeJ.....stripURLProtocolE.d.....&.(S.. .IaE...=....$Qgr.....locStoreLinkCreatedSave.E.d.... .....&.(S...IaR.....QdZq.4....urlHasParam.E.d.....&.(S...Ia.....Qd.y.2....urlParamGet.E.d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf6b71a8f83625f5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	719
Entropy (8bit):	5.7572977714117215
Encrypted:	false
SSDEEP:	12:bT/2E3hSU3TKeoux2peyyQL13CMxHDPnIze7o+BmsKlehRO9CzD0zb:H+Eb3OnuyeyyQL1SuDvY2oSmsKleheCy
MD5:	57C10A89C4718C08C1CAF33EB9CEBBC2
SHA1:	BEB12013268BB581B0BFAE0EF1A82626AE4F7E11
SHA-256:	FDCF7F5931E177E54BFC8BAFDC2DE991D14894CAF56AA7816874514B00161A2D
SHA-512:	25423D14A2570B38D09E905E30BCB6190E2307A379F85E9EB5862769E4CAD0C2D09ADFD6C5E7EBD913322D055E9E4CF20E9A18C85A8BF6FC8DABE4327954F8 E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf6b71a8f83625f5_0	
Preview:	0\r..m.....K....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/739694307/?random=1626202311856&cv=9&fst=1626202311856&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa770&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.osano.com%2Farticles%2Fccpa-guide&tiba=California%20Consumer%20Privacy%20Act%20(CCPA)%20compliance%20guide%3A%20Everything%20you%20need%20to%20know%20%7C%20Osano&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://osano.com/'.r..%/.....^.....*'.6..Xh..K.P...y8^.y.... .A..Eo.....mq.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c14ae1b8e3912eb2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	448
Entropy (8bit):	6.074980995871831
Encrypted:	false
SSDEEP:	12:i2Em80vbm4dXmrlfMMZXlazLm8vAeKvLp++zwl:i2fnvbTnMZXlanmb12
MD5:	1C9BE0C392FA3714185571F1125FD914
SHA1:	B72FE100BFF59C442BCD151D736E0A47A8FFDDCB
SHA-256:	B1C8060BBDD8A9A78E4FAD713509C982B90C3DF05FE00453311692F4766E52F5
SHA-512:	83153A8DB0A25ADD16E8DDF6E8A385A6A26C23F955B5B16931F3C4655BCCF2ADC89F1DAD58E44EEA9876A90A9FF367BD3B00A36E9D8600B8B309933218BB4ADA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<....Cq....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.de.nfC-qpizUn4.O/am=B8BxhwIIGCABAEAOAAAAAAAAAHA0CCgHczzDJw/d=0/excm=glif_initial_css/ed=1/rs=ABkqax2rIQXvBiM_NlHa1QKxh9v2Yn_xOw/m=n73qwf,MpJwZc,NpD4ec,SF3gsd,O8k1Cd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,otPmVb,rlNAl .https://accounts.google.com/..#..%/.....GC.....%.t4l...K...:Q...r..S..P....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c9480df859bb86c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	401952
Entropy (8bit):	6.0599460383839245
Encrypted:	false
SSDEEP:	12288:MBhjGKgvyveLywnEgE0m3VBw15VY6By+wyF:MBhPgIeZEgE0m3VBYJy+t
MD5:	DBC2CE44AA09F353A5466A7F9792F852
SHA1:	A004D1DD3DB35434EE603506CE36074798A0CAC5
SHA-256:	2B1C071BAE1A31E87B0F47598A17C8EB4E1D49AE28C263ECD95DA0BAC8F705B4
SHA-512:	551EC1C0A692006ADB92B07D665ADFFE42B3B7B480397D48EE9ED059D8FD465B852FA1B2D3FF5A678DA69949F6658699976E739D4B7DF723FEBC82A870800DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...YE.....F6E41ED76CF40DCEE5BF9E649BBEC4639D10BA921B0C7AC83FDFD197FEF04EA1.....'..u....Ov...x...f.V.....X.....t.....d.....8.....$...t(..L.....|.....4&.....P.....h.....P.....<.....8.....h.....t.....(S.....`.....Q.L`.....(S...`'....`L`,....PRc$.....Qb.I.....e.....Qbv.,C....t.....Qb..j.....n.....Qb&O."....r.....S.d$.....I`....Da.....(S...`.....L`.....Qc.-.....exports..$..a.....C..Qb.|a.....l...H..1 ...a.....Qb.. .....call...!..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca94bfbcd194da51_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50737
Entropy (8bit):	5.922756151755232
Encrypted:	false
SSDEEP:	768:zmaWHZGyDjnlteFj0caagLI2OVtbUErs742dyxC9+xOqH8Hx5mxE7Vp2uVzYGZVV:S/Hsejnaaal+ysXxJ6SGVPpT
MD5:	C5BC7E738BB6FB2B4B5E33243D68AF74
SHA1:	14B8980EA256800E4E9ECFD352B51FE528BE2527
SHA-256:	1E6D5A1452D7EFA79130063A908D7E2F1D34A31553D889AD4CC0D41CF21D1D01
SHA-512:	4D4A7D527D3F1BA65EAE5782E2D3389D453D0C91DCD7487860EBBE3D54261BA8B798D60F52FC45E8BEBAA203A16A4E8880E1202AE5A914C49E23079F8C4047A8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....,_keyhttps://js.hubspotfeedback.com/feedbackweb-new.js .https://osano.com/.Oj..%/.....zbg....K].nQT.h..e...~0..+..W.A..Eo....._.....A..Eo.....'.:v....O.....d'.....t.....H.....P.....(S.....`.....lL`2....(S...`.....L`.....Rc<.....Qb".....r.....Qb.....o.....S....M...Qb..c.....Qb..q.....f.....Qb..P....s.....Qb..\P....d.....Qb.Pe....l....Qb...-....p.....QbZ.....h.....O...QbN.....m.....Qb.[.....v.....Qb.....y.....Qb.....w.....Qb..q.....k.....Qb*.)c....x..Qb&.}.....E.....Qb.....j.....Qb.H.....O.....Qb6.|.....S.....Qb.....I.....QbR..0...._.....Qb.W.....T.....Qb..<!....L.....Qb..8)....C.....Qb.....P.....Qb.:.....W.....Qb^.....A.....Qb.....N.....Qb".....q.....Qbv.....D.....Qb.:mw....U.....Qb..l.....V.....Qb~}.....z.....Qb.o.....B.....Qb.t.....G.....Qb.V.....Z.....Qb>.....X...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cba48e6402f88eb4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4935
Entropy (8bit):	6.044959271675586
Encrypted:	false
SSDEEP:	96:DaPAOFyax3IaMliPPlwHp3s6zX2JWrmaYc/t0vofxkqFfqg82:DaIewaMUtgzGorbb/lRfX82
MD5:	02CB1F98AFA9A2D0D1BC10DB8FA74C71
SHA1:	BF547CC8AAE39D480392D47672D0E4946956C043
SHA-256:	751CE80CC553BD0E0191C690160FAF281C408E74F9C3965225A788368A91F2FA
SHA-512:	C0E66BC3618FF7D277B675D09C422D6BD89C692E7EE6CC1C061C622CA65C8C5104BB081AD10E3297A4EA8AE77C321BD06A1C986C9F50AD9A3076753050F8397
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....!'x...._keyhttps://f.vimeocdn.com/js_opt/modules/utils/vuid.min.js .https://vimeo.com/...../.....J...Ea.....B...M..w~-..A..Eo.....P.....A..Eo.....'.h.....O.....y.....(S.4..`$.....L`.....(S.I..`H.....L`F....HRc .....Qd..A...._getrandmax...Qc.mDO...._rand.....Qc....._round....Qb.J....._ordc.....I`....Da.....(S.(.`.....L`.....Xa.....A..K`....Dd.....,Rc.....`....Dan.....@.-....DP.....7...https://f.vimeocdn.com/js_opt/modules/utils/vuid.min.js.a.....D`....D`....D`.....0...`....&...&....&..!.&.(S....`.....L`.....<Rc.....Qb..W.....min...Qb..OG....max.a....d.....A.`....Da.....M...Qb..Z.....Math..Qc..^....floor.....Qc2@'.....random....K`....D|0.....%...%....&.(...&..h.....&.\.....&.(...&....&.(...&.X...&...&...5..@..6..&.Y....&...4.....e.....@

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cef4a1434eb85d8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1095
Entropy (8bit):	5.3520558292900215
Encrypted:	false
SSDEEP:	24:YMq8dd6/RbC7WRbgTF4gEOC8dAz0ylJNbAimX5oxnMRbe:Yn8LuC7Q8zQ86YI3bKXm4e
MD5:	5EDD00B98E5EBF5FBD56A9CC36E8868D
SHA1:	74DB3E298F0608C38715B8B4946B6704870DBCA6
SHA-256:	D5BD611A8EA3399C9581F0853EDE0EDD4EA6B3422B0BC7E252A5DC117F77501D
SHA-512:	27A5DD2331D882B66FDB23B0CD70EFBB0AF383E0C4B2DC4CD6047A4DA18B5C3CFADFEE0D7511B16B8FCFEF60F9E240FC441AC9AFD36C9FABA23B81AAC45A6BB1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...{i.[...._keyhttps://linksplit.io/js/url-shortener.js .https://linksplit.io/.O%..%/.....^..a.....|S.d.h..X.n..i&...,8.A..Eo.....}.....A..Eo.....O%..%/.....^..a.....|S.d.h..X.n..i&...,8.A..Eo.....T<'n.....O%..%/.....'.....O.....0.....(S.T..`^.....L`.....L`.....(S....Ia"...z.....d.....(Qh.s6.....shortLinkCreatedModalOpen...E.@.-....4P.....(...https://linksplit.io/js/url-shortener.jsa.....D`....D`"...D`.....0...`....&...&....D&.(S.....Ia.....(Qhb=.....shortLinkCreatedModalClose..E....d....#.....&.(S...Ia.....,g.....d.....@.....d.....IE.d.....D`....Dl]d....".....`.....A.`.....Q.@.{l.....document..Qc>.a....ready.....K`....Do .....&.'..a9.....&...&.]...&.(...&.....&.Y....&.....$Rc....`.....lb.....c.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d189f289189e4734_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	191
Entropy (8bit):	5.313444496581335
Encrypted:	false
SSDEEP:	3:m+lpXIzs8RzYUL9QqgAd7sDzL9QqslHCFZMfPWDTP4/GzMmIZI///pK5kt:mkXIRYUrgABMr3Fyno4ujT//hK6t
MD5:	62573F0ACFFCAA945A31D8A944BC2AC5
SHA1:	0EDE26E88FEFD011C1290E577587EFE6BEB365F3
SHA-256:	1F6F46817CE5393CBAF6D41B96B467949F57A6FBBA207DF8591868F0B7F1A67F
SHA-512:	8CE97BF286AFD2AAEC91BA19D01707EA3498B17A566FDFD73997D762BECC951E5C9FB6BF2AB41D80FCDBBAF867782CC719A295C8747B93EF26769453C3B60F42
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;...~V.D...._keyhttps://linksplit.io/js/index.js .https://linksplit.io/.%F..%/..... .....3.g..^..$.....U.....&..A..Eo.....I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\db5b53bc02019426_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	357
Entropy (8bit):	5.862475492254971
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\db5b53bc02019426_0	
SSDEEP:	6:mXfgEYGLgLKfyOuwQP6KSy3/NDllFNAjMVzbK6tflVzdU2fQSwOah039DllFNA4:zRLKvCP6KSepnXmUzNjVasQjOay3hnX
MD5:	8AD56FFE1F04053B747FC42788B357A3
SHA1:	014671281C8D5E2B560F4F882F30C10AFB1BC587
SHA-256:	6E60159799382E87EB61312818676BF230E2B5B9BD4D095FB367939D58467873
SHA-512:	82AC88CCCABE7A2EAEF99646440C13F8CD5E714EE99B4BDCBB2E4608700E78AA208496151053BBDFB95D8BD675506447FFB05C5AFA1C618BBF33D44366A87D F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....._keyhttps://www.cookiesandyou.com/assets/js/scripts_6876243bd9.js .https://cookiesandyou.com/!....%/.....i.....O&....v.f..p.b.&....D...p..#..A.. Eo.....t:.....A..Eo.....!....%/..!..4834E1DEAFA5F1ACF80C2846894240E7903345B96FD17F8698947A4EC038BE1B..O&....v.f..p.b.&....D...p..#..A..Eo.....L.. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ddff1a5ff7aa3ab1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.477173778765557
Encrypted:	false
SSDEEP:	6:m+PVlXYET08NyEZKqhEzFUr1BAd1uM4qHEb54t0/ZK6t:Jtlzg8NyE0qhXrwxzmT
MD5:	0F7F090A74495A7153A1C0E3B04043B4
SHA1:	4939DED7EFECC97A07628C27623DE386FA3FC799
SHA-256:	A695496EFCBD2A0BAF59DED1DA59C4097DF2E51596F4D8705AC633CC631EC1B6
SHA-512:	73613A124E208E117D638CB3AEBD8F2F570EF9C590C17C11532E4513BC638005507F9E3B9552A6DCC653D817F3886DD5D5BD05D987585F8D4B78D0B7A7532DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...s.a....._keyhttps://cdnjs.cloudflare.com/ajax/libs/vanilla-lazyload/10.17.0/lazyload.min.js .https://linksplit.io/~.B..%/.....e...)....A.4...!m.~.`>R=..M:.x.. A..Eo.....X0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e40b398d18280ba9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8965
Entropy (8bit):	5.943235098731734
Encrypted:	false
SSDEEP:	192:Q09g4xXpfKa2DFjme3LP7oy74783w3/se4/e4CgQgeRRRzWmxmbcKMcKJ6E66Tz9:U4FGjmuLP7oy74783w3/se4/e4CgQgex
MD5:	4332083D1BA053F3C6DE251C7958019B
SHA1:	CD2149F8C9F9213BA94A45827FA3C77004D4662E
SHA-256:	CE0D3A4D55838926B747A5B7E615F007BB8DB1C08EE1A82812B725F4F330119B
SHA-512:	89B18C7A932237333C2A29608E929CB6ADDC984BA942582A6D100A9199EEEB1E589264598E4B96FECA12A39BDDDA9CF771161C7B3E189CA89B52F050199758B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...*"[A...._keyhttps://unpkg.com/ionicons@4.1.2/dist/ionicons/oypc542y.js .https://linksplit.io/..K..%/.....T..T...".O...lq.a;.3.(v....A..Eo.....@..... A..Eo.....'.....O.....!..S.4.....0.....(S....`.....dLa....j....(S...`z....0L`.....Qb.....md....Qd.....toLowerCase...Qb.WS8....ios.. Qf.6".....^md-|^ios- |^logo-.....Qb.....test..Qb.S.....-...I..Qb...N....trim..QcjJ.....replace...Qd.....[a-z]|-|\d....K`....D.1.(...(.....%.....&.(...&.X...&.%.....&.%.h....(...&.X...&..M%.....&.%.h....(...&.X. ..&..0%...y...&.(...&.Y....P....4..&.(...&.X...4..&.%.s.....&.(...&.X...h.....&..&.(...&.y. .&...&.Z....!h.#.....%....,Rc.....Qb.....s...`....Dad,..J....XRc(....c.....Qb...x....t.....S.. .a...Qbvl.+....n...c.....Ib.....$/... ..`.....]..L`.....Qb.....e...`.....L`.....Qc.....IonIcon..]`.....Q.a.....$..g$.....X.....@.... .L. .@.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e40f83db75fdb6df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23179
Entropy (8bit):	5.743549274930433
Encrypted:	false
SSDEEP:	384:TYoNpyhxauietCbCNA9zAFNSZQB9qgKCVdH/g0wA:TXyhUuioC9EFNSw9fYk
MD5:	11F192596F26FA5BD07C685A217E590E
SHA1:	9E8586EC80ED7C8C98B8ADB741D05AEB64AAA456
SHA-256:	D6702C155227276C651AA9FB945D9F5C646A9F7E1DF4306B8DD80EFBB75AB37F
SHA-512:	E3B91E39EF610EA6FAB8E4BDBD993CC800FDE6671D7E42D308740962AF02372E305D16B4DE6072648341390 15F6590BBE2526D2E468EDB48B55686FDD6F6BAC E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e40f83db75fdb6df_0	
Preview:	0\r..m.....S....a...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://osano.com/.]o..%/.....[.!.u?7^..s~a..2nA5Z!O.!....A..Eo.....d.N.... .....A..Eo.....'.....O.....Y....[.....p.....(S.<..`2.....L`.....(S....`*....M.L`.....Rc.....j.....Qb.V.:....aa....Qb.Pe.....l.....Qb.....ca.... Qb6.w.....da....Qb.~.....t.....Qb.....ea....Qb.[.....v.....QbR..e....fa....Qb.OO_....ha....Qb^.....A.....Qb..:....ia....Qb.....ka....Qb6.....ma....Qb.L.....la....QbV.].....na....Qb..u*.... oa....Qb.....pa....Qb".....qa....Qb>?X.....ra....Qb^.....sa....QbVWE.....xa....Qb.}S.....Aa....Qb.....Ca....QbBu.|....Da....Qb..~.....Ea....Qbz.....Fa....Qb..X....Ga....Qb6`./... .Ha....Qb..c.....Ia....Qbf.;.....Ja....Qb.o.....B.....Qb.....Ka....Qb~.....La....Qb./D.....Na....QbV.'.....Oa....QbJS.....Ma....Qb.....Pa....Qb.C.....Ra....QbnG.....Sa....Qb.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e6dd3e78319382db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.269494357646828
Encrypted:	false
SSDEEP:	3:m+lyvlLA8RzYUL9QqgLaUvDzL9QqYP11lHCCz5RBQMLt+JPP5ml/tpK5kt:mxlVYUrgeerYlCHLMx4EbK6t
MD5:	A8A03BFEE81B4AFD91B03B2F0927F8A6
SHA1:	8AC77B4FD56ED52072493F687B096B4424FAD1D6
SHA-256:	2BD533AA617DB3FEF092552A54FD5FBF580D9F559897FB2364ABAB231A7AEFB8
SHA-512:	AD929E77C326A548057B6A51CAE6CEF93A60DC64209A114C020C79BEFDE0D3E824C1140C7AEDFF10485D236347B8C75883A4589FE650B0CF59109690AD130A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B.....-|...._keyhttps://linksplit.io/js/link-rotator.js .https://linksplit.io/.m9..%/.....Lk#.#mF.L.f..8..N3}..f..E.h.|..A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e8d31d226215b290_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	705
Entropy (8bit):	5.724574678104199
Encrypted:	false
SSDEEP:	12:ejE3hSUtc4oux2peyyQL13CMxHDPnIzhQJaW55WpW4xMvV+CzquvC0mp:EEbtcBuyeyyQL1SuDvYhQznW44pCzrzG
MD5:	3CCAB57C7DE88B9AEBDF5A8C63EDE911
SHA1:	CAA7BE31A547CE3F72E5D4EBA0601F62EC09C55F
SHA-256:	0360D5BC8C9D4CE59282E1B264D4881F1578E3ADD046BCF3A6B4251DD4C87F8D
SHA-512:	63EE99FF5942CFB041F58C21D76F2D5A56915FEF2961F063FDE21A5D914BBBEA7D1E0D2D58645A8D55A185437819F12799E1DAFBB03EFF2F7BD469D5EC27421
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=....n.X...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/739694307/?random=1626202322352&cv=9&fst=1626202322352&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=120&u_java=fa lse&u_nplug=1&u_nmime=2&gtm=2oa770&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.osano.com%2Farticles%2Fgdpr-compliance- regulations&tiba=12%20Facts%20about%20GDPR%20Compliance%20Regulations%20You%20Need%20to%20Know%20%7C%20Osano&hn=www.googleadservic es.com&async=1&rfmt=3&fmt=4 .https://osano.com/o..../.....0.....*..1..\k..R..._.W....?.h.X....}.A..Eo.....Z.&_.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f17c7f5a63070cac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97368
Entropy (8bit):	5.790925582917552
Encrypted:	false
SSDEEP:	1536:yQeMf7VS3XQ6BG3BF9h9b/+WVbt6q9ThI/pBZ2+YXO+oRKJt:yQeMf7VS3AKG3BF9nb/+WVbDXaXZiHWg
MD5:	44FB1F7BAD1F838C718A7A83FB07E3A0
SHA1:	5A9204BCE3FE7EA4C76FF7258A72692F89B2A627
SHA-256:	9046C3544C9C15663D3965517B4CE2E536377AECD6A69804DDE04B0FFFA9298C
SHA-512:	3D82C3E2C3C48C0E9151C9106A873937C4079693C43B5714F1B78DE949C315E7E1872C3C55BD5F0BD39ED167A112403CDA659DEFF887CD9C8AA180D7666F69F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....q.u....B2D10AC120DCC1525D629F631316DE81C5E95207E6B67097101735E197816562.....'.*p....O!....{.....t&..d.....h.... .....(S.0..`.....L`.....(S...u&..`.L.....e.L`.....RcJ.....Qb..9.....data..Qb.....ba....Qb..2e....da....Qb.....ea....Qb.J.....l a....Qb*V.....pa....Qb.....qa....Qb.l.....ra....Qbz.U.....sa....Qb.Z".....ta....Qb.....ua....Qb.....va....Qb.01i....wa....Qbj.n!....xa....Qb...H....za....Qbn.#/....Aa....Qb.....B a....Qb..kM....Ea....Qb.....Ia....Qb.....Ja....Qb.sA5....Ka....Qb.z.1....La....Qb62.....Na....Qb.U.e....Oa....Qb.a.....Pa.....Qb>.....Ha....Qb*.g.....Ra....Qb..o.....Ta....Qb..'. ....Ua....Qb.'.....Va....Qb.@.....Wa....QbV.y.....Xa....QbV.....Za....Qbz.Q.....ab....Qb.0.*....bb....QbBG>/....eb....Qb2.....cb....Qb.....fb....Qb..-.....gb....Qb..<U....kb....Qb:vf5. ...mb....QbN

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f29f86b73c320c8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f29f86b73c320c8d_0	
File Type:	data
Category:	dropped
Size (bytes):	77280
Entropy (8bit):	5.762461823168011
Encrypted:	false
SSDEEP:	1536:Dsef8Nhh+caaYRbtYEcnMoKjqHwMdga+2fLY:Dsef8Nhh+7aYRBYEUMfSwMJ+2U
MD5:	27FCE2088EDE48A98B370D4B3A3CE6D8
SHA1:	215ED009DD9B94B81B25C63183731DD777E2DD29
SHA-256:	46C494AAB15B596282C4597BD4CA2741F574E57C607F1F698F2DAC68D1866FD4
SHA-512:	758972B2E88B872A88AD47669F9242BAE7C830C8ABEBDC84F929D6040D26AE33739C5B3A091A3C9D2782B7A755108A81BB3BDF23DCFAAAC811C49F121A803C 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....T.....980221479666CE22D890A9047E86279F6953222EA87CF275429383A4EB83A99E.....'..j....O....,.....W.....D&..8..... .....(S.0..`.....L`.....(S...E&.`>L.....9.L`.....Rc.....Qb..9.....data..Qb.....ba....Qb.....ea....Qb.J.....la....Qb*V.....pa....Qb.....qa. .....Qb.I.....ra....Qbz.U.....sa....Qb.Z".....ta....Qb.....ua....Qb.....va....Qb.01i....wa....Qbj.n!....xa....Qb...H....za....Qbn.#/....Aa....Qb.....Ba....Qb..kM....Ea....Qb.....la....Qb... ....Ja....Qb.sA5....Ka....Qb.z.1....La....Qb.>.....Ma....Qb62.....Na....Qb.U.e....Oa....Qb.a.....Pa.....Qb>.....Ha....Qb*.g.....Ra....Qb..o.....Ta....Qb..'.....Ua....Qb.'.....Va.... Qb.@.....Wa....QbV.y.....Xa....QbV.....Za....Qbb.....$a....Qbz.Q.....ab....Qb.0.*....bb....QbBG>/....eb....Qb2.....cb....Qb.....fb....Qb..-.....gb....Qb..<U....kb....Qb:vf5....mb.... QbN..1....n

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f37b23163de7c9f2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97840
Entropy (8bit):	5.834351362498272
Encrypted:	false
SSDEEP:	1536:5VkGe64Vog5vwWpxhMP8m1jom6t/NtYr2wRwAOR77t2PfkBwpRVamR:Ub6X2GEjHj6R
MD5:	1CAF8C600D94BEEFC4CEB3D31E65A322
SHA1:	E49912BFF354B54B404BF24FE7225C257A44AA81
SHA-256:	26BA0A8AF677885AE14D4DF208D021C1B997B4D64CE9553AB82612EAD3CB5AFB
SHA-512:	0A172025DECB0085D25D4413867076CBD25FE417AD27E1E6A4921ED0D689CAAE60F4F1A0D5B19EA39E20147A4D791174C30B0AF1224B0BF793FB54CC78D6DA 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....BD748424BF2E93A9D9E0E2E103F32D01AA8A46C6BFB072B1ACFA6221F3CF418F.....'..]....O!....|... i*.....`&..... .....`.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb.~.....t...`....I`....Da....j.....Q.@..>.....module....Qc.....exports...Qcz..?... .document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....HP.....:..https://www.osano.com/hubfs/v2/vendors/jquery-3.5.1.m in.js..a.....D`....D`....D`.....`....&...&..!.&....&.(S...a&..`|L.....L`.....Rcd.....*.....Qb..8)....C.....Qb"....r.....Qb..P....s.....R.....S...Qbn{.....n.....Qb.....o.....Qb. [.....v.....M...Qb.Pe.....l.....Qb.....y.....QbN.....m.....Qb*.)c....x.....Qb&.}.....E.....Qb.....c.....O...Qb.....w.....Qb6.|.....S.....Qb...-....p.....QbZ.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f60b41527a6cf03c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35989
Entropy (8bit):	5.532855308219212
Encrypted:	false
SSDEEP:	768:6xVFU02J5ijgZxees1UvIb7sPH2mJ1Or/6b1GnNg8:8VFL+muHXAbIf2P6bV8
MD5:	125B2D52981FAA3C5ECDC8B7AA6FC544
SHA1:	825AE777AEDD75D9E0A2D8643A912A1B1911338F
SHA-256:	718357C1C69E4AD2512FC321C051763D7298831F83DBA3168A7EE2EBBC352846
SHA-512:	C0996FBC2DB003F9DB426CB1AA87968A6DE02DE2136082F12AEDEE6AEA32AD61C2F3BDA1A62287162665C1E306D2D244C4BEC9BE5598D53EBA6324310B80A5 82
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M...6....._keyhttps://browser.sentry-cdn.com/5.1.1/bundle.min.js .https://linksplit.io/..D..%/.....z..2.....[..B...1.....h;`...YY.A..Eo.....s..Q.....A..Eo..... .....'.....O.....>.%.....(S.@..`<.....L`.....L`.....Qc.....Sentry...(S...`.....L`t....Y.Rc.....Qb^.N.....n.....Qb.8.....t.... .Qbz\.8....r.....R....Qb.....c.....QbJ/F.....s.....M...Qb.A.....f.....Qb..k....h.....QbNd.<....v.....Qb...U....l.....QbFea=....d.....Qb.qn.....p.....Qb.....m.....QbZwT.....y.....O...Qb..... .w.....Qb.5.....E.....Qb6*.....j.....Qbf.Z.....x.....Qb.ip.....S.....QbN.uQ....O.....Qb....._.....QbZ.kj....k.....QbB.P.....R.....Qb~.....D.....Qb.....I.....Qb^qv.....A.....Qb.X;7....C... ..Qb2.Ix....L.....Qb2.....M.....Qb.0.....N.....Qb...L....F.....Qb..3y....U.....Qb.'N....P.....QbN.Kn....q.....QbZ.....H.....QbZ1^.....W.....QbN.ol...

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 13, 2021 20:50:53.963255882 CEST	192.168.2.4	8.8.8.8	0xe3f2	Standard query (0)	linksplit.io	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.565917969 CEST	192.168.2.4	8.8.8.8	0xc9c4	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.565944910 CEST	192.168.2.4	8.8.8.8	0x1aa8	Standard query (0)	ajax.cloudflare.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.283710003 CEST	192.168.2.4	8.8.8.8	0x41a8	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.298855066 CEST	192.168.2.4	8.8.8.8	0x89e4	Standard query (0)	browser.sentry-cdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.301621914 CEST	192.168.2.4	8.8.8.8	0x5c27	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:56.659508944 CEST	192.168.2.4	8.8.8.8	0x4c18	Standard query (0)	linksplit.io	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.637527943 CEST	192.168.2.4	8.8.8.8	0xed7f	Standard query (0)	cookiesandyou.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.845869064 CEST	192.168.2.4	8.8.8.8	0x8e0f	Standard query (0)	www.cookiesandyou.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.030457973 CEST	192.168.2.4	8.8.8.8	0x3978	Standard query (0)	player.vimeo.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.146980047 CEST	192.168.2.4	8.8.8.8	0xa848	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.290843010 CEST	192.168.2.4	8.8.8.8	0xa598	Standard query (0)	s.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.406744003 CEST	192.168.2.4	8.8.8.8	0x1b84	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.406827927 CEST	192.168.2.4	8.8.8.8	0x9b5d	Standard query (0)	fresnel.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.406848907 CEST	192.168.2.4	8.8.8.8	0xc3e	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:04.995162964 CEST	192.168.2.4	8.8.8.8	0x9794	Standard query (0)	vimeo.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:06.406497002 CEST	192.168.2.4	8.8.8.8	0x5f1b	Standard query (0)	www.cookiesandyou.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:08.797512054 CEST	192.168.2.4	8.8.8.8	0xcdc3	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:14.544595003 CEST	192.168.2.4	8.8.8.8	0x2a54	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:16.100948095 CEST	192.168.2.4	8.8.8.8	0xc0bb	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:23.969913960 CEST	192.168.2.4	8.8.8.8	0x8573	Standard query (0)	li.sten.to	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.715497017 CEST	192.168.2.4	8.8.8.8	0xc8ec	Standard query (0)	static.cloudflareinsights.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.719280958 CEST	192.168.2.4	8.8.8.8	0xcb72	Standard query (0)	client.crisp.chat	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:25.335120916 CEST	192.168.2.4	8.8.8.8	0x4c24	Standard query (0)	client.relay.crisp.chat	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:26.687411070 CEST	192.168.2.4	8.8.8.8	0x6c18	Standard query (0)	li.sten.to	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 13, 2021 20:51:28.283241034 CEST	192.168.2.4	8.8.8.8	0xac58	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.284363985 CEST	192.168.2.4	8.8.8.8	0xa057	Standard query (0)	linksplit.io	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.302316904 CEST	192.168.2.4	8.8.8.8	0xb952	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:30.588334084 CEST	192.168.2.4	8.8.8.8	0x738d	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.371846914 CEST	192.168.2.4	8.8.8.8	0xebda	Standard query (0)	www.cookiesandyou.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.704724073 CEST	192.168.2.4	8.8.8.8	0x26de	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.705570936 CEST	192.168.2.4	8.8.8.8	0xe410	Standard query (0)	fresnel.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.705835104 CEST	192.168.2.4	8.8.8.8	0x9f36	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:46.202708960 CEST	192.168.2.4	8.8.8.8	0x212f	Standard query (0)	www.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.312673092 CEST	192.168.2.4	8.8.8.8	0x4b3a	Standard query (0)	cdn.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.315570116 CEST	192.168.2.4	8.8.8.8	0xf7fa	Standard query (0)	cmp.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.597364902 CEST	192.168.2.4	8.8.8.8	0xe3df	Standard query (0)	no-cache.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:49.955174923 CEST	192.168.2.4	8.8.8.8	0xde58	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:50.621741056 CEST	192.168.2.4	8.8.8.8	0xcc4c	Standard query (0)	consent.api.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.378000021 CEST	192.168.2.4	8.8.8.8	0x87b4	Standard query (0)	js.hsleadflows.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.535607100 CEST	192.168.2.4	8.8.8.8	0xdc0	Standard query (0)	app.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.667192936 CEST	192.168.2.4	8.8.8.8	0xde2a	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.784713984 CEST	192.168.2.4	8.8.8.8	0x4203	Standard query (0)	js.usemessages.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.789437056 CEST	192.168.2.4	8.8.8.8	0xd062	Standard query (0)	js.hubspotfeedback.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.794445038 CEST	192.168.2.4	8.8.8.8	0xf693	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.821156025 CEST	192.168.2.4	8.8.8.8	0xa182	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.189152956 CEST	192.168.2.4	8.8.8.8	0x844e	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.287730932 CEST	192.168.2.4	8.8.8.8	0x9f1e	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.429680109 CEST	192.168.2.4	8.8.8.8	0x3978	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.832259893 CEST	192.168.2.4	8.8.8.8	0xa6b6	Standard query (0)	perf.hsforms.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.832694054 CEST	192.168.2.4	8.8.8.8	0x2d4d	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.832881927 CEST	192.168.2.4	8.8.8.8	0x7906	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.017684937 CEST	192.168.2.4	8.8.8.8	0x80ae	Standard query (0)	static.hsappstatic.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.043138027 CEST	192.168.2.4	8.8.8.8	0xc530	Standard query (0)	api.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.486174107 CEST	192.168.2.4	8.8.8.8	0x7935	Standard query (0)	feedback.hubapi.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.735620022 CEST	192.168.2.4	8.8.8.8	0xb5af	Standard query (0)	f.hubspotusercontent40.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.085621119 CEST	192.168.2.4	8.8.8.8	0x45b3	Standard query (0)	www.osano.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.145139933 CEST	192.168.2.4	8.8.8.8	0x5cfe	Standard query (0)	no-cache.hubspot.com	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.089375973 CEST	192.168.2.4	8.8.8.8	0x3249	Standard query (0)	static.hsappstatic.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:59.141958952 CEST	192.168.2.4	8.8.8.8	0x7b09	Standard query (0)	f.hubspotusercontent40.net	A (IP address)	IN (0x0001)
Jul 13, 2021 20:52:21.008003950 CEST	192.168.2.4	8.8.8.8	0x8b43	Standard query (0)	tattle.api.osano.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:50:54.029756069 CEST	8.8.8.8	192.168.2.4	0xe3f2	No error (0)	linksplit.io		104.21.2.221	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.029756069 CEST	8.8.8.8	192.168.2.4	0xe3f2	No error (0)	linksplit.io		172.67.129.190	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.586687088 CEST	8.8.8.8	192.168.2.4	0x1aa8	No error (0)	ajax.cloudflare.com		104.16.168.35	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.586687088 CEST	8.8.8.8	192.168.2.4	0x1aa8	No error (0)	ajax.cloudflare.com		104.16.167.35	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.606534958 CEST	8.8.8.8	192.168.2.4	0xc9c4	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:54.606534958 CEST	8.8.8.8	192.168.2.4	0xc9c4	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.312261105 CEST	8.8.8.8	192.168.2.4	0x89e4	No error (0)	browser.sentry-cdn.com		151.101.2.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.312261105 CEST	8.8.8.8	192.168.2.4	0x89e4	No error (0)	browser.sentry-cdn.com		151.101.194.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.312261105 CEST	8.8.8.8	192.168.2.4	0x89e4	No error (0)	browser.sentry-cdn.com		151.101.130.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.312261105 CEST	8.8.8.8	192.168.2.4	0x89e4	No error (0)	browser.sentry-cdn.com		151.101.66.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.324126959 CEST	8.8.8.8	192.168.2.4	0x41a8	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.324126959 CEST	8.8.8.8	192.168.2.4	0x41a8	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.324126959 CEST	8.8.8.8	192.168.2.4	0x41a8	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.324126959 CEST	8.8.8.8	192.168.2.4	0x41a8	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.324126959 CEST	8.8.8.8	192.168.2.4	0x41a8	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:55.331589937 CEST	8.8.8.8	192.168.2.4	0x5c27	No error (0)	www.googleoptimize.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:56.708674908 CEST	8.8.8.8	192.168.2.4	0x4c18	No error (0)	linksplit.io		172.67.129.190	A (IP address)	IN (0x0001)
Jul 13, 2021 20:50:56.708674908 CEST	8.8.8.8	192.168.2.4	0x4c18	No error (0)	linksplit.io		104.21.2.221	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.656546116 CEST	8.8.8.8	192.168.2.4	0xed7f	No error (0)	cookiesandyou.com		143.204.98.55	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.656546116 CEST	8.8.8.8	192.168.2.4	0xed7f	No error (0)	cookiesandyou.com		143.204.98.120	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.656546116 CEST	8.8.8.8	192.168.2.4	0xed7f	No error (0)	cookiesandyou.com		143.204.98.117	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.656546116 CEST	8.8.8.8	192.168.2.4	0xed7f	No error (0)	cookiesandyou.com		143.204.98.89	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.867291927 CEST	8.8.8.8	192.168.2.4	0x8e0f	No error (0)	www.cookiesandyou.com		143.204.98.44	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.867291927 CEST	8.8.8.8	192.168.2.4	0x8e0f	No error (0)	www.cookiesandyou.com		143.204.98.37	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.867291927 CEST	8.8.8.8	192.168.2.4	0x8e0f	No error (0)	www.cookiesandyou.com		143.204.98.89	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:02.867291927 CEST	8.8.8.8	192.168.2.4	0x8e0f	No error (0)	www.cookiesandyou.com		143.204.98.51	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:03.042614937 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	player.vimeo.com	vimeo.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:03.042614937 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	vimeo.map.fastly.net		151.101.0.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.042614937 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	vimeo.map.fastly.net		151.101.64.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.042614937 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	vimeo.map.fastly.net		151.101.128.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.042614937 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	vimeo.map.fastly.net		151.101.192.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.173120022 CEST	8.8.8.8	192.168.2.4	0xa848	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:03.173120022 CEST	8.8.8.8	192.168.2.4	0xa848	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.306370020 CEST	8.8.8.8	192.168.2.4	0xa598	No error (0)	s.osano.com		52.45.97.212	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.306370020 CEST	8.8.8.8	192.168.2.4	0xa598	No error (0)	s.osano.com		18.211.217.166	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.421263933 CEST	8.8.8.8	192.168.2.4	0x1b84	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:03.421263933 CEST	8.8.8.8	192.168.2.4	0x1b84	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.421295881 CEST	8.8.8.8	192.168.2.4	0x9b5d	No error (0)	fresnel.vimeocdn.com		34.120.202.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:03.422707081 CEST	8.8.8.8	192.168.2.4	0xc3e	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:03.422707081 CEST	8.8.8.8	192.168.2.4	0xc3e	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:05.008614063 CEST	8.8.8.8	192.168.2.4	0x9794	No error (0)	vimeo.com		151.101.192.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:05.008614063 CEST	8.8.8.8	192.168.2.4	0x9794	No error (0)	vimeo.com		151.101.128.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:05.008614063 CEST	8.8.8.8	192.168.2.4	0x9794	No error (0)	vimeo.com		151.101.0.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:05.008614063 CEST	8.8.8.8	192.168.2.4	0x9794	No error (0)	vimeo.com		151.101.64.217	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:06.425826073 CEST	8.8.8.8	192.168.2.4	0x5f1b	No error (0)	www.cookiesandyou.com		143.204.98.44	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:06.425826073 CEST	8.8.8.8	192.168.2.4	0x5f1b	No error (0)	www.cookiesandyou.com		143.204.98.37	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:06.425826073 CEST	8.8.8.8	192.168.2.4	0x5f1b	No error (0)	www.cookiesandyou.com		143.204.98.51	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:06.425826073 CEST	8.8.8.8	192.168.2.4	0x5f1b	No error (0)	www.cookiesandyou.com		143.204.98.89	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:08.811166048 CEST	8.8.8.8	192.168.2.4	0xcdc3	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:08.811166048 CEST	8.8.8.8	192.168.2.4	0xcdc3	No error (0)	star-mini.c10r.facebook.com		157.240.196.35	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:14.570859909 CEST	8.8.8.8	192.168.2.4	0x2a54	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:16.114531994 CEST	8.8.8.8	192.168.2.4	0xc0bb	No error (0)	use.fontawesome.com	use.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:23.990197897 CEST	8.8.8.8	192.168.2.4	0x8573	No error (0)	li.sten.to		104.26.0.226	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:23.990197897 CEST	8.8.8.8	192.168.2.4	0x8573	No error (0)	li.sten.to		172.67.75.199	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:23.990197897 CEST	8.8.8.8	192.168.2.4	0x8573	No error (0)	li.sten.to		104.26.1.226	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.734525919 CEST	8.8.8.8	192.168.2.4	0xc8ec	No error (0)	static.cloudflareinsights.com		104.16.94.65	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.734525919 CEST	8.8.8.8	192.168.2.4	0xc8ec	No error (0)	static.cloudflareinsights.com		104.16.95.65	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.740130901 CEST	8.8.8.8	192.168.2.4	0xcb72	No error (0)	client.crisp.chat		104.18.28.91	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:24.740130901 CEST	8.8.8.8	192.168.2.4	0xcb72	No error (0)	client.crisp.chat		104.18.29.91	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:25.348050117 CEST	8.8.8.8	192.168.2.4	0x4c24	No error (0)	client.relay.crisp.chat		134.209.238.18	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:25.348050117 CEST	8.8.8.8	192.168.2.4	0x4c24	No error (0)	client.relay.crisp.chat		64.227.36.222	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:26.700381994 CEST	8.8.8.8	192.168.2.4	0x6c18	No error (0)	li.sten.to		104.26.0.226	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:26.700381994 CEST	8.8.8.8	192.168.2.4	0x6c18	No error (0)	li.sten.to		172.67.75.199	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:26.700381994 CEST	8.8.8.8	192.168.2.4	0x6c18	No error (0)	li.sten.to		104.26.1.226	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.297507048 CEST	8.8.8.8	192.168.2.4	0xac58	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.297507048 CEST	8.8.8.8	192.168.2.4	0xac58	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.326894999 CEST	8.8.8.8	192.168.2.4	0xb952	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.326894999 CEST	8.8.8.8	192.168.2.4	0xb952	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.326894999 CEST	8.8.8.8	192.168.2.4	0xb952	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.326894999 CEST	8.8.8.8	192.168.2.4	0xb952	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.326894999 CEST	8.8.8.8	192.168.2.4	0xb952	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.351983070 CEST	8.8.8.8	192.168.2.4	0xa057	No error (0)	linksplit.io		172.67.129.190	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:28.351983070 CEST	8.8.8.8	192.168.2.4	0xa057	No error (0)	linksplit.io		104.21.2.221	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:30.617511034 CEST	8.8.8.8	192.168.2.4	0x738d	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:40.385201931 CEST	8.8.8.8	192.168.2.4	0xebda	No error (0)	www.cookiesandyou.com		143.204.98.44	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.385201931 CEST	8.8.8.8	192.168.2.4	0xebda	No error (0)	www.cookiesandyou.com		143.204.98.37	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.385201931 CEST	8.8.8.8	192.168.2.4	0xebda	No error (0)	www.cookiesandyou.com		143.204.98.51	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.385201931 CEST	8.8.8.8	192.168.2.4	0xebda	No error (0)	www.cookiesandyou.com		143.204.98.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:40.717963934 CEST	8.8.8.8	192.168.2.4	0xe410	No error (0)	fresnel.vimeocdn.com		34.120.202.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.718677998 CEST	8.8.8.8	192.168.2.4	0x26de	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:40.718677998 CEST	8.8.8.8	192.168.2.4	0x26de	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:40.720352888 CEST	8.8.8.8	192.168.2.4	0x9f36	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:40.720352888 CEST	8.8.8.8	192.168.2.4	0x9f36	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:46.256006002 CEST	8.8.8.8	192.168.2.4	0x212f	No error (0)	www.osano.com	4785246.group46.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:46.256006002 CEST	8.8.8.8	192.168.2.4	0x212f	No error (0)	4785246.group46.sites.hubspot.net	group46.sites.hscoscdn40.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:46.256006002 CEST	8.8.8.8	192.168.2.4	0x212f	No error (0)	group46.sites.hscoscdn40.net		199.60.103.228	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:46.256006002 CEST	8.8.8.8	192.168.2.4	0x212f	No error (0)	group46.sites.hscoscdn40.net		199.60.103.28	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.345931053 CEST	8.8.8.8	192.168.2.4	0xf7fa	No error (0)	cmp.osano.com	d2gt2ux04o03l1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:48.345931053 CEST	8.8.8.8	192.168.2.4	0xf7fa	No error (0)	d2gt2ux04o03l1.cloudfront.net		143.204.98.25	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.345931053 CEST	8.8.8.8	192.168.2.4	0xf7fa	No error (0)	d2gt2ux04o03l1.cloudfront.net		143.204.98.90	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.345931053 CEST	8.8.8.8	192.168.2.4	0xf7fa	No error (0)	d2gt2ux04o03l1.cloudfront.net		143.204.98.114	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.345931053 CEST	8.8.8.8	192.168.2.4	0xf7fa	No error (0)	d2gt2ux04o03l1.cloudfront.net		143.204.98.20	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.347286940 CEST	8.8.8.8	192.168.2.4	0x4b3a	No error (0)	cdn.osano.com	4785246.group46.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:48.347286940 CEST	8.8.8.8	192.168.2.4	0x4b3a	No error (0)	4785246.group46.sites.hubspot.net	group46.sites.hscoscdn40.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:48.347286940 CEST	8.8.8.8	192.168.2.4	0x4b3a	No error (0)	group46.sites.hscoscdn40.net		199.60.103.28	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.347286940 CEST	8.8.8.8	192.168.2.4	0x4b3a	No error (0)	group46.sites.hscoscdn40.net		199.60.103.228	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.618529081 CEST	8.8.8.8	192.168.2.4	0xe3df	No error (0)	no-cache.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:48.618529081 CEST	8.8.8.8	192.168.2.4	0xe3df	No error (0)	no-cache.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:49.976234913 CEST	8.8.8.8	192.168.2.4	0xde58	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:50.643884897 CEST	8.8.8.8	192.168.2.4	0xcc4c	No error (0)	consent.api.osano.com		143.204.98.90	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:50.643884897 CEST	8.8.8.8	192.168.2.4	0xcc4c	No error (0)	consent.api.osano.com		143.204.98.19	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:50.643884897 CEST	8.8.8.8	192.168.2.4	0xcc4c	No error (0)	consent.api.osano.com		143.204.98.120	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:50.643884897 CEST	8.8.8.8	192.168.2.4	0xcc4c	No error (0)	consent.api.osano.com		143.204.98.79	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.398308039 CEST	8.8.8.8	192.168.2.4	0x87b4	No error (0)	js.hsleadflows.net		104.17.234.204	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:51.398308039 CEST	8.8.8.8	192.168.2.4	0x87b4	No error (0)	js.hsleadflows.net		104.17.232.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.398308039 CEST	8.8.8.8	192.168.2.4	0x87b4	No error (0)	js.hsleadflows.net		104.17.233.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.398308039 CEST	8.8.8.8	192.168.2.4	0x87b4	No error (0)	js.hsleadflows.net		104.17.231.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.398308039 CEST	8.8.8.8	192.168.2.4	0x87b4	No error (0)	js.hsleadflows.net		104.17.230.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.574934006 CEST	8.8.8.8	192.168.2.4	0xdc0	No error (0)	app.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.574934006 CEST	8.8.8.8	192.168.2.4	0xdc0	No error (0)	app.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.687294960 CEST	8.8.8.8	192.168.2.4	0xde2a	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:51.687294960 CEST	8.8.8.8	192.168.2.4	0xde2a	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:51.687294960 CEST	8.8.8.8	192.168.2.4	0xde2a	No error (0)	glb-na.mix.linkedin.com	pop-eda6.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:51.687294960 CEST	8.8.8.8	192.168.2.4	0xde2a	No error (0)	pop-eda6.mix.linkedin.com		108.174.11.69	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.804745913 CEST	8.8.8.8	192.168.2.4	0x4203	No error (0)	js.usemessages.com		104.17.235.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.804745913 CEST	8.8.8.8	192.168.2.4	0x4203	No error (0)	js.usemessages.com		104.17.237.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.804745913 CEST	8.8.8.8	192.168.2.4	0x4203	No error (0)	js.usemessages.com		104.17.239.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.804745913 CEST	8.8.8.8	192.168.2.4	0x4203	No error (0)	js.usemessages.com		104.17.238.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.804745913 CEST	8.8.8.8	192.168.2.4	0x4203	No error (0)	js.usemessages.com		104.17.236.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.812789917 CEST	8.8.8.8	192.168.2.4	0xd062	No error (0)	js.hubspotfeedback.com		104.17.113.162	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.812789917 CEST	8.8.8.8	192.168.2.4	0xd062	No error (0)	js.hubspotfeedback.com		104.17.112.162	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.812789917 CEST	8.8.8.8	192.168.2.4	0xd062	No error (0)	js.hubspotfeedback.com		104.17.116.162	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.812789917 CEST	8.8.8.8	192.168.2.4	0xd062	No error (0)	js.hubspotfeedback.com		104.17.114.162	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.812789917 CEST	8.8.8.8	192.168.2.4	0xd062	No error (0)	js.hubspotfeedback.com		104.17.115.162	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.815896988 CEST	8.8.8.8	192.168.2.4	0xf693	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.815896988 CEST	8.8.8.8	192.168.2.4	0xf693	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.815896988 CEST	8.8.8.8	192.168.2.4	0xf693	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.815896988 CEST	8.8.8.8	192.168.2.4	0xf693	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.815896988 CEST	8.8.8.8	192.168.2.4	0xf693	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:51.839206934 CEST	8.8.8.8	192.168.2.4	0xa182	No error (0)	js.hs-banner.com		104.18.20.191	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:51.839206934 CEST	8.8.8.8	192.168.2.4	0xa182	No error (0)	js.hs-banner.com		104.18.21.191	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.202766895 CEST	8.8.8.8	192.168.2.4	0x844e	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:52.301661015 CEST	8.8.8.8	192.168.2.4	0x9f1e	No error (0)	googleads.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.444053888 CEST	8.8.8.8	192.168.2.4	0x3978	No error (0)	www.google.ch		172.217.168.3	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.853264093 CEST	8.8.8.8	192.168.2.4	0xa6b6	No error (0)	perf.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.853264093 CEST	8.8.8.8	192.168.2.4	0xa6b6	No error (0)	perf.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.853264093 CEST	8.8.8.8	192.168.2.4	0xa6b6	No error (0)	perf.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.853264093 CEST	8.8.8.8	192.168.2.4	0xa6b6	No error (0)	perf.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.853264093 CEST	8.8.8.8	192.168.2.4	0xa6b6	No error (0)	perf.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.854119062 CEST	8.8.8.8	192.168.2.4	0x2d4d	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.854119062 CEST	8.8.8.8	192.168.2.4	0x2d4d	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.855981112 CEST	8.8.8.8	192.168.2.4	0x7906	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:52.855981112 CEST	8.8.8.8	192.168.2.4	0x7906	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.044730902 CEST	8.8.8.8	192.168.2.4	0x80ae	No error (0)	static.hsappstatic.net		104.17.9.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.044730902 CEST	8.8.8.8	192.168.2.4	0x80ae	No error (0)	static.hsappstatic.net		104.17.8.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.044730902 CEST	8.8.8.8	192.168.2.4	0x80ae	No error (0)	static.hsappstatic.net		104.17.6.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.044730902 CEST	8.8.8.8	192.168.2.4	0x80ae	No error (0)	static.hsappstatic.net		104.17.7.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:53.044730902 CEST	8.8.8.8	192.168.2.4	0x80ae	No error (0)	static.hsappstatic.net		104.17.5.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.062241077 CEST	8.8.8.8	192.168.2.4	0xc530	No error (0)	api.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.062241077 CEST	8.8.8.8	192.168.2.4	0xc530	No error (0)	api.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.507961988 CEST	8.8.8.8	192.168.2.4	0x7935	No error (0)	feedback.hubapi.com		104.17.202.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.507961988 CEST	8.8.8.8	192.168.2.4	0x7935	No error (0)	feedback.hubapi.com		104.17.201.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.507961988 CEST	8.8.8.8	192.168.2.4	0x7935	No error (0)	feedback.hubapi.com		104.17.203.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.507961988 CEST	8.8.8.8	192.168.2.4	0x7935	No error (0)	feedback.hubapi.com		104.17.200.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.507961988 CEST	8.8.8.8	192.168.2.4	0x7935	No error (0)	feedback.hubapi.com		104.17.204.204	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:54.760296106 CEST	8.8.8.8	192.168.2.4	0xb5af	No error (0)	f.hubspotusercontent40.net		104.16.183.114	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 13, 2021 20:51:54.760296106 CEST	8.8.8.8	192.168.2.4	0xb5af	No error (0)	f.hubspotusercontent40.net		104.16.182.114	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.138643026 CEST	8.8.8.8	192.168.2.4	0x45b3	No error (0)	www.osano.com	4785246.group46.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:57.138643026 CEST	8.8.8.8	192.168.2.4	0x45b3	No error (0)	4785246.group46.sites.hubspot.net	group46.sites.hscoscdn40.net		CNAME (Canonical name)	IN (0x0001)
Jul 13, 2021 20:51:57.138643026 CEST	8.8.8.8	192.168.2.4	0x45b3	No error (0)	group46.sites.hscoscdn40.net		199.60.103.228	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.138643026 CEST	8.8.8.8	192.168.2.4	0x45b3	No error (0)	group46.sites.hscoscdn40.net		199.60.103.28	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.165144920 CEST	8.8.8.8	192.168.2.4	0x5cfe	No error (0)	no-cache.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:57.165144920 CEST	8.8.8.8	192.168.2.4	0x5cfe	No error (0)	no-cache.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.110450983 CEST	8.8.8.8	192.168.2.4	0x3249	No error (0)	static.hsappstatic.net		104.17.9.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.110450983 CEST	8.8.8.8	192.168.2.4	0x3249	No error (0)	static.hsappstatic.net		104.17.8.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.110450983 CEST	8.8.8.8	192.168.2.4	0x3249	No error (0)	static.hsappstatic.net		104.17.6.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.110450983 CEST	8.8.8.8	192.168.2.4	0x3249	No error (0)	static.hsappstatic.net		104.17.5.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:58.110450983 CEST	8.8.8.8	192.168.2.4	0x3249	No error (0)	static.hsappstatic.net		104.17.7.210	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:59.166023016 CEST	8.8.8.8	192.168.2.4	0x7b09	No error (0)	f.hubspotusercontent40.net		104.16.182.114	A (IP address)	IN (0x0001)
Jul 13, 2021 20:51:59.166023016 CEST	8.8.8.8	192.168.2.4	0x7b09	No error (0)	f.hubspotusercontent40.net		104.16.183.114	A (IP address)	IN (0x0001)
Jul 13, 2021 20:52:21.026907921 CEST	8.8.8.8	192.168.2.4	0x8b43	No error (0)	tattle.api.osano.com		107.20.89.168	A (IP address)	IN (0x0001)
Jul 13, 2021 20:52:21.026907921 CEST	8.8.8.8	192.168.2.4	0x8b43	No error (0)	tattle.api.osano.com		54.156.254.108	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 13, 2021 20:50:55.353518963 CEST	151.101.2.217	443	192.168.2.4	49754	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021 Tue Jul 28 02:00:00 CEST 2020	Sat Mar 26 20:39:57 CET 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.084798098 CEST	151.101.0.217	443	192.168.2.4	49786	CN=*.vimeo.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 21 06:17:14 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Wed Jun 22 06:17:13 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.534867048 CEST	52.45.97.212	443	192.168.2.4	49788	CN=*.osano.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	Sun Nov 08 01:00:00 CET 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	Wed Dec 08 00:59:59 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	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=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 13, 2021 20:51:03.555737019 CEST	151.101.114.109	443	192.168.2.4	49789	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.556387901 CEST	151.101.114.109	443	192.168.2.4	49791	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.558207035 CEST	151.101.114.109	443	192.168.2.4	49790	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.562154055 CEST	151.101.114.109	443	192.168.2.4	49792	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.562226057 CEST	151.101.114.109	443	192.168.2.4	49795	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:03.562721014 CEST	151.101.114.109	443	192.168.2.4	49794	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:05.044151068 CEST	151.101.192.217	443	192.168.2.4	49797	CN=*.vimeo.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 21 06:17:14 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Wed Jun 22 06:17:13 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 13, 2021 20:51:06.466393948 CEST	143.204.98.44	443	192.168.2.4	49805	CN=*.cookiesandyou.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	Fri Mar 19 01:00:00 CET 2021	Mon Apr 18 01:59:59 CEST 2022	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 13, 2021 20:51:06.473649979 CEST	143.204.98.44	443	192.168.2.4	49804	CN=*.cookiesandyou.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	Fri Mar 19 01:00:00 CET 2021	Mon Apr 18 01:59:59 CEST 2022	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 13, 2021 20:51:11.943902969 CEST	151.101.2.217	443	192.168.2.4	49830	CN=*.sentry-cdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Mon Feb 22 20:39:57 CET 2021	Sat Mar 26 20:39:57 CET 2022	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
							Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:25.750581026 CEST	134.209.238.18	443	192.168.2.4	49921	CN=client.relay.crisp.chat CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jun 03 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Jul 05 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=Sectigo ECC Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 13, 2021 20:51:26.738785982 CEST	104.26.0.226	443	192.168.2.4	49929	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jun 11 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jun 11 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:26.739141941 CEST	104.26.0.226	443	192.168.2.4	49930	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jun 11 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jun 11 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:40.780204058 CEST	151.101.114.109	443	192.168.2.4	49978	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:40.782295942 CEST	151.101.114.109	443	192.168.2.4	49979	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	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=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 13, 2021 20:51:51.426969051 CEST	104.17.234.204	443	192.168.2.4	50021	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jul 07 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Jul 07 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:51.835032940 CEST	104.17.235.204	443	192.168.2.4	50023	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jul 13 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jul 13 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:51.842128038 CEST	104.17.113.162	443	192.168.2.4	50024	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jul 06 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Wed Jul 06 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:51.850189924 CEST	104.17.70.176	443	192.168.2.4	50025	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Aug 14 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sat Aug 14 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 13, 2021 20:51:51.960445881 CEST	108.174.11.69	443	192.168.2.4	50022	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	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=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jul 13, 2021 20:51:57.182988882 CEST	199.60.103.228	443	192.168.2.4	50058	CN=www.osano.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jun 18 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jun 18 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:57.183274031 CEST	199.60.103.228	443	192.168.2.4	50059	CN=www.osano.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jun 18 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jun 18 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:57.193919897 CEST	104.19.155.83	443	192.168.2.4	50060	CN=hubspot.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sat Jun 26 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sun Jun 26 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 13, 2021 20:51:58.138087034 CEST	104.17.9.210	443	192.168.2.4	50076	CN=hsappstatic.net, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jun 10 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Fri Jun 10 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6448 Parent PID: 5008

General

Start time:	20:50:48
Start date:	13/07/2021
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://linksplit.io/'
Imagebase:	0x7ff609c80000
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

Key Value Modified

Analysis Process: chrome.exe PID: 6696 Parent PID: 6448

General

Start time:	20:50:50
Start date:	13/07/2021
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=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff609c80000
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: 6188 Parent PID: 6448

General

Start time:	20:51:31
Start date:	13/07/2021
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=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=7588 /prefetch:8
Imagebase:	0x7ff609c80000
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: 5484 Parent PID: 6448

General

Start time:	20:51:32
Start date:	13/07/2021
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=1572,11679005891178451375,4562770034682752523,131072 --lang=en-GB --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=7336 /prefetch:8
Imagebase:	0x7ff609c80000
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