ID: 800796
Cookbook: browseurl.jbs
Time: 19:56:27
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

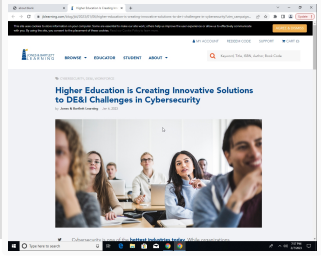
Windows Analysis Report

https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM..

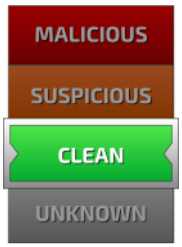
Overview

General Information

Sample URL:	https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CM...9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k
Analysis ID:	800796
Infos:	



Detection

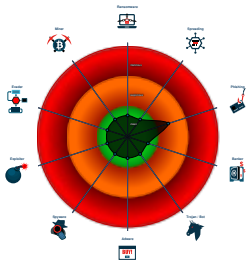


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found iframes
- No HTML title found
- Form action URLs do not match ma…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5484 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5308 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1812 --field-trial-handle=1848,i,2574996844283921396,7295772534104560468,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4720 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

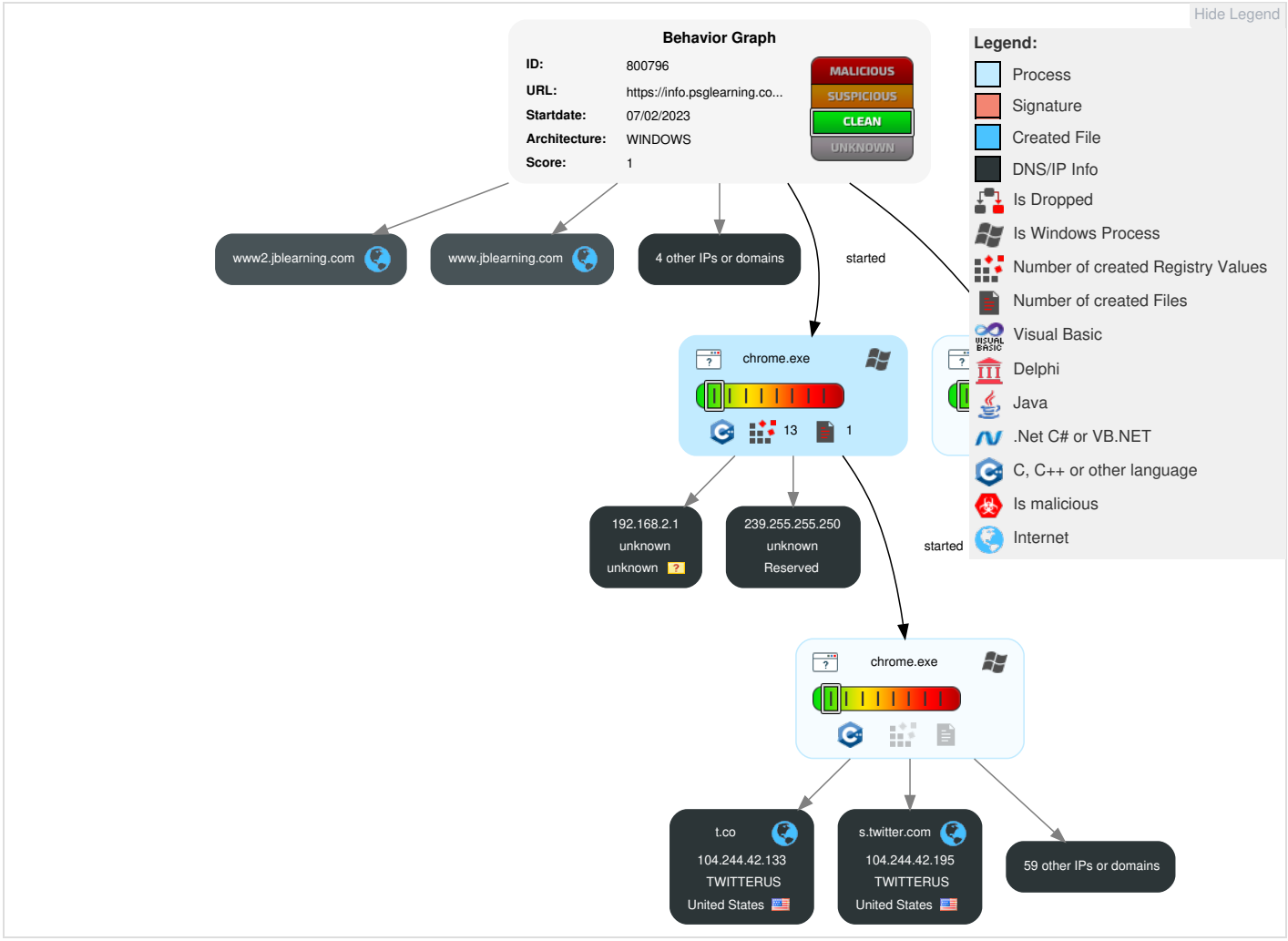
Joe Sandbox Signatures

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	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

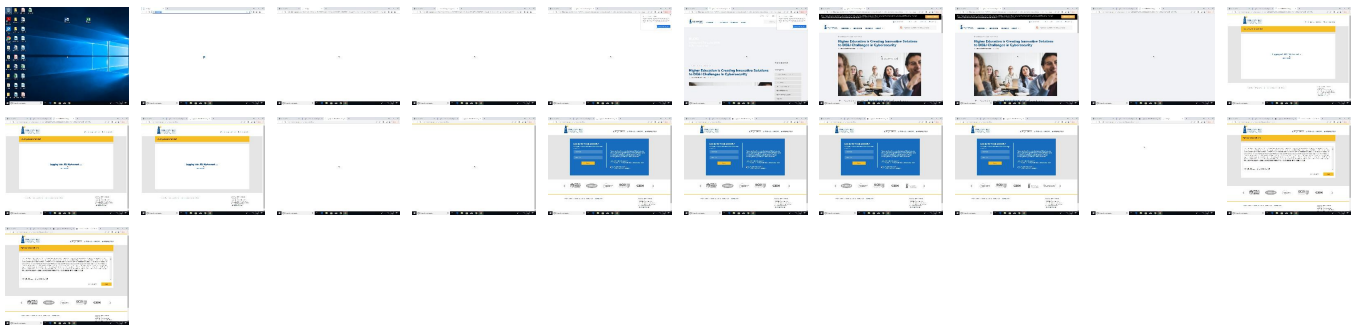
Behavior Graph



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://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1	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.hsleadflows.net/leadflows.js	0%	URL Reputation	safe	
http://https://js.hsadspixel.net/fb.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://bam.nr-data.net/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVANXUANVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=16220&ck=1&ref=https://www2.jblearning.com/my-account/login&ap=69&be=3266&fe=15885&dc=14321&tt=A0F3543576409569&af=err,xhr,stn,ins&perf=%7B%22timing%22:%7B%22of%22:1675828693636,%22n%22:0,%22f%22:2598,%22dn%22:2779,%22dne%22:2779,%22c%22:2779,%22s%22:2780,%22ce%22:2883,%22rq%22:2883,%22rp%22:3144,%22rpe%22:3263,%22dl%22:3199,%22di%22:14319,%22ds%22:14321,%22de%22:14325,%22dc%22:15885,%22l%22:15885,%22le%22:15907%7D,%22navigation%22:%7B%7D%7D&fp=5082&fcp=14074&jsonp=NREUM.setToken	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-HPKNEKFDEN&cid=2012528678.1675828662>m=45je3260&aip=1&z=1102161816	0%	Avira URL Cloud	safe	
http://https://bam.nr-data.net/resources/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVANXUANVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=44429&ck=1&ref=https://www2.jblearning.com/my-account/login&ptid=d76a3ef8-0001-bde3-fa24-01862d3e72d3&st=1675828693636	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/pagead/1p-user-list/670254787/?random=1675828659401&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45He3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSI4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&fmt=3&is_vtc=1&random=22329945&rmt_tld=1&ipr=y	0%	Avira URL Cloud	safe	
http://https://bam.nr-data.net/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVFVSAgNVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=9061&ck=1&ref=https://www2.jblearning.com/my-account/terms-and-conditions&ap=55&be=6530&fe=8954&dc=7557&tt=3E5AF455BAD710BE&af=err,xhr,stn,ins&perf=%7B%22timing%22:%7B%22of%22:1675828719328,%22n%22:0,%22f%22:4,%22dn%22:37,%22dne%22:37,%22c%22:37,%22s%22:57,%22ce%22:110,%22rq%22:110,%22rp%22:734,%22rpe%22:6620,%22dl%22:4195,%22di%22:7557,%22ds%22:7557,%22de%22:7558,%22dc%22:8954,%22l%22:8954,%22le%22:8985%7D,%22navigation%22:%7B%7D%7D&fp=6949&fcp=7222&jsonp=NREUM.setToken	0%	Avira URL Cloud	safe	
http://https://fast.fonts.net/t/1.css?apiType=css&projectid=0a5a817c-07a1-4284-91cc-2e5a8d413223	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/pagead/1p-user-list/924662483/?random=1675828674266&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45be3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSI4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&data=event%3Dgtag.config&fmt=3&is_vtc=1&random=2670459441&rmt_tld=1&ipr=y	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-1846188-1&cid=2012528678.1675828662&jid=1434085864&_u=YCDACEABRAAAACAEKC~&z=457024448	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=GTM-P88GWCP	0%	Avira URL Cloud	safe	
http://https://info.psglearning.com/events/public/v1/encoded/track/tc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1?_ud=1bdd180c-2306-4546-b89c-755fff0e547e&_jss=1&_fl=8&_pl=0&_hc=4&_lg=en-US,en&_plt=Win32&_scr=1280,1024	0%	Avira URL Cloud	safe	
http://https://forms.hsforms.com/embed/v3/form/2491413/7b653472-411f-4d9c-afb8-9126eab8d8de/json?hs_static_app=forms-embed&hs_static_app_version=1.2642&X-HubSpot-Static-App-Info=forms-embed-1.2642	0%	Avira URL Cloud	safe	
http://https://perf-na1.hsforms.com/embed/v3/counters.gif?key=config-loaded-success&value=1	0%	Avira URL Cloud	safe	
http://https://forms.hsforms.com/embed/v3/counters.gif?key=forms-embed-v2-DEFINITION_SUCCESS&count=1	0%	Avira URL Cloud	safe	
http://https://forms-na1.hsforms.com/embed/v3/counters.gif?key=forms-embed-v2-RENDER_SUCCESS&count=1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
forms.hsforms.com	104.16.89.5	true	false		unknown
fastly-tls12-bam.nr-data.net	162.247.243.29	true	false		unknown
forms.hubspot.com	104.19.155.83	true	false		high
cta-service-cms2.hubspot.com	104.19.154.83	true	false		high
js.hs-analytics.net	104.17.71.176	true	false		unknown
platform.twitter.map.fastly.net	146.75.120.157	true	false		unknown
stats.g.doubleclick.net	142.251.31.157	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
d2oh4tlt9mrke9.cloudfront.net	13.224.98.228	true	false		high
t.co	104.244.42.133	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
js.hsforms.net	104.17.182.73	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
js.hs-scripts.com	104.17.213.204	true	false		high
group13.sites.hscoscdn10.net	199.60.103.225	true	false		unknown
www.google.com	142.250.180.132	true	false		high
js.hs-banner.com	172.64.154.85	true	false		unknown
star-mini.c10r.facebook.com	157.240.253.35	true	false		high
accounts.google.com	216.58.209.45	true	false		high
s.twitter.com	104.244.42.195	true	false		high
js.hubspot.com	104.19.154.83	true	false		high
js.hsadspixel.net	104.17.112.176	true	false		unknown
region1.analytics.google.com	216.239.34.36	true	false		high
cdn.gbqofs.com	104.18.25.13	true	false		unknown
auth.jblearning.com	104.16.13.69	true	false		high
www.googleoptimize.com	142.250.180.174	true	false		unknown
recording-elb-2-1543527570.us-east-1.elb.amazonaws.com	18.233.129.81	true	false		high
js.hsleadflows.net	104.17.233.204	true	false		unknown
youtube-ui.l.google.com	142.250.184.78	true	false		high
googleads.g.doubleclick.net	142.250.184.98	true	false		high
forms-na1.hsforms.com	104.16.86.5	true	false		unknown
fast.fonts.net	104.17.225.78	true	false		unknown
d1ni990a184w7d.cloudfront.net	13.224.103.3	true	false		high
api.hubapi.com	104.17.201.204	true	false		high
www.google.co.uk	142.251.209.3	true	false		unknown
tags.srv.stackadapt.com	34.196.141.135	true	false		high
clients.l.google.com	142.250.180.174	true	false		high
perf-na1.hsforms.com	104.16.89.5	true	false		unknown
www2.jblearning.com	104.16.13.69	true	false		high
www.jblearning.com	104.16.13.69	true	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.linkedin.oribi.io	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
ws.sessioncam.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
bam.nr-data.net	unknown	unknown	false		unknown
analytics.twitter.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
snap.licdn.com	unknown	unknown	false		high
info.psglearning.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/Images/icon-questionmark.png	false		high
http://https://bam.nr-data.net/resources/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVANXUANVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=44429&ck=1&ref=https://www2.jblearning.com/my-account/login&ptid=d76a3ef8-0001-bde3-fa24-01862d3e72d3&st=1675828693636	false	• Avira URL Cloud: safe	unknown
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/global/font-awesome.min.css?v=637764826420000000	false		high
http://https://www.jblearning.com/images/default-source/logos/footer-logo.png	false		high
http://https://www2.jblearning.com/images/default-source/icons/fa-chevron-right.png	false		high
http://https://www.jblearning.com/Frontend-Assembly/Telerik.Sitefinity.Frontend.Search/Mvc/Scripts/SearchBox/Search-box.min.js?package=Main&v=MTMuMy43NjM5LjA%3d	false		high
http://https://www2.jblearning.com/images/default-source/logos/bkg/cara-tarascon-bkg.png	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/Styles/ui-lightness/jquery-ui-1.11.0.min.css	false		high
http://https://bam.nr-data.net/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVANXUANVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=16220&ck=1&ref=https://www2.jblearning.com/my-account/login&ap=69&be=3266&fe=15885&dc=14321&tt=A0F3543576409569&af=err,xhr,stn,ins&perf=%7B%22timing%22:%7B%22of%22:1675828693636,%22n%22:0,%22f%22:2598,%22dn%22:2779,%22dne%22:2779,%22c%22:2779,%22s%22:2780,%22ce%22:2883,%22rq%22:2883,%22rp%22:3144,%22rpe%22:3263,%22dl%22:3199,%22di%22:14319,%22ds%22:14321,%22de%22:14325,%22dc%22:15885,%22l%22:15885,%22le%22:15907%7D,%22navigation%22:%7B%7D%7D&fp=5082&fcp=14074&jsonp=NREUM.setToken	false	• Avira URL Cloud: safe	unknown
http://https://www.jblearning.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/Images/favicon.ico	false		high
http://https://ws.sessioncam.com/Record/config.aspx?url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&jsver=596&originalUrl=https://www.jblearning.com&sse=1675828667387&inTg=a&acr=0	false		high
http://https://js.hsleadflows.net/leadflows.js	false	• URL Reputation: safe	unknown
http://https://www.google.com/pagead/1p-user-list/924662483/?random=1675828708979&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45be3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww2.jblearning.com%2Fmy-account%2Flogin&ref=https%3A%2F%2Fwww2.jblearning.com%2F&tiba=Login%20%7C%20Jones%20%26%20Bartlett%20Learning&data=event%3Dgtag.config&fmt=3&is_vtc=1&random=2786660044&rmt_tld=0&ipr=y	false		high
http://https://www.jblearning.com/Frontend-Assembly/Ascend.CookieBanner/MVC/Scripts/CookieBanner/cookiebanner.js?package=Main&v=Mi4yNS4wLjA%3d	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/angular-sanitize/1.8.2/angular-sanitize.min.js	false		high
http://https://www.google.com/pagead/1p-user-list/924662483/?random=1675828674266&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45be3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&data=event%3Dgtag.config&fmt=3&is_vtc=1&random=2670459441&rmt_tld=0&ipr=y	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/assets/avenirwebfont/c4352a95-7a41-48c1-83ce-d8ffd2a3b118.woff	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/images/default-source/icons/fa-wrench.png	false		high

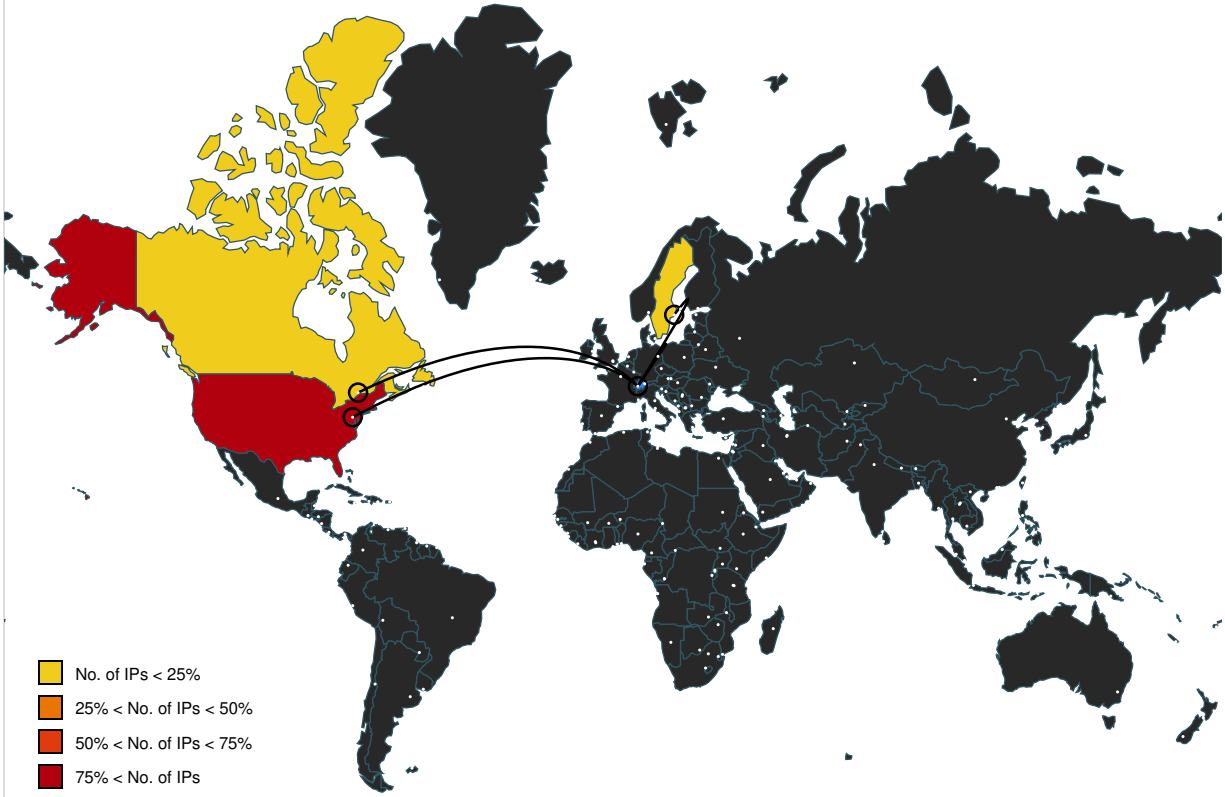
Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.co.uk/pagead/1p-user-list/670254787/?random=1675828659401&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45He3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&fmt=3&is_vtc=1&random=22329945&rmt_tld=1&ipr=y	false	• Avira URL Cloud: safe	unknown
http://https://www2.jblearning.com/ResourcePackages/Bootstrap4/assets/dist/js/popper.min.js	false		high
http://https://www.youtube.com/iframe_api	false		high
http://https://www2.jblearning.com/api/jbl/login/validatesession	false		high
http://https://www.jblearning.com/ResourcePackages/Main/assets/fonts/Avenir/Avenir-Light.woff	false		high
http://https://www2.jblearning.com/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=ctl07_TSM&compress=0&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3aen%3a9ddf364d-d65d-4f01-a69e-8b015049e026%3aea597d4b%3ab25378d2	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-1846188-1&cid=2012528678.1675828662&jid=1434085864&gjid=1354173061&_gid=156726841.1675828666&_u=YCDACEABRAAAACAEKC~&z=343653667	false		high
http://https://bam.nr-data.net/1/f7f7db9847?a=9225788&v=1216.487a282&to=ZwQGZERSV0RVBhAMCV5OJWNmHEpRRAQDABVVExJZVVYWVFVSAgNVBFlJBldVWBoCUFVUS1JYVlYbVV8HBFVUVVUIWFACaV5YXlpLBRYWSA%3D%3D&rst=9061&ck=1&ref=https://www2.jblearning.com/my-account/terms-and-conditions&ap=55&be=6530&fe=8954&dc=7557&tt=3E5AF455BAD710BE&af=err,xhr,stn,ins&perf=%7B%22timing%22:%7B%22of%22:1675828719328,%22n%22:0,%22f%22:4,%22dn%22:37,%22dne%22:37,%22c%22:37,%22s%22:57,%22ce%22:110,%22rq%22:110,%22rp%22:734,%22rpe%22:6620,%22dl%22:4195,%22di%22:7557,%22ds%22:7557,%22de%22:7558,%22dc%22:8954,%22l%22:8954,%22le%22:8985%7D,%22navigation%22:%7B%7D%7D&fp=6949&fcp=7222&jsonp=NREUM.setToken	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/en_US/fbevents.js	false		high
http://https://www.google.com/pagead/1p-user-list/670254787/?random=1675828659401&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45He3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&fmt=3&is_vtc=1&random=22329945&rmt_tld=0&ipr=y	false		high
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-HPKNEKFDEN&cid=2012528678.1675828662>m=45je3260&aip=1&z=1102161816	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/97ea7458/www-widgetapi.vflset/www-widgetapi.js	false		high
http://https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1	false		unknown
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/jquery.validator.min.js	false		high
http://https://track.hubspot.com/__ptq.gif?k=1&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=2241477399&v=1.1&a=2491413&rcu=https%3A%2F%2Fwww2.jblearning.com%2F&r=https%3A%2F%2Fwww2.jblearning.com%2F&pu=https%3A%2F%2Fwww2.jblearning.com%2Fmy-account%2Flogin&t=Login+%7C+Jones+%26+Bartlett+Learning&cts=1675828709533&vi=9fe9da005605a410d9b45a8b68cabfca&nc=false&u=254270999.9fe9da005605a410d9b45a8b68cabfca.1675828672791.1675828672791.1675828672791.1&b=254270999.2.1675828672791&cc=15	false		high
http://https://cta-service-cms2.hubspot.com/web-interactives/public/v1//embed/configs?portalId=2491413&previewScheduled=null&isPreview=false¤tUrl=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email	false		high
http://https://www2.jblearning.com/my-account/login	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://forms.hubspot.com/lead-flows-config/v1/config/json?portalId=2491413&utk=9fe9da005605a410d9b45a8b68cabfca&__hstc=254270999.9fe9da005605a410d9b45a8b68cabfca.1675828672791.1675828672791.1675828672791.1&__hssc=254270999.1.1675828672791¤tUrl=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email	false		high
http://https://www2.jblearning.com/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZExrPE5pZbVgfspwJbSs3Ze0qcX_fxujzL1rieFLfimB8A57gHP1bUj2oUyWWmfibcGaSiKy2cOzZ9Hgplrj8LWQBD_br8nhEMRfR9KM5XDC0&t=637814473746327080	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-174575747-1&cid=2012528678.1675828662&jid=1994248400&_u=YCDACEABRAAAACAEKC~&z=1190023695	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/jquery.cookie.js	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-1846188-1&cid=2012528678.1675828662&jid=878366690&gjid=1583693134&_gid=156726841.1675828666&_u=SCCAgEABQAAAAGAEKC~&z=1729408282	false		high
http://https://www.jblearning.com/blog/jbl/2023/01/06/higher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity?utm_campaign=JBL_CS_Cyber_Blog_2023&utm_medium=email&_hsmi=244995107&_hsenc=p2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ&utm_content=244995107&utm_source=hs_email	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/jquery.tablesorter.min.js	false		high
http://https://t.co/i/adsct?bci=3&eci=2&event_id=90e27783-095d-40e5-8206-13e3aaa64098&events=%5B%5B%22pageview%22%2C%7B%7D%5D%5D&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=8176e464-4339-4a04-ba99-a8ea462f1dcc&tw_document_href=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tw_iframe_status=0&tw_order_quantity=0&tw_sale_amount=0&txn_id=o3i8c&type=javascript&version=2.3.29	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/jquery.validator.additional-methods.min.js	false		high
http://https://js.hsforms.net/forms/v2.js	false		high
http://https://fast.fonts.net/t/1.css?apiType=css&projectid=0a5a817c-07a1-4284-91cc-2e5a8d413223	false	• Avira URL Cloud: safe	unknown
http://https://js.hsadspixel.net/fb.js	false	• URL Reputation: safe	unknown
http://https://www2.jblearning.com/cdn-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js	false		high
http://https://www2.jblearning.com/images/default-source/logos/bkg/cara-recert-bkg.png	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&tid=G-767K326XBN&cid=2012528678.1675828662>m=45je3260&aip=1	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-1846188-42&cid=2012528678.1675828662&jid=1936052815&_u=SCCAgEABQAAAAEAEKC~&z=683800814	false		high
http://https://www.jblearning.com/ResourcePackages/Main/assets/css/common.min.css	false		high
http://https://perf-na1.hsforms.com/embed/v3/counters.gif?key=config-loaded-success&value=1	false	• Avira URL Cloud: safe	unknown
http://https://www.jblearning.com/ResourcePackages/Main/assets/fonts/Avenir/Avenir-Black.woff	false		high
http://https://www2.jblearning.com//ualoginresponse.aspx	false		high
http://https://www.jblearning.com/ResourcePackages/Main/assets/src/js/min/main.min.js	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/images/default-source/theme/jones-and-bartlett-logo.gif	false		high
http://https://static.ads-twitter.com/uwt.js	false	• URL Reputation: safe	unknown
http://https://www2.jblearning.com/images/default-source/theme/jones-and-bartlett-logo.gif	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-96584732-5&cid=2012528678.1675828662&jid=707895511&gjid=27736071&_gid=156726841.1675828666&_u=SCCAAEABQAAAAGAEKC~&z=153069381	false		high
http://https://www2.jblearning.com/images/default-source/logos/bkg/cara-cdx-bkg.png	false		high
http://https://forms-na1.hsforms.com/embed/v3/counters.gif?key=forms-embed-v2-RENDER_SUCCESS&count=1	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://track.hubspot.com/__ptq.gif?k=1&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=2241477399&v=1.1&a=2491413&rcu=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity&pu=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&t=Higher+Education+Is+Creating+Innovative+Solutions+To+De+I+Challenges+In+Cybersecurity+-+Higher+Education+is+Creating+Innovative+Solutions+to+DE%26I+Challenges+in+Cybersecurity&cts=1675828672862&vi=9fe9da005605a410d9b45a8b68cabfca&nc=true&u=254270999.9fe9da005605a410d9b45a8b68cabfca.1675828672791.1675828672791.1675828672791.1&b=254270999.1.1675828672791&cc=15	false		high
http://https://d2oh4tlt9mrke9.cloudfront.net/Record/js/sessioncam.recorder.js	false		high
http://https://connect.facebook.net/signals/config/289378774863753?v=2.9.95&r=stable	false		high
http://https://www.google.co.uk/pagead/1p-user-list/924662483/?random=1675828674266&cv=11&fst=1675825200000&bg=ffffff&guid=ON&async=1>m=45be3260&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&tiba=Higher%20Education%20Is%20Creating%20Innovative%20Solutions%20To%20De%20I%20Challenges%20In%20Cybersecurity%20-%20Higher%20Education%20is%20Creating%20Innovative%20Solutions%20to%20DE%26I%20Challenges%20in%20Cybersecurity&data=event%3Dgtag.config&fmt=3&is_vtc=1&random=2670459441&rmt_tld=1&ipr=y	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-96584732-5&cid=2012528678.1675828662&jid=707895511&_u=SCCAAEABQAAAAGAEKC~&z=1304019849	false		high
http://https://js.hubspot.com/web-interactives-embed.js	false		high
http://https://www.jblearning.com/WebResource.axd?d=NjxTqR2bqTw1rewxxlkHPjsxojz0B5I93vdbWX4ld67OJQwsenLtHNQWhpwzXw3u1kf0Lh3guJmYquH8CTUVTqHSNmnRF25g9aloqu60s0xNcuUGhznAyOAr8szeyeMlYQHHo2aetZzyKI1-UlSxDt_jD1jpq1bSK8MNVbYx0BhFpFHdAUzZc7j2oA15lG8rdWPKcS40WXMD8QYqW5c6WZROCu61vgatAJOuuThlZ-A1&t=637824974900000000	false		high
http://https://www2.jblearning.com/images/default-source/logos/bkg/cara-psg-bkg.png	false		high
http://https://www2.jblearning.com/Scripts/UserSession.1.4.js	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/images/default-source/icons/fs-lang1.png	false		high
http://https://www.googleoptimize.com/optimize.js?id=GTM-P88GWCP	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/Images/icon-rt-arrow.png	false		high
http://https://www.jblearning.com/Ascend.Frontend/dist/polyfills.7da9278c3d58fe34.js	false		high
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-1846188-1&cid=2012528678.1675828662&jid=1434085864&_u=YCDACEABRAAAACAEKC~&z=457024448	false	• Avira URL Cloud: safe	unknown
http://https://www2.jblearning.com/Telerik.Web.UI.WebResource.axd?compress=0&_TSM_CombinedScripts_=%3b%3bTelerik.Sitefinity.Resources%2c+Version%3d7.0.5100.0%2c+Culture%3dneutral%2c+PublicKeyToken%3dnull%3aen%3aa6635f48-e22f-44c2-8ae2-67269b80c83c%3a83fa35c7%3a850288ef%3a7a90d6a	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/global/layout.css?v=635768054227285516	false		high
http://https://www.facebook.com/tr/?id=289378774863753&ev=PageView&dl=https%3A%2F%2Fwww.jblearning.com%2Fblog%2Fjbl%2F2023%2F01%2F06%2Fhigher-education-is-creating-innovative-solutions-to-de-i-challenges-in-cybersecurity%3Futm_campaign%3DJBL_CS_Cyber_Blog_2023%26utm_medium%3Demail%26_hsmi%3D244995107%26_hsenc%3Dp2ANqtz-97Mdt0_FwXsW_N9RyEjgbhvetuqPz-lNdAFSl4h2PzRX6W3Ju8VhgTAUxy5BnOCsNrIteSCyMxXYHPKRLHnCVyXBRSwQ%26utm_content%3D244995107%26utm_source%3Dhs_email&rl=&if=false&ts=1675828667599&sw=1280&sh=1024&v=2.9.95&r=stable&ec=0&o=29&cs_est=true&fbp=fb.1.1675828667597.1578228301&it=1675828660308&coo=false&rqm=GET	false		high
http://https://www.jblearning.com/images/default-source/hero-images/jbl-blog-hero.jpg	false		high
http://https://www.jblearning.com/images/default-source/default-album/students_smiling_classroom.png?sfvrsn=b2a761bc_0	false		high
http://https://forms.hsforms.com/embed/v3/counters.gif?key=forms-embed-v2-DEFINITION_SUCCESS&count=1	false	• Avira URL Cloud: safe	unknown
http://https://www2.jblearning.com/my-account/terms-and-conditions	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://info.psglearning.com/events/public/v1/encoded/track/tc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1?_ud=1bdd180c-2306-4546-b89c-755fff0e547e&_jss=1&_fl=8&_pl=0&_hc=4&_lg=en-US,en&_plt=Win32&_scr=1280,1024	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-174575747-2&cid=2012528678.1675828662&jid=688392651&gjid=1392856995&_gid=156726841.1675828666&_u=SCCAiEABRAAAAGAEKC~&z=758368686	false		high
http://https://www.jblearning.com/images/default-source/logos/header-logo.png	false		high
http://https://www.jblearning.com/ResourcePackages/Main/assets/Images/favicon.png	false		high
http://https://js.hs-scripts.com/2491413.js	false		high
http://https://forms.hsforms.com/embed/v3/form/2491413/7b653472-411f-4d9c-afb8-9126eab8d8de/json?hs_static_app=forms-embed&hs_static_app_version=1.2642&X-HubSpot-Static-App-Info=forms-embed-1.2642	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-1846188-42&cid=2012528678.1675828662&jid=1936052815&gjid=921806912&_gid=156726841.1675828666&_u=SCCAgEABQAAAAEAEKC~&z=1764471385	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/images/default-source/icons/fa-tag.png	false		high
http://https://connect.facebook.net/signals/config/1300222089994483?v=2.9.95&r=stable	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/global.9.2.6250.0-2.js	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/JS/jquery-ui-1.11.0.min.js	false		high
http://https://forms.hubspot.com/lead-flows-config/v1/config/json?portalId=2491413&utk=9fe9da005605a410d9b45a8b68cabfca&__hstc=254270999.9fe9da005605a410d9b45a8b68cabfca.1675828672791.1675828672791.1675828672791.1&__hssc=254270999.3.1675828672791¤tUrl=https%3A%2F%2Fwww2.jblearning.com%2Fmy-account%2Fterms-and-conditions	false		high
http://https://www2.jblearning.com/my-account/terms-and-conditions	false		high
http://https://www2.jblearning.com/Sitefinity/WebsiteTemplates/Main/App_Themes/Main/global/Reset.css?v=637764826420000000	false		high
http://https://www2.jblearning.com/images/default-source/icons/fa-tag.png	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.17.225.78	fast.fonts.net	United States		13335	CLOUDFLARENETUS	false
104.17.213.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
142.251.209.3	www.google.co.uk	United States		15169	GOOGLEUS	false
216.58.209.45	accounts.google.com	United States		15169	GOOGLEUS	false
104.18.25.13	cdn.gbqofs.com	United States		13335	CLOUDFLARENETUS	false
142.250.184.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.19.154.83	cta-service-cms2.hubspot.com	United States		13335	CLOUDFLARENETUS	false
142.251.31.157	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
199.60.103.225	group13.sites.hscoscdn10.net	Canada		23181	QUICKSILVER1CA	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.16.86.5	forms-na1.hsforms.com	United States		13335	CLOUDFLARENETUS	false
34.196.141.135	tags.srv.stackadapt.com	United States		14618	AMAZON-AESUS	false
104.17.112.176	js.hsadspixel.net	United States		13335	CLOUDFLARENETUS	false
146.75.120.157	platform.twitter.map.fastly.net	Sweden		30051	SCCGOVUS	false
157.240.253.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
142.250.180.174	www.googleoptimize.com	United States		15169	GOOGLEUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.180.132	www.google.com	United States		15169	GOOGLEUS	false
142.250.184.66	unknown	United States		15169	GOOGLEUS	false
18.233.129.81	recording-elb-2-1543527570.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
104.17.71.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
104.17.210.204	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.13.69	auth.jblearning.com	United States		13335	CLOUDFLARENETUS	false
13.224.103.3	d1ni990a184w7d.cloudfront.net	United States		16509	AMAZON-02US	false
104.17.201.204	api.hubapi.com	United States		13335	CLOUDFLARENETUS	false
104.17.182.73	js.hsforms.net	United States		13335	CLOUDFLARENETUS	false
142.250.184.78	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
104.17.233.204	js.hsleadflows.net	United States		13335	CLOUDFLARENETUS	false
104.244.42.195	s.twitter.com	United States		13414	TWITTERUS	false
172.64.154.85	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
162.247.243.29	fastly-tls12-bam.nr-data.net	United States		13335	CLOUDFLARENETUS	false
104.16.89.5	forms.hsforms.com	United States		13335	CLOUDFLARENETUS	false
13.224.98.228	d2oh4tlt9mrke9.cloudfront.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800796
Start date and time:	2023-02-07 19:56:27 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 38s
Hypervisor based Inspection enabled:	false

Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http:// https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@27/0@55/38
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www2.jblearning.com/my-account/login • Browse: https://www2.jblearning.com/my-account/terms-and-conditions

Warnings

- Exclude process from analysis (whitelisted): HxTsr.exe, RuntimeBroker.exe, SgrmBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.184.99, 34.104.35.123, 69.16.175.10, 69.16.175.42, 142.250.184.74, 142.250.180.168, 142.250.180.170, 142.251.209.10, 142.251.209.42, 216.58.209.42, 142.250.184.106, 142.250.180.138, 142.250.184.110, 204.79.197.200, 13.107.21.200, 80.67.82.235, 80.67.82.240, 13.107.42.14, 216.239.34.36, 216.239.32.36, 142.250.180.163, 151.101.2.137, 151.101.66.137, 151.101.130.137, 151.101.194.137
- Excluded domains from analysis (whitelisted): www.bing.com, www-linkedin-com.l-0005.l-msedge.net, client.wns.windows.com, cds.s5x3j6q5.hwcdn.net, fs.microsoft.com, content-autofill.googleapis.com, ajax.googleapis.com, dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, clientservices.googleapis.com, od.linkedin.edgesuite.net, k.sni.global.fastly.net, region1.google-analytics.com, l-0005.l-msedge.net, bat-bing-com.a-0001.a-msedge.net, edgedl.me.gvt1.com, login.live.com, www.googletagmanager.com, bat.bing.com, update.googleapis.com, cdn.onenote.net, a1916.dscg2.akamai.net, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:57:33.989370108 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:33.989434958 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:33.989564896 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:33.990643978 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:33.990731955 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:33.990817070 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.006263018 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.006359100 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.006443977 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.006988049 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.007016897 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.007359982 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.007411957 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.009948969 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.010020018 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.049689054 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.049753904 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.049830914 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.050329924 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.050355911 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.057193041 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.057677031 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.057729959 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.060116053 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.060254097 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.098370075 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.098754883 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.098798037 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.100917101 CET	443	49714	142.250.180.174	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:57:34.101018906 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.102982998 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.103074074 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.124572992 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.128876925 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.128947973 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.131165981 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.131300926 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.179701090 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.196954012 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.197022915 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.199569941 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.199681044 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.367008924 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.367042065 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.367321968 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.367682934 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.367731094 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.367916107 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.368115902 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.368145943 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.369025946 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.369056940 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.369216919 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.369277000 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.369292974 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.369566917 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.369597912 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.370109081 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.370130062 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.370155096 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.410105944 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.410209894 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.410242081 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.410269976 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.410331011 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.412561893 CET	49714	443	192.168.2.6	142.250.180.174
Feb 7, 2023 19:57:34.412599087 CET	443	49714	142.250.180.174	192.168.2.6
Feb 7, 2023 19:57:34.448808908 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.448808908 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.448810101 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.448836088 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.448841095 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.448857069 CET	443	49716	142.250.180.132	192.168.2.6
Feb 7, 2023 19:57:34.459562063 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.459711075 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.459747076 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.460038900 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.460136890 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.478640079 CET	49712	443	192.168.2.6	216.58.209.45
Feb 7, 2023 19:57:34.478682995 CET	443	49712	216.58.209.45	192.168.2.6
Feb 7, 2023 19:57:34.546483040 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.546574116 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.546581984 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.546596050 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.546646118 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.546648979 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.546660900 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.546731949 CET	49711	443	192.168.2.6	199.60.103.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 19:57:34.546749115 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.547055960 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.547107935 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.552768946 CET	49716	443	192.168.2.6	142.250.180.132
Feb 7, 2023 19:57:34.607812881 CET	49711	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.607860088 CET	443	49711	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.632288933 CET	49719	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.632356882 CET	443	49719	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.632499933 CET	49719	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.633759975 CET	49719	443	192.168.2.6	199.60.103.225
Feb 7, 2023 19:57:34.633789062 CET	443	49719	199.60.103.225	192.168.2.6
Feb 7, 2023 19:57:34.681437016 CET	443	49719	199.60.103.225	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:33.905908108 CET	192.168.2.6	8.8.8.8	0x8a1b	Standard query (0)	info.psglearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.907449961 CET	192.168.2.6	8.8.8.8	0x448b	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.912770033 CET	192.168.2.6	8.8.8.8	0x1128	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.915128946 CET	192.168.2.6	8.8.8.8	0x28c9	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:34.010226011 CET	192.168.2.6	8.8.8.8	0x1525	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:35.166531086 CET	192.168.2.6	8.8.8.8	0xecfd	Standard query (0)	www.jblearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:36.310206890 CET	192.168.2.6	8.8.8.8	0x174a	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:36.334619999 CET	192.168.2.6	8.8.8.8	0x1799	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:37.994764090 CET	192.168.2.6	8.8.8.8	0xadbc	Standard query (0)	js.hsforms.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.752310038 CET	192.168.2.6	8.8.8.8	0x5186	Standard query (0)	forms.hsforms.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.845024109 CET	192.168.2.6	8.8.8.8	0x180c	Standard query (0)	cdn.gbqofs.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.875056028 CET	192.168.2.6	8.8.8.8	0x5055	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.887521029 CET	192.168.2.6	8.8.8.8	0xe8bf	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.910269976 CET	192.168.2.6	8.8.8.8	0x8c37	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.921711922 CET	192.168.2.6	8.8.8.8	0x3f	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.064915895 CET	192.168.2.6	8.8.8.8	0x7410	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.068270922 CET	192.168.2.6	8.8.8.8	0x5fa3	Standard query (0)	d2oh4tlt9mrke9.cloudfront.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.075356960 CET	192.168.2.6	8.8.8.8	0xa5d5	Standard query (0)	tags.srv.stackadapt.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.601010084 CET	192.168.2.6	8.8.8.8	0xb4d6	Standard query (0)	forms-na1.hsforms.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.719491959 CET	192.168.2.6	8.8.8.8	0x62b9	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.749212027 CET	192.168.2.6	8.8.8.8	0x8e7d	Standard query (0)	cdn.linkedin.oribi.io	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:42.166146994 CET	192.168.2.6	8.8.8.8	0x18e2	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.581763983 CET	192.168.2.6	8.8.8.8	0x2498	Standard query (0)	t.co	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.583909988 CET	192.168.2.6	8.8.8.8	0xf40b	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.090538025 CET	192.168.2.6	8.8.8.8	0x7b46	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:47.091455936 CET	192.168.2.6	8.8.8.8	0xe6fc	Standard query (0)	region1.analytics.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.186388016 CET	192.168.2.6	8.8.8.8	0xdcda	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.234879017 CET	192.168.2.6	8.8.8.8	0xe390	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.237453938 CET	192.168.2.6	8.8.8.8	0x7ea8	Standard query (0)	js.hsadspixel.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.240303040 CET	192.168.2.6	8.8.8.8	0xfb94	Standard query (0)	js.hubspot.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.242443085 CET	192.168.2.6	8.8.8.8	0xf697	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.250880003 CET	192.168.2.6	8.8.8.8	0x9b10	Standard query (0)	js.hsleadflows.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.253475904 CET	192.168.2.6	8.8.8.8	0x6808	Standard query (0)	ws.sessioncam.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.257635117 CET	192.168.2.6	8.8.8.8	0x8de1	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:52.955410957 CET	192.168.2.6	8.8.8.8	0x827a	Standard query (0)	cta-service-cms2.hubspot.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.174882889 CET	192.168.2.6	8.8.8.8	0x1e00	Standard query (0)	api.hubapi.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.651453972 CET	192.168.2.6	8.8.8.8	0x4926	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.651998997 CET	192.168.2.6	8.8.8.8	0x4e41	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.652096987 CET	192.168.2.6	8.8.8.8	0xf7e5	Standard query (0)	perf-na1.hsforms.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.821465015 CET	192.168.2.6	8.8.8.8	0x8338	Standard query (0)	www.jblearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.953901052 CET	192.168.2.6	8.8.8.8	0xb287	Standard query (0)	t.co	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.980740070 CET	192.168.2.6	8.8.8.8	0x121a	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:08.667759895 CET	192.168.2.6	8.8.8.8	0x2133	Standard query (0)	www2.jblearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:10.531280994 CET	192.168.2.6	8.8.8.8	0x7567	Standard query (0)	fast.fonts.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:14.135523081 CET	192.168.2.6	8.8.8.8	0x2494	Standard query (0)	auth.jblearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.290303946 CET	192.168.2.6	8.8.8.8	0x37d3	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.308860064 CET	192.168.2.6	8.8.8.8	0x636e	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:30.071352959 CET	192.168.2.6	8.8.8.8	0xa825	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:30.375005007 CET	192.168.2.6	8.8.8.8	0xfd6d	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:39.790328026 CET	192.168.2.6	8.8.8.8	0x71f3	Standard query (0)	www2.jblearning.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:39.878087997 CET	192.168.2.6	8.8.8.8	0xb571	Standard query (0)	fast.fonts.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.583658934 CET	192.168.2.6	8.8.8.8	0xe278	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.586812019 CET	192.168.2.6	8.8.8.8	0x7cd1	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:49.314403057 CET	192.168.2.6	8.8.8.8	0x4137	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:49.655771017 CET	192.168.2.6	8.8.8.8	0x2644	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:33.932626963 CET	8.8.8.8	192.168.2.6	0x1128	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:33.932626963 CET	8.8.8.8	192.168.2.6	0x1128	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.932986975 CET	8.8.8.8	192.168.2.6	0x28c9	No error (0)	www.google.com		142.250.180.132	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.933130026 CET	8.8.8.8	192.168.2.6	0x448b	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.937542915 CET	8.8.8.8	192.168.2.6	0x8a1b	No error (0)	info.psglearning.com	2491413.group13.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:33.937542915 CET	8.8.8.8	192.168.2.6	0x8a1b	No error (0)	2491413.group13.sites.hubspot.net	group13.sites.hscoscdn10.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:33.937542915 CET	8.8.8.8	192.168.2.6	0x8a1b	No error (0)	group13.sites.hscoscdn10.net		199.60.103.225	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:33.937542915 CET	8.8.8.8	192.168.2.6	0x8a1b	No error (0)	group13.sites.hscoscdn10.net		199.60.103.31	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:34.036915064 CET	8.8.8.8	192.168.2.6	0x1525	No error (0)	www.google.com		142.250.180.132	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:35.189088106 CET	8.8.8.8	192.168.2.6	0xecfd	No error (0)	www.jblearning.com		104.16.13.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:35.189088106 CET	8.8.8.8	192.168.2.6	0xecfd	No error (0)	www.jblearning.com		104.16.12.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:36.329716921 CET	8.8.8.8	192.168.2.6	0x174a	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:36.354841948 CET	8.8.8.8	192.168.2.6	0x1799	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:36.354841948 CET	8.8.8.8	192.168.2.6	0x1799	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.014959097 CET	8.8.8.8	192.168.2.6	0xadbc	No error (0)	js.hsforms.net		104.17.182.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.014959097 CET	8.8.8.8	192.168.2.6	0xadbc	No error (0)	js.hsforms.net		104.17.186.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.014959097 CET	8.8.8.8	192.168.2.6	0xadbc	No error (0)	js.hsforms.net		104.17.185.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.014959097 CET	8.8.8.8	192.168.2.6	0xadbc	No error (0)	js.hsforms.net		104.17.184.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.014959097 CET	8.8.8.8	192.168.2.6	0xadbc	No error (0)	js.hsforms.net		104.17.183.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.772739887 CET	8.8.8.8	192.168.2.6	0x5186	No error (0)	forms.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.772739887 CET	8.8.8.8	192.168.2.6	0x5186	No error (0)	forms.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.772739887 CET	8.8.8.8	192.168.2.6	0x5186	No error (0)	forms.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.772739887 CET	8.8.8.8	192.168.2.6	0x5186	No error (0)	forms.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:38.772739887 CET	8.8.8.8	192.168.2.6	0x5186	No error (0)	forms.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.868275881 CET	8.8.8.8	192.168.2.6	0x180c	No error (0)	cdn.gbqofs.com		104.18.25.13	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.868275881 CET	8.8.8.8	192.168.2.6	0x180c	No error (0)	cdn.gbqofs.com		104.18.24.13	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:39.896697044 CET	8.8.8.8	192.168.2.6	0x5055	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:39.896697044 CET	8.8.8.8	192.168.2.6	0x5055	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.913780928 CET	8.8.8.8	192.168.2.6	0xe8bf	No error (0)	googleads.g.doubleclick.net		142.250.184.98	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.927833080 CET	8.8.8.8	192.168.2.6	0x8c37	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:39.927833080 CET	8.8.8.8	192.168.2.6	0x8c37	No error (0)	platform.twitter.map.fastly.net		146.75.120.157	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:39.943120003 CET	8.8.8.8	192.168.2.6	0x3f	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:40.084925890 CET	8.8.8.8	192.168.2.6	0x7410	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.084925890 CET	8.8.8.8	192.168.2.6	0x7410	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.084925890 CET	8.8.8.8	192.168.2.6	0x7410	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.084925890 CET	8.8.8.8	192.168.2.6	0x7410	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.084925890 CET	8.8.8.8	192.168.2.6	0x7410	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.091156006 CET	8.8.8.8	192.168.2.6	0x5fa3	No error (0)	d2oh4tlt9mrke9.cloudfront.net		13.224.98.228	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.091156006 CET	8.8.8.8	192.168.2.6	0x5fa3	No error (0)	d2oh4tlt9mrke9.cloudfront.net		13.224.98.181	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.091156006 CET	8.8.8.8	192.168.2.6	0x5fa3	No error (0)	d2oh4tlt9mrke9.cloudfront.net		13.224.98.156	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.091156006 CET	8.8.8.8	192.168.2.6	0x5fa3	No error (0)	d2oh4tlt9mrke9.cloudfront.net		13.224.98.223	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.095113039 CET	8.8.8.8	192.168.2.6	0xa5d5	No error (0)	tags.srv.stackadapt.com		34.196.141.135	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.095113039 CET	8.8.8.8	192.168.2.6	0xa5d5	No error (0)	tags.srv.stackadapt.com		54.237.31.137	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.095113039 CET	8.8.8.8	192.168.2.6	0xa5d5	No error (0)	tags.srv.stackadapt.com		34.230.204.192	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.095113039 CET	8.8.8.8	192.168.2.6	0xa5d5	No error (0)	tags.srv.stackadapt.com		3.232.86.255	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.095113039 CET	8.8.8.8	192.168.2.6	0xa5d5	No error (0)	tags.srv.stackadapt.com		52.20.251.240	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.623135090 CET	8.8.8.8	192.168.2.6	0xb4d6	No error (0)	forms-na1.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.623135090 CET	8.8.8.8	192.168.2.6	0xb4d6	No error (0)	forms-na1.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.623135090 CET	8.8.8.8	192.168.2.6	0xb4d6	No error (0)	forms-na1.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.623135090 CET	8.8.8.8	192.168.2.6	0xb4d6	No error (0)	forms-na1.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.623135090 CET	8.8.8.8	192.168.2.6	0xb4d6	No error (0)	forms-na1.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:40.752166986 CET	8.8.8.8	192.168.2.6	0x62b9	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:40.752166986 CET	8.8.8.8	192.168.2.6	0x62b9	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:40.770581961 CET	8.8.8.8	192.168.2.6	0x8e7d	No error (0)	cdn.linkedin.oribi.io	d1ni990a184w7d.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:40.770581961 CET	8.8.8.8	192.168.2.6	0x8e7d	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.770581961 CET	8.8.8.8	192.168.2.6	0x8e7d	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.16	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.770581961 CET	8.8.8.8	192.168.2.6	0x8e7d	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.41	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:40.770581961 CET	8.8.8.8	192.168.2.6	0x8e7d	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:42.193150997 CET	8.8.8.8	192.168.2.6	0x18e2	No error (0)	www.google.co.uk		142.251.209.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.599234104 CET	8.8.8.8	192.168.2.6	0x2498	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.599234104 CET	8.8.8.8	192.168.2.6	0x2498	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.599234104 CET	8.8.8.8	192.168.2.6	0x2498	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.599234104 CET	8.8.8.8	192.168.2.6	0x2498	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:46.603113890 CET	8.8.8.8	192.168.2.6	0xf40b	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.116662979 CET	8.8.8.8	192.168.2.6	0x7b46	No error (0)	stats.g.doubleclick.net		142.251.31.157	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.116662979 CET	8.8.8.8	192.168.2.6	0x7b46	No error (0)	stats.g.doubleclick.net		142.251.31.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.116662979 CET	8.8.8.8	192.168.2.6	0x7b46	No error (0)	stats.g.doubleclick.net		142.251.31.156	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.116662979 CET	8.8.8.8	192.168.2.6	0x7b46	No error (0)	stats.g.doubleclick.net		142.251.31.154	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.118076086 CET	8.8.8.8	192.168.2.6	0xe6fc	No error (0)	region1.analytics.google.com		216.239.34.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.118076086 CET	8.8.8.8	192.168.2.6	0xe6fc	No error (0)	region1.analytics.google.com		216.239.32.36	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:47.206278086 CET	8.8.8.8	192.168.2.6	0xdcda	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:48.258351088 CET	8.8.8.8	192.168.2.6	0xe390	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.258351088 CET	8.8.8.8	192.168.2.6	0xe390	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.258351088 CET	8.8.8.8	192.168.2.6	0xe390	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.258351088 CET	8.8.8.8	192.168.2.6	0xe390	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.258351088 CET	8.8.8.8	192.168.2.6	0xe390	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.259422064 CET	8.8.8.8	192.168.2.6	0x7ea8	No error (0)	js.hsadspixel.net		104.17.112.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.259422064 CET	8.8.8.8	192.168.2.6	0x7ea8	No error (0)	js.hsadspixel.net		104.17.114.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.259422064 CET	8.8.8.8	192.168.2.6	0x7ea8	No error (0)	js.hsadspixel.net		104.17.116.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.259422064 CET	8.8.8.8	192.168.2.6	0x7ea8	No error (0)	js.hsadspixel.net		104.17.115.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.259422064 CET	8.8.8.8	192.168.2.6	0x7ea8	No error (0)	js.hsadspixel.net		104.17.113.176	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.260504007 CET	8.8.8.8	192.168.2.6	0xfb94	No error (0)	js.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.260504007 CET	8.8.8.8	192.168.2.6	0xfb94	No error (0)	js.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.263725042 CET	8.8.8.8	192.168.2.6	0xf697	No error (0)	js.hs-banner.com		172.64.154.85	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.263725042 CET	8.8.8.8	192.168.2.6	0xf697	No error (0)	js.hs-banner.com		104.18.33.171	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.271625996 CET	8.8.8.8	192.168.2.6	0x6808	No error (0)	ws.sessioncam.com	recording-elb-2-1543527570.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:48.271625996 CET	8.8.8.8	192.168.2.6	0x6808	No error (0)	recording-elb-2-1543527570.us-east-1.elb.amazonaws.com		18.233.129.81	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.271625996 CET	8.8.8.8	192.168.2.6	0x6808	No error (0)	recording-elb-2-1543527570.us-east-1.elb.amazonaws.com		44.196.79.185	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.271625996 CET	8.8.8.8	192.168.2.6	0x6808	No error (0)	recording-elb-2-1543527570.us-east-1.elb.amazonaws.com		50.17.81.177	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.272931099 CET	8.8.8.8	192.168.2.6	0x9b10	No error (0)	js.hsleadflows.net		104.17.233.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.272931099 CET	8.8.8.8	192.168.2.6	0x9b10	No error (0)	js.hsleadflows.net		104.17.232.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.272931099 CET	8.8.8.8	192.168.2.6	0x9b10	No error (0)	js.hsleadflows.net		104.17.230.204	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:48.272931099 CET	8.8.8.8	192.168.2.6	0x9b10	No error (0)	js.hsleadflows.net		104.17.234.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.272931099 CET	8.8.8.8	192.168.2.6	0x9b10	No error (0)	js.hsleadflows.net		104.17.231.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:48.276815891 CET	8.8.8.8	192.168.2.6	0x8de1	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:48.276815891 CET	8.8.8.8	192.168.2.6	0x8de1	No error (0)	star-mini.c10r.facebook.com		157.240.253.35	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:52.976046085 CET	8.8.8.8	192.168.2.6	0x827a	No error (0)	cta-service-cms2.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:52.976046085 CET	8.8.8.8	192.168.2.6	0x827a	No error (0)	cta-service-cms2.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.198256016 CET	8.8.8.8	192.168.2.6	0x1e00	No error (0)	api.hubapi.com		104.17.201.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.198256016 CET	8.8.8.8	192.168.2.6	0x1e00	No error (0)	api.hubapi.com		104.17.204.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.198256016 CET	8.8.8.8	192.168.2.6	0x1e00	No error (0)	api.hubapi.com		104.17.203.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.198256016 CET	8.8.8.8	192.168.2.6	0x1e00	No error (0)	api.hubapi.com		104.17.200.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.198256016 CET	8.8.8.8	192.168.2.6	0x1e00	No error (0)	api.hubapi.com		104.17.202.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.672245979 CET	8.8.8.8	192.168.2.6	0xf7e5	No error (0)	perf-na1.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.672245979 CET	8.8.8.8	192.168.2.6	0xf7e5	No error (0)	perf-na1.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.672245979 CET	8.8.8.8	192.168.2.6	0xf7e5	No error (0)	perf-na1.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.672245979 CET	8.8.8.8	192.168.2.6	0xf7e5	No error (0)	perf-na1.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.672245979 CET	8.8.8.8	192.168.2.6	0xf7e5	No error (0)	perf-na1.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.673517942 CET	8.8.8.8	192.168.2.6	0x4926	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.673517942 CET	8.8.8.8	192.168.2.6	0x4926	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.673902988 CET	8.8.8.8	192.168.2.6	0x4e41	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:53.673902988 CET	8.8.8.8	192.168.2.6	0x4e41	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.844376087 CET	8.8.8.8	192.168.2.6	0x8338	No error (0)	www.jblearning.com		104.16.13.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.844376087 CET	8.8.8.8	192.168.2.6	0x8338	No error (0)	www.jblearning.com		104.16.12.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.971378088 CET	8.8.8.8	192.168.2.6	0xb287	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.971378088 CET	8.8.8.8	192.168.2.6	0xb287	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.971378088 CET	8.8.8.8	192.168.2.6	0xb287	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:57:57.971378088 CET	8.8.8.8	192.168.2.6	0xb287	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:57:57.998101950 CET	8.8.8.8	192.168.2.6	0x121a	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:08.688731909 CET	8.8.8.8	192.168.2.6	0x2133	No error (0)	www2.jblearning.com		104.16.13.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:08.688731909 CET	8.8.8.8	192.168.2.6	0x2133	No error (0)	www2.jblearning.com		104.16.12.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:10.553293943 CET	8.8.8.8	192.168.2.6	0x7567	No error (0)	fast.fonts.net		104.17.225.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:10.553293943 CET	8.8.8.8	192.168.2.6	0x7567	No error (0)	fast.fonts.net		104.17.224.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:14.156193972 CET	8.8.8.8	192.168.2.6	0x2494	No error (0)	auth.jblearning.com		104.16.13.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:14.156193972 CET	8.8.8.8	192.168.2.6	0x2494	No error (0)	auth.jblearning.com		104.16.12.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.250.184.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.250.184.110	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.250.180.142	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.251.209.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.310250998 CET	8.8.8.8	192.168.2.6	0x37d3	No error (0)	youtube-ui.l.google.com		142.251.209.46	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:19.335171938 CET	8.8.8.8	192.168.2.6	0x636e	No error (0)	www.googleoptimize.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:30.090565920 CET	8.8.8.8	192.168.2.6	0xa825	No error (0)	js-agent.newrelic.com	k.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:58:30.392282009 CET	8.8.8.8	192.168.2.6	0xfd6d	No error (0)	bam.nr-data.net	bam.cell.nr-data.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:58:30.392282009 CET	8.8.8.8	192.168.2.6	0xfd6d	No error (0)	bam.cell.nr-data.net	fastly-tls12-bam.nr-data.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:58:30.392282009 CET	8.8.8.8	192.168.2.6	0xfd6d	No error (0)	fastly-tls12-bam.nr-data.net		162.247.243.29	A (IP address)	IN (0x0001)	false

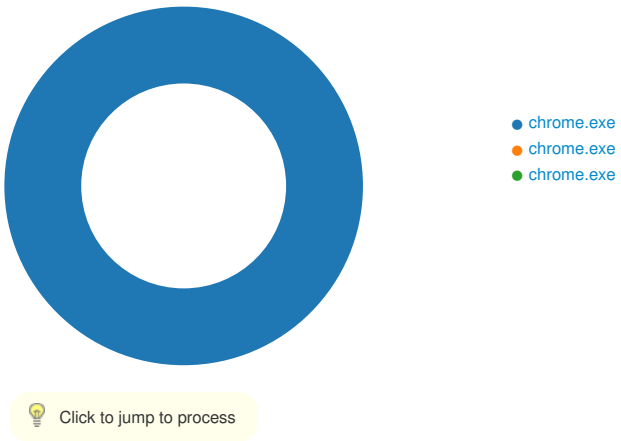
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 19:58:39.818049908 CET	8.8.8.8	192.168.2.6	0x71f3	No error (0)	www2.jblearning.com		104.16.12.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:39.818049908 CET	8.8.8.8	192.168.2.6	0x71f3	No error (0)	www2.jblearning.com		104.16.13.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:39.898756027 CET	8.8.8.8	192.168.2.6	0xb571	No error (0)	fast.fonts.net		104.17.225.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:39.898756027 CET	8.8.8.8	192.168.2.6	0xb571	No error (0)	fast.fonts.net		104.17.224.78	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.605720043 CET	8.8.8.8	192.168.2.6	0xe278	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.605720043 CET	8.8.8.8	192.168.2.6	0xe278	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.605720043 CET	8.8.8.8	192.168.2.6	0xe278	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.605720043 CET	8.8.8.8	192.168.2.6	0xe278	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.605720043 CET	8.8.8.8	192.168.2.6	0xe278	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:47.617966890 CET	8.8.8.8	192.168.2.6	0x7cd1	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 19:58:47.617966890 CET	8.8.8.8	192.168.2.6	0x7cd1	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:49.342633009 CET	8.8.8.8	192.168.2.6	0x4137	No error (0)	googleads.g.doubleclick.net		142.250.184.66	A (IP address)	IN (0x0001)	false
Feb 7, 2023 19:58:49.674084902 CET	8.8.8.8	192.168.2.6	0x2644	No error (0)	www.google.com		142.250.180.132	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- info.psglearning.com
- www.jblearning.com
- https:
  - cdnjs.cloudflare.com
  - js.hsforms.net
  - forms.hsforms.com
  - cdn.gbqofs.com
  - connect.facebook.net
  - googleads.g.doubleclick.net
  - static.ads-twitter.com
  - d2oh4tlt9mrke9.cloudfront.net
  - js.hs-scripts.com
  - forms-na1.hsforms.com
  - tags.srv.stackadapt.com
  - cdn.linkedin.oribi.io
  - www.google.com
  - www.google.co.uk
  - analytics.twitter.com
  - t.co
  - stats.g.doubleclick.net
  - www.facebook.com
  - js.hs-analytics.net
  - ws.sessioncam.com
  - js.hsleadflows.net
  - js.hubspot.com
  - js.hs-banner.com
  - js.hsadspixel.net
  - cta-service-cms2.hubspot.com
  - api.hubapi.com
  - track.hubspot.com
  - forms.hubspot.com
  - perf-na1.hsforms.com
  - www2.jblearning.com
  - fast.fonts.net
  - auth.jblearning.com
  - www.googleoptimize.com
  - www.youtube.com
  - bam.nr-data.net

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5484**, Parent PID: **2040**

General

Target ID:	0
Start time:	19:57:26
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5308**, Parent PID: **5484**

General

Target ID:	1
Start time:	19:57:28
Start date:	07/02/2023
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 --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1812 --field-trial-handle=1848,i,2574996844283921396,7295772534104560468,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **4720**, Parent PID: **2040**

General

Target ID:	2
Start time:	19:57:28
Start date:	07/02/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://info.psglearning.com/e3t/Ctc/T6+113/chRph04/VX0jT92wpDgdN8nVwc6r5CMdW5r_q0D4WM1g3N3ypqDL5nCT_V3Zsc37CgYLzW7h3pTJ25gdH9W2WNZNh2vwqtZW8FZMx74BlH2-W1YNMLJ4RwRncW34DFZb665LM_W8vlcVg7bfs92W2lK0Sp5k6h63W6w_X3-6F545NVh34nt2FQBRFW9j6zS75pZd3LW6PL48g4-m_WkW3R5pc86pdq6pW2h1q1p5C6DsxW6P6N0h9jQbqZW6mYvMv7hws6YW1CRlCn8qvZw3W1jwq2c5NDnS5W1P96Yk3g28_JW5ZXHps7JXYjsW1Y20138h2DwhW7Ym8LF7WbhRzW3H73QM6NSSq0W3NHqWW3nPnSdW3nNnjM3jQXMPV83Pjm8bRJhXW87jw4J10ThdvW7QGj6J7tnk-JW9lBrsN4s1JBhW4L4MRw39YCDNMYD9hp4P0dmW2CZgKf4SL-gxW4tDBtw3Qz4KfN2FS2s0G72MDN8cwJVt9Mjqs38dq1
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly