ID: 800711
Cookbook: browseurl.jbs
Time: 18:32:31
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

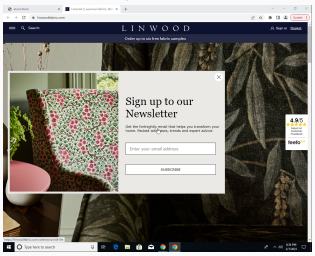
Windows Analysis Report

http://mailto:Warrick@linwoodfabric.com

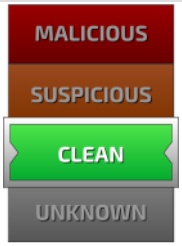
Overview

General Information

Sample URL:	http://mailto:Warrick@linwoodfabric.com
Analysis ID:	800711
Infos:	



Detection

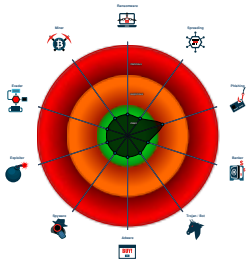


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6092 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2148 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=1948 --field-trial-handle=1772,i,16511072594903400105,15930520381033309042,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4732 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://mailto:Warrick@linwoodfabric.com 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

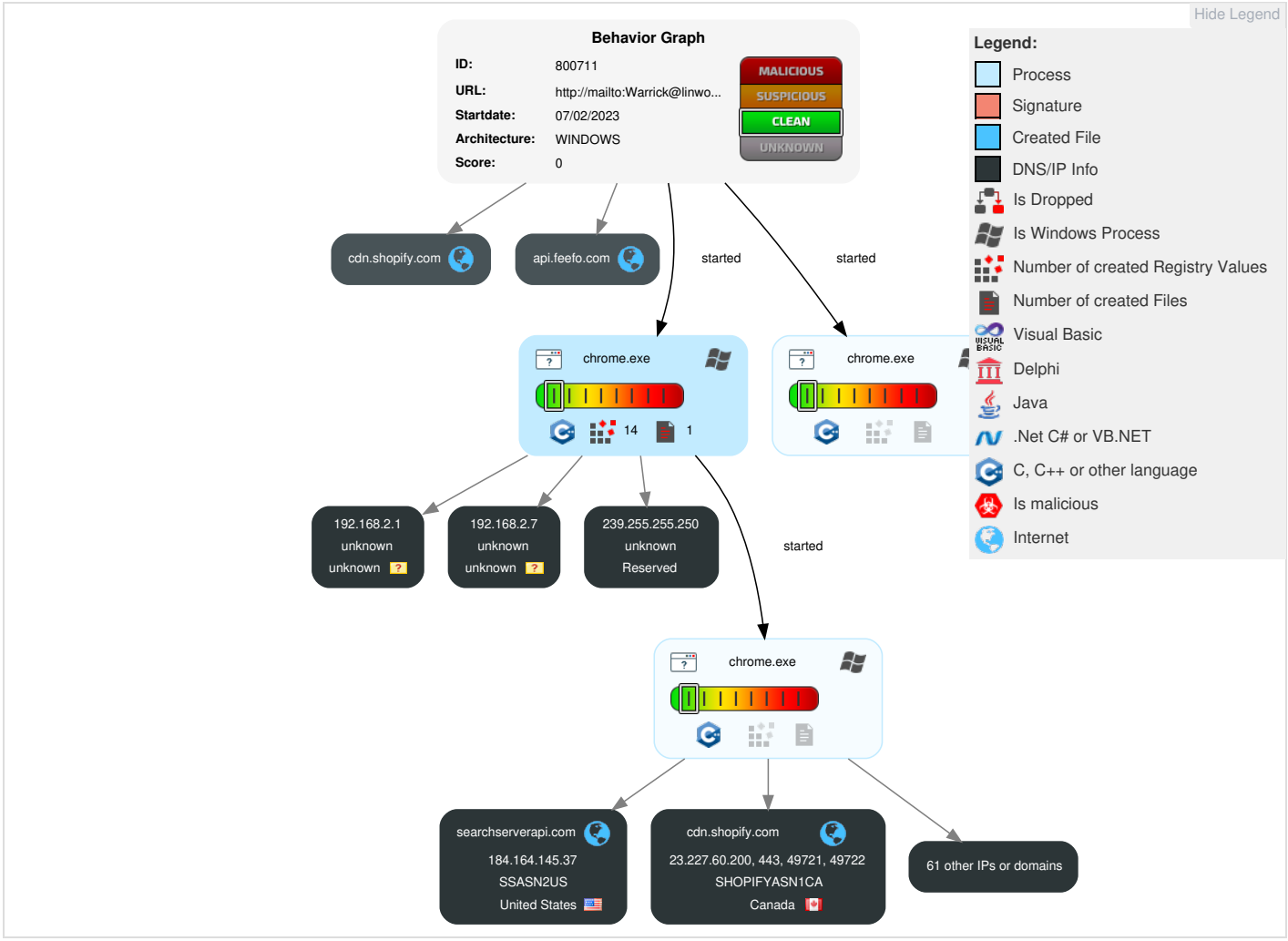
Joe Sandbox Signatures

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
Valid Accounts	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

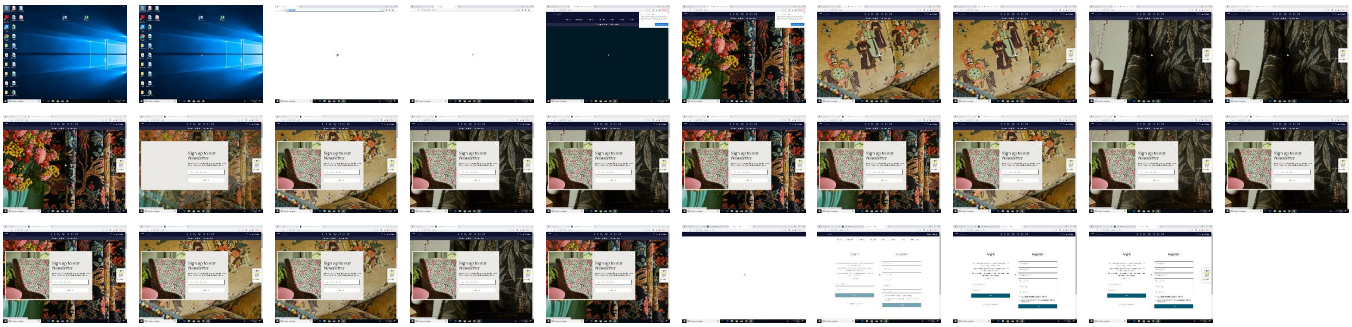
Behavior Graph

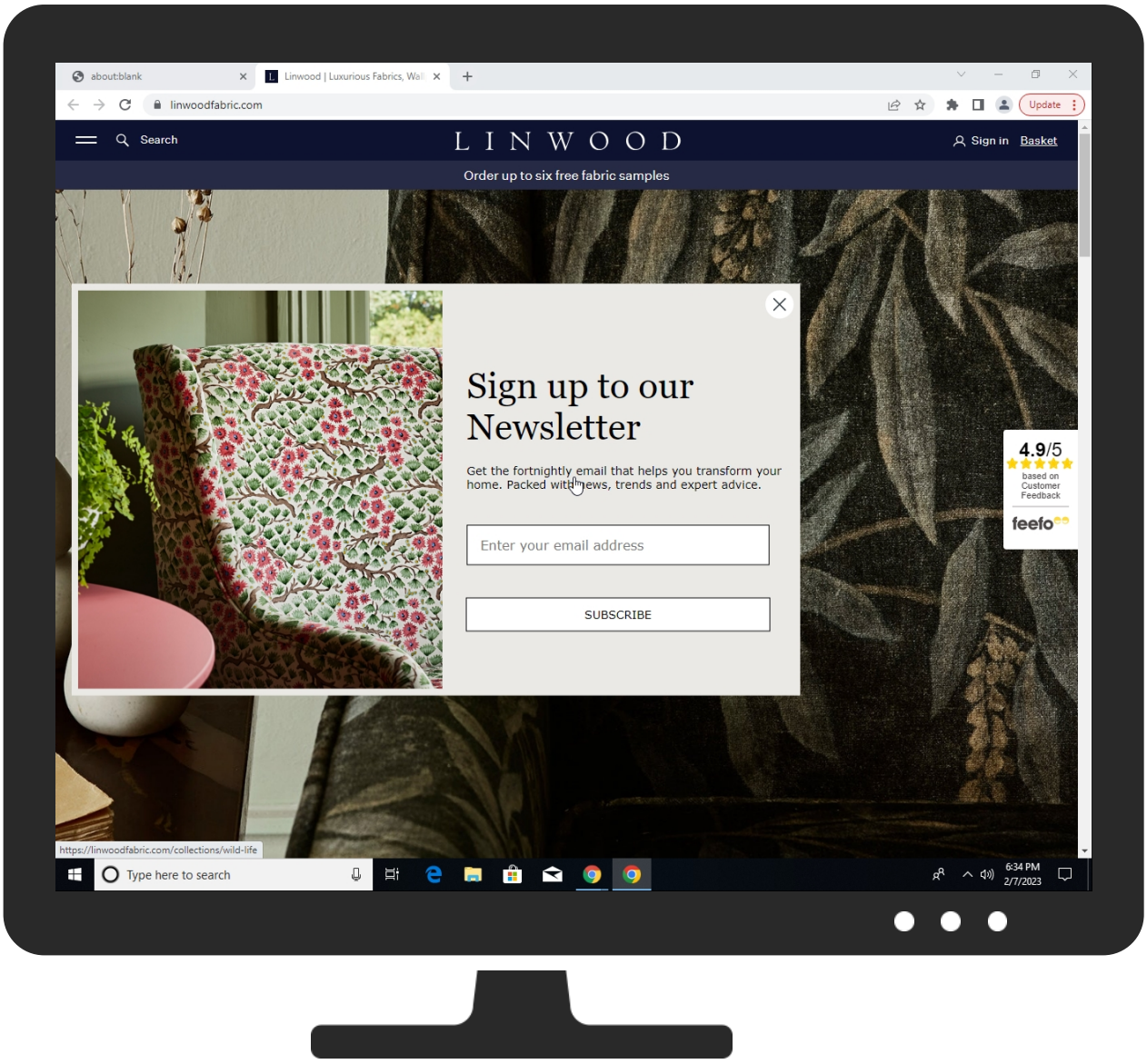


Screenshots

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://mailto:Warrick@linwoodfabric.com	0%	Virustotal		Browse
http://mailto:Warrick@linwoodfabric.com	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://monorail-edge.shopifysvc.com/unstable/produce_batch	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://shopapi.wyldcode.com/api.js?themeid=135115276530&url=https%3A%2F%2Flinwoodfabric.com%2F	0%	Avira URL Cloud	safe	
http://https://json.geoiplookup.io/	0%	Avira URL Cloud	safe	
http://https://shop.app/pay/session?v=1&token=3a35aedd-aeaa-4ae3-8f19-5213cc35ddcd&shop_id=7553056868	0%	Avira URL Cloud	safe	
http://https://shopapi.wyldcode.com/api.js?themeid=135115276530&url=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin	0%	Avira URL Cloud	safe	
http://https://image-optimizer.salessquad.co.uk/scripts/tiny_img_not_found_notifier_a83e31e34816bed528beda869e5ada2c.js?shop=linwood-fabrics.myshopify.com	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-22607785-1&cid=717999850.1675823618&jid=670498306&_u=YGBAgEABBAAAAEgCIAB~&z=1464074527	0%	Avira URL Cloud	safe	
http://https://www.clarity.ms/eus2-d/s/0.7.1/clarity.js	0%	Avira URL Cloud	safe	
http://https://chimpstatic.com/mcjs-connected/js/users/8ec43436947ade27e1170f22b/9e411277c642242fa9708f370.js?shop=linwood-fabrics.myshopify.com	0%	Avira URL Cloud	safe	
http://https://easy-image-mapper.herokuapp.com/main.min.js?shop=linwood-fabrics.myshopify.com	0%	Avira URL Cloud	safe	
http://https://searchserverapi.com/widgets/shopify/init.js?a=9X2R2q0M5z&shop=linwood-fabrics.myshopify.com	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-22607785-1&cid=717999850.1675823618&jid=1566687571&_u=QCCAgEABBAAAAEgCIAB~&z=132639384	0%	Avira URL Cloud	safe	
http://https://www.clarity.ms/tag/a62hdekh3h?ref=gtm2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.feefo.com	104.16.138.15	true	false		high
monorail-edge.shopifysvc.com	185.146.173.20	true	false		unknown
image-optimizer.salessquad.co.uk	167.114.156.181	true	false		unknown
stats.g.doubleclick.net	142.251.31.156	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
s3.amazonaws.com	52.217.135.136	true	false		high
cdnjs.cloudflare.com	104.17.25.14	true	false		high
p-chzh00.kxcdn.com	94.126.16.223	true	false		high
www.google.com	142.250.184.100	true	false		high
linwoodfabric.com	23.227.38.65	true	false		high
klaviyo-onsite.map.fastly.net	151.101.2.133	true	false		unknown
star-mini.c10r.facebook.com	157.240.253.35	true	false		high
json.geoiplookup.io	104.26.8.192	true	false		unknown
a.nel.cloudflare.com	35.190.80.1	true	false		high
searchserverapi.com	184.164.145.37	true	false		unknown
accounts.google.com	216.58.209.45	true	false		high
klaviyo-app.map.fastly.net	151.101.2.133	true	false		unknown
collect.feefo.com	104.16.75.76	true	false		high
cdn.shopify.com	23.227.60.200	true	false		high
register.feefo.com	104.16.138.15	true	false		high
shop.app	23.227.38.33	true	false		unknown
easy-image-mapper.herokuapp.com	54.205.8.205	true	false		unknown
telemetrics.klaviyo.com	13.224.103.75	true	false		high
d3k81ch9hvuctc.cloudfront.net	13.224.103.69	true	false		high
dualstack.pinterest.map.fastly.net	146.75.120.84	true	false		unknown
d1ni990a184w7d.cloudfront.net	13.224.103.7	true	false		high
chimpstatic.com	184.28.113.54	true	false		unknown
www.google.co.uk	142.251.209.3	true	false		unknown
clients.l.google.com	142.250.180.174	true	false		high
shopapi.wyldcode.com	172.67.184.153	true	false		unknown
part-0032.t-0009.fb-t-msedge.net	13.107.253.60	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.jsdelivr.net	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
static-forms.klaviyo.com	unknown	unknown	false		high
j.clarity.ms	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
static-tracking.klaviyo.com	unknown	unknown	false		high
static.klaviyo.com	unknown	unknown	false		high
cdn.linkedin.oribi.io	unknown	unknown	false		high
c.clarity.ms	unknown	unknown	false		unknown
fast.a.klaviyo.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.clarity.ms	unknown	unknown	false		unknown
www.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
searchanise-ef84.kxcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/files/SMALL-PRINTS-LANDSCAPE-2_650x450_crop_center.jpg?v=1671461926	false		high
http://https://linwoodfabric.com/.well-known/shopify/monorail/v1/produce	false		high
http://https://cdn.shopify.com/shopifycloud/shopify/assets/shopify_pay/storefront-c31d2fa4962d2ef90b673e945ee33f4f87302b97d0882cd8e83a629b84b30dab.js?v=20220906	false		high
http://https://www.facebook.com/tr/?id=286902193304953&ev=PageView&dl=https%3A%2F%2Flinwoodfabric.com%2F&rl=&if=false&ts=1675823621349&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=0&o=30&cs_est=true&fbp=fb.1.1675823621333.2046901142&it=1675823618128&coo=false&eid=2edf284d-00BA-4CB9-237F-DD97EE4A0BDA&rqm=GET	false		high
http://https://linwoodfabric.com/	false		high
http://https://linwoodfabric.com/.well-known/shopify/monorail/unstable/produce_batch	false		high
http://https://www.facebook.com/tr/?id=802872436827590&ev=Microdata&dl=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin&rl=&if=false&ts=1675823679564&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Account%5Cn%E2%80%93%20Linwood%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Linwood%20Fabrics%20%26%20Wallpapers%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin%22%2C%22og%3Atitle%22%3A%22Account%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Asecure_url%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Awidth%22%3A%221200%22%2C%22og%3Aimage%3Aheight%22%3A%22628%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=1&o=30&fbp=fb.1.1675823621333.2046901142&it=1675823678155&coo=false&es=automatic&tm=3&rqm=GET	false		high
http://https://register.feefo.com//feefo-widget-v2/js/739.feefo-widget.js	false		high
http://https://linwoodfabric.com/account/login	false		high
http://https://cdn.shopify.com/shopifycloud/consent-tracking-api/v0.1/consent-tracking-api.js	false		high
http://https://json.geoiplookup.io/	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-22607785-1&cid=717999850.1675823618&jid=1566687571&gjid=182966863&_gid=722167047.1675823618&_u=QCCAgEABBAAAAEgCIAB~&z=1091598125	false		high
http://https://static.klaviyo.com/onsite/js/vendors~signup_forms.a31dd14a1ce62f91235b.js?cb=1	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/runtime.latest.en.8645d252f07ec25fdbc6.js	false		high
http://https://static.klaviyo.com/onsite/js/signup_forms.e4023c6f8e62b93d2fc6.js?cb=1	false		high
http://https://static-tracking.klaviyo.com/onsite/js/ClientStore.849bd009ce74f18b2b01.js	false		high
http://https://static-tracking.klaviyo.com/onsite/js/vendors~Render.70ff401011c5901815b0.js	false		high

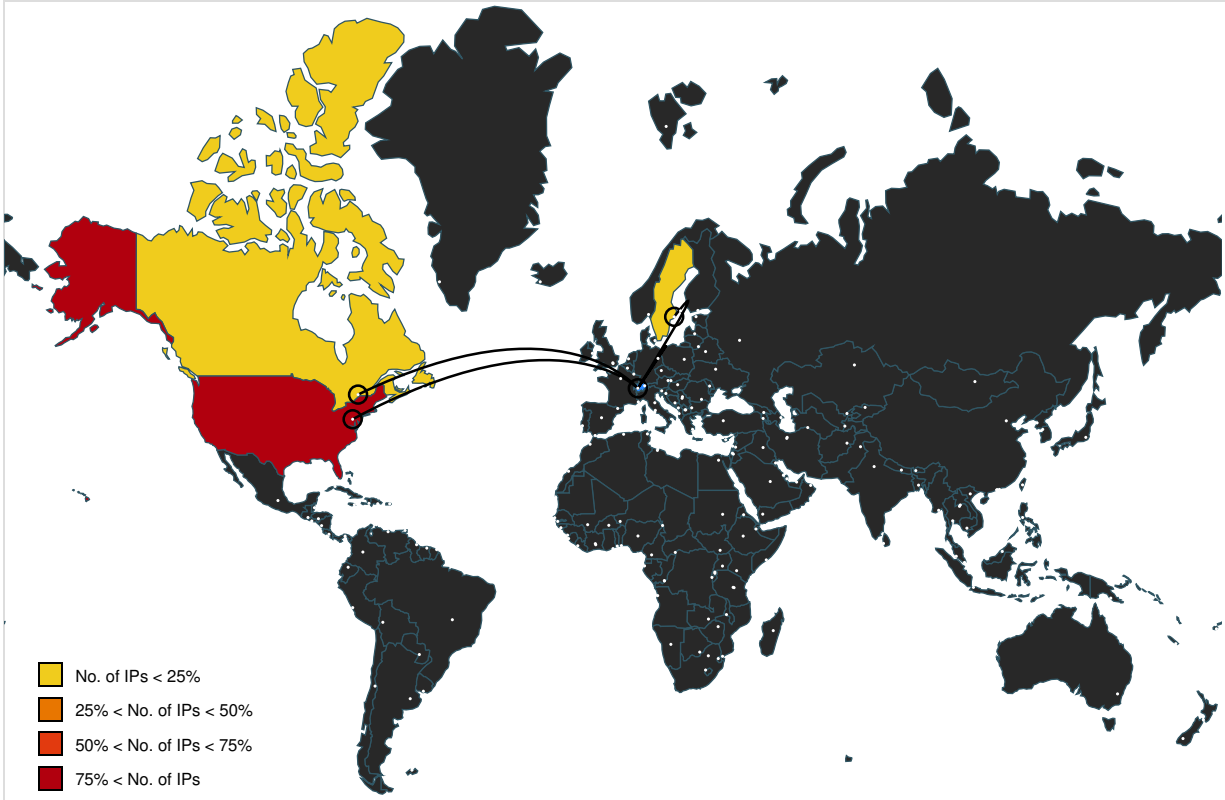
Name	Malicious	Antivirus Detection	Reputation
http://https://searchanise-ef84.kxcdn.com/preload_data.9X2R2q0M5z.js	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/checkout-web-ui~app.latest.en.86cd9328cdcd6cd3a58f.js	false		high
http://https://d3k81ch9hvuctc.cloudfront.net/company/XrNiV6/images/61caf4f8-139c-47f0-a97a-c601be9a14b9.jpeg	false		high
http://https://connect.facebook.net/en_US/fbevents.js	false		high
http://https://telemetrics.klaviyo.com/v1/metric	false		high
http://https://static-tracking.klaviyo.com/onsite/js/static.18cfb961fcdbcf83a5c0.js?cb=1	false		high
http://https://www.facebook.com/tr/?id=286902193304953&ev=Microdata&dl=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin&rl=&if=false&ts=1675823679626&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Account%5Cn%E2%80%93%20Linwood%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Linwood%20Fabrics%20%26%20Wallpapers%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin%22%2C%22og%3Atitle%22%3A%22Account%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Asecure_url%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Awidth%22%3A%221200%22%2C%22og%3Aimage%3Aheight%22%3A%22628%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=1&o=30&fbp=fb.1.1675823621333.2046901142&it=1675823678155&coo=false&es=automatic&tm=3&rqm=GET	false		high
http://https://shopapi.wyldcode.com/api.js?themeid=135115276530&url=https%3A%2F%2Flinwoodfabric.com%2F	false	• Avira URL Cloud: safe	unknown
http://https://register.feefo.com//feefo-widget-v2/js/8e073a5e15c91cfbd7ee.svg	false		high
http://https://static.klaviyo.com/onsite/js/klaviyo.js?company_id=XrNiV6	false		high
http://https://www.clarity.ms/eus2-d/s/0.7.1/clarity.js	false	• Avira URL Cloud: safe	unknown
http://https://static-tracking.klaviyo.com/onsite/js/fender_analytics.655ce7424169cb36416e.js?cb=1	false		high
http://linwoodfabric.com/	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/Information~Payment~ShopPay.latest.en.da9f06164a980bf8e7ea.css	false		high
http://https://www.facebook.com/tr/?id=802872436827590&ev=Microdata&dl=https%3A%2F%2Flinwoodfabric.com%2F&rl=&if=false&ts=1675823621881&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Linwood%20%7C%20Luxurious%20Fabrics%2C%20Wallpapers%20%26%20Cushions%22%2C%22meta%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Linwood%20Fabrics%20%26%20Wallpapers%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Flinwoodfabric.com%2F%22%2C%22og%3Atitle%22%3A%22Linwood%20%7C%20Luxurious%20Fabrics%2C%20Wallpapers%20%26%20Cushions%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Asecure_url%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Aheight%22%3A%22628%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=1&o=30&fbp=fb.1.1675823621333.2046901142&it=1675823618128&coo=false&es=automatic&tm=3&rqm=GET	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/files/SLIDER-WILD-LIFE-1_1600x@2x.jpg?v=1671106454	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.facebook.com/tr/?id=286902193304953&ev=Microdata&dl=https%3A%2F%2Flinwoodfabric.com%2F&rl=&if=false&ts=1675823621886&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Linwood%20%7C%20Luxurious%20Fabrics%2C%20Wallpapers%20%26%20Cushions%22%2C%22meta%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Linwood%20Fabrics%20%26%20Wallpapers%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Flinwoodfabric.com%2F%22%2C%22og%3Atitle%22%3A%22Linwood%20%7C%20Luxurious%20Fabrics%2C%20Wallpapers%20%26%20Cushions%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Asecure_url%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Awidth%22%3A%221200%22%2C%22og%3Aimage%3Aheight%22%3A%22628%22%7D&cd[Schema.org]=%5B%5D&cd[JSON-LD]=%5B%5D&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=1&o=30&fbp=fb.1.1675823621333.2046901142&it=1675823618128&coo=false&es=automatic&tm=3&rqm=GET	false		high
http://https://cdn.shopify.com/s/files/1/0194/1736/6592/t/1/assets/cookie_constent_shopify_secure.js?v=2898568124078079453	false		high
http://https://www.facebook.com/tr/?id=286902193304953&ev=PageView&dl=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin&rl=&if=false&ts=1675823679037&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=0&o=30&cs_est=true&fbp=fb.1.1675823621333.2046901142&it=1675823678155&coo=false&eid=2ee0167f-CBE9-4E3D-84EB-771C11BB20CD&rqm=GET	false		high
http://https://static-tracking.klaviyo.com/onsite/js/vendors~ClientStore.e95745514b016f9bd495.js	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/icon-user.svg	false		high
http://https://static-tracking.klaviyo.com/onsite/js/Render.34aa495e3f987975f99c.js	false		high
http://https://image-optimizer.salessquad.co.uk/scripts/tiny_img_not_found_notifier_a83e31e34816bed528beda869e5ada2c.js?shop=linwood-fabrics.myshopify.com	false	• Avira URL Cloud: safe	unknown
http://https://searchanise-ef84.kxcdn.com/templates.9X2R2q0M5z.js	false		high
http://https://cdn.shopify.com/shopifycloud/shopify/assets/themes_support/shopify_common-8ea6ac3faf357236a97f5de749df4da6e8436ca107bc3a4ee805cbf08bc47392.js	false		high
http://https://shopapi.wyldcode.com/api.js?themeid=135115276530&url=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/shopifycloud/shopify/assets/shop_events_listener-65cd0ba3fcd81a1df33f2510ec5bcf8c0e0958653b50e3965ec972dd638ee13f.js	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/lazysizes.min.js?v=137840748483113993891662728793	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/app.latest.en.6b4c79ead7042980b29d.css	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/temp-home.scss.css?v=194408923392758565916666619140	false		high
http://https://static.klaviyo.com/onsite/js/ClientStore.849bd009ce74f18b2b01.js	false		high
http://https://shop.app/pay/session?v=1&token=3a35aedd-aeaa-4ae3-8f19-5213cc35ddcd&shop_id=7553056868	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/main.scss.css?v=104031220010326407181666347571	false		high
http://https://cdn.shopify.com/shopifycloud/boomerang/shopify-boomerang-1.0.0.min.js	false		high
http://https://chimpstatic.com/mcjs-connected/js/users/8ec43436947ade27e1170f22b/9e411277c642242fa9708f370.js?shop=linwood-fabrics.myshopify.com	false	• Avira URL Cloud: safe	unknown
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/vendors~app.latest.en.e788719f193b49c039a3.css	false		high
http://https://api.feefo.com/api/translations/en-US/FeefoWidget?origin=linwoodfabric.com	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/icon-arrow.svg	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/booster_eu_cookie_7553056868.js?v=1662728787&shop=linwood-fabrics.myshopify.com	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/checkout-web-packages~app.latest.en.f5154093d2604596d084.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-22607785-1&cid=717999850.1675823618&jid=670498306&_u=YGBAgEABBAAAAEgCIAB~&z=1464074527	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
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://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/main.js?v=95611375962619535831673018164	false		high
http://https://searchserverapi.com/widgets/shopify/init.js?a=9X2R2q0M5z&shop=linwood-fabrics.myshopify.com	false	• Avira URL Cloud: safe	unknown
http://https://www.facebook.com/tr/?id=802872436827590&ev=PageView&dl=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin&rl=&if=false&ts=1675823679030&sw=1280&sh=1024&v=2.9.95&r=stable&a=shopify&ec=0&o=30&cs_est=true&fbp=fb.1.1675823621333.2046901142&it=1675823678155&coo=false&eid=2ee0167f-CBE9-4E3D-84EB-771C11BB20CD&rqm=GET	false		high
http://https://api.feefo.com/api/merchants/widgetintegration/all?merchant_identifier=linwood-fabric&origin=linwoodfabric.com	false		high
http://https://register.feefo.com//feefo-widget-v2/js/slideout-reviews-widget-slideout-reviews-widget-jsx.css	false		high
http://https://s3.amazonaws.com/verge-shopify/verge-json-ld.js?shop=linwood-fabrics.myshopify.com	false		high
http://https://static.klaviyo.com/onsite/js/Render.34aa495e3f987975f99c.js	false		high
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-22607785-1&cid=717999850.1675823618&jid=670498306&gjid=1366653155&_gid=722167047.1675823618&_u=YGBAgEABBAAAAEgCIAB~&z=160895486	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-22607785-1&cid=717999850.1675823618&jid=670498306&_u=YGBAgEABBAAAAEgCIAB~&z=1464074527	false		high
http://https://connect.facebook.net/signals/config/286902193304953?v=2.9.95&r=stable	false		high
http://https://monorail-edge.shopifysvc.com/unstable/produce_batch	false	• URL Reputation: safe	unknown
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/vendors~app.latest.en.b4546f9bffad10b3673b.js	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/logo.svg?v=115832163940476509511662728792	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/checkout-web-packages~Information~NoAddressLocation~Payment~PostPurchase~Review~Shipping~ShopPay~Sho~cf13f96e.latest.en.04837ae4ff5a8e949953.js	false		high
http://https://a.nel.cloudflare.com/report/v3?s=h2zd5GKs2wvIfyn9aWYq7zWF%2BphHzQZSOvcc1Dgiu7gAem9KMV2Mo1y88H%2FvGMGSb9JFLnonIUriqVnE82b4vgb0yTR0abLEI5xIGPAD2o%2FbKHrQwBnX1gqoBxu4xBRD4Q%3D%3D	false		high
http://https://api.feefo.com/api/10/reviews/summary/service?since_period=YEAR&unanswered_feedback=include&source=on_page_service_integration&merchant_identifier=linwood-fabric&origin=linwoodfabric.com	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/checkout-web-ui~app.latest.en.9f2a5e9ec696775e2217.css	false		high
http://https://easy-image-mapper.herokuapp.com/main.min.js?shop=linwood-fabrics.myshopify.com	false	• Avira URL Cloud: safe	unknown
http://https://searchanise-ef84.kxcdn.com/widgets.78125.min.js	false		high
http://https://register.feefo.com//feefo-widget-v2/js/677.feefo-widget.js	false		high
http://https://register.feefo.com//feefo-widget-v2/js/646.feefo-widget.js	false		high
http://https://register.feefo.com//feefo-widget-v2/js/feefo-widget.js	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/favicon.png?v=151257522448072920881662728793	false		high
http://https://static.klaviyo.com/onsite/js/532.dd9a1df84d96cf83ca19.css	false		high
http://https://fast.a.klaviyo.com/custom-fonts/api/v1/company-fonts/onsite?company_id=XrNiV6	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-22607785-1&cid=717999850.1675823618&jid=1566687571&_u=QCCAgEABBAAAAEgCIAB~&z=132639384	false	• Avira URL Cloud: safe	unknown
http://https://linwoodfabric.com/account/login	false		high
http://https://cdn.shopify.com/shopifycloud/shopify/assets/storefront/features-87e8399988880142f2c62771b9d8f2ff6c290b3ff745dd426eb0dfe0db9d1dae.js	false		high
http://https://api.feefo.com/api/javascript/linwood-fabric	false		high
http://https://cdn.shopify.com/s/files/1/0075/5305/6868/t/39/assets/logo-white.svg	false		high
http://https://static.klaviyo.com/onsite/js/vendors~Render.70ff401011c5901815b0.js	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.facebook.com/tr/?a=shopify&cd[DataLayer]=%5B%5D&cd[JSON-LD]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Account%5Cn%E2%80%93%20Linwood%22%7D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Linwood%20Fabrics%20%26%20Wallpapers%22%2C%22og%3Aurl%22%3A%22https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin%22%2C%22og%3Atitle%22%3A%22Account%22%2C%22og%3Atype%22%3A%22website%22%2C%22og%3Adescription%22%3A%22Designers%20and%20suppliers%20of%20beautiful%20fabrics%2C%20wallpapers%20%26%20cushions.%20Offering%20a%20wide%20range%20of%20fabrics%20for%20curtains%20and%20upholstery%20including%20stain%20resistant%20velvets%2C%20weaves%2C%20wools%2C%20contemporary%20and%20classic%20prints.%20Request%20your%20samples%20of%20our%20fabrics%20and%20wallpapers.%22%2C%22og%3Aimage%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Asecure_url%22%3A%22https%3A%2F%2Fcdn.shopify.com%2Fs%2Ffiles%2F1%2F0075%2F5305%2F6868%2Ffiles%2FLinwood_Logo.png%3Fheight%3D628%26pad_color%3Dfff%26v%3D1613176814%26width%3D1200%22%2C%22og%3Aimage%3Awidth%22%3A%221200%22%2C%22og%3Aimage%3Aheight%22%3A%22628%22%7D&cd[Schema.org]=%5B%5D&coo=false&dl=https%3A%2F%2Flinwoodfabric.com%2Faccount%2Flogin&ec=1&es=automatic&ev=Microdata&fbp=fb.1.1675823621333.2046901142&id=2869021933049 53&if=false&it=1675823678155&o=30&r=stable&redirect=0&rl=&rqm=GET&sh=1024&sw=1280&tm=3&ts=1675823679626&v=2.9.95	false		high
http://https://s.pinimg.com/ct/core.js	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/Information~Payment~ShopPay.latest.en.84ff9c0024faf7f72c14.js	false		high
http://https://static-forms.klaviyo.com/forms/api/v6/XrNiV6/full-forms	false		high
http://https://searchanise-ef84.kxcdn.com/items_modern.78125.css	false		high
http://https://s.pinimg.com/ct/lib/main.e9706407.js	false		high
http://https://cdn.shopify.com/shopifycloud/web-pixels-manager/0.0.211/browser.modern.js	false		high
http://https://searchanise-ef84.kxcdn.com/recommendation.78125.css	false		high
http://https://cdn.shopify.com/shopifycloud/checkout-web/assets/app.latest.en.931851b1b02f1bcae42a.js	false		high
http://https://www.clarity.ms/tag/a62hdekh3h?ref=gtm2	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.59.224	unknown	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
13.107.253.60	part-0032.t-0009.fb-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.75.116.84	unknown	Sweden		30051	SCCGOVUS	false
142.250.184.100	www.google.com	United States		15169	GOOGLEUS	false
142.251.31.156	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
13.224.103.75	telemetrics.klaviyo.com	United States		16509	AMAZON-02US	false
142.251.31.155	unknown	United States		15169	GOOGLEUS	false
54.205.8.205	easy-image-mapper.herokuapp.com	United States		14618	AMAZON-AESUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.217.135.136	s3.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.103.69	d3k81ch9hvuctc.cloudfront.net	United States		16509	AMAZON-02US	false
157.240.253.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
184.28.113.54	chimpstatic.com	United States		20940	AKAMAI-ASN1EU	false
142.250.180.174	clients.l.google.com	United States		15169	GOOGLEUS	false
23.227.60.200	cdn.shopify.com	Canada		62679	SHOPIFYASN1CA	false
104.26.8.192	json.geoiplookup.io	United States		13335	CLOUDFLARENETUS	false
23.227.38.33	shop.app	Canada		13335	CLOUDFLARENETUS	false
146.75.120.84	dualstack.pinterest.map.fastly.net	Sweden		30051	SCCGOVUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
13.224.103.7	d1ni990a184w7d.cloudfront.net	United States		16509	AMAZON-02US	false
185.146.173.20	monorail-edge.shopifysvc.com	Sweden		200760	ELOGIC-ASElogicSrl-CloudServicesIT	false
184.164.145.37	searchserverapi.com	United States		20454	SSASN2US	false
104.16.75.76	collect.feefo.com	United States		13335	CLOUDFLARENETUS	false
104.17.24.14	unknown	United States		13335	CLOUDFLARENETUS	false
167.114.156.181	image-optimizer.salessquad.co.uk	Canada		16276	OVHFR	false
94.126.16.223	p-chzh00.kxcdn.com	Switzerland		21069	ASN-METANETRoutingpeeringissuesnocmetanetchCH	false
104.16.138.15	api.feefo.com	United States		13335	CLOUDFLARENETUS	false
23.227.38.65	linwoodfabric.com	Canada		13335	CLOUDFLARENETUS	false
151.101.2.133	klaviyo-onsite.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
192.168.2.7
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800711
Start date and time:	2023-02-07 18:32:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://mailto:Warrick@linwoodfabric.com
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:	clean0.win@27/0@63/35
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://linwoodfabric.com/account/login

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, 142.250.184.106, 104.16.85.20, 104.16.88.20, 104.16.86.20, 104.16.87.20, 104.16.89.20, 142.250.184.74, 142.250.180.138, 142.250.180.170, 142.251.209.10, 142.251.209.42, 216.58.209.42, 69.16.175.42, 69.16.175.10, 142.250.180.168, 80.67.82.240, 80.67.82.235, 216.239.32.178, 216.239.38.178, 216.239.34.178, 216.239.36.178, 13.107.42.14, 216.239.34.36, 216.239.32.36, 20.85.30.134, 142.250.184.67, 23.211.4.189, 20.234.93.27, 204.79.197.200, 13.107.21.200, 152.199.19.160, 142.250.180.163, 142.250.184.110
- Excluded domains from analysis (whitelisted): cdn.jsdelivr.net.cdn.cloudflare.net, cds.s5x3j6q5.hwcdn.net, global-entry-afdthirdparty-fallback-first.trafficmanager.net, c-msn-com-nsatc.trafficmanager.net, c-bing-com.a-0001.a-msedge.net, clientservices.googleapis.com, region1.google-analytics.com, maps.googleapis.com, 2-01-37d2-0006.cdx.cedexis.net, l-0005.l-msedge.net, mscomajax.vo.msecnd.net, login.live.com, www.googletagmanager.com, star-azurefd-prod.trafficmanager.net, 2-01-37d2-0018.cdx.cedexis.net, update.googleapis.com, e6449.a.akamaiedge.net, cdn.onenote.net, www.google-analytics.com, www.bing.com, www-linkedin-com.l-0005.l-msedge.net, client.wns.windows.com, fonts.googleapis.com, fs.microsoft.com, vmss-clarity-ingest-eus2-d.eastus2.cloudapp.azure.com, content-autofill.googleapis.com, ajax.googleapis.com, fonts.gstatic.com, dual-a-0001.a-msedge.net, cs22.wpc.v0cdn.net, www-alv.google-analytics.com, ctldl.windowsupdate.com, od.linkedin.edgesuite.net, www.pinterest.com.edgekey.net, edgedl.me.gvt1.com, c.
- 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

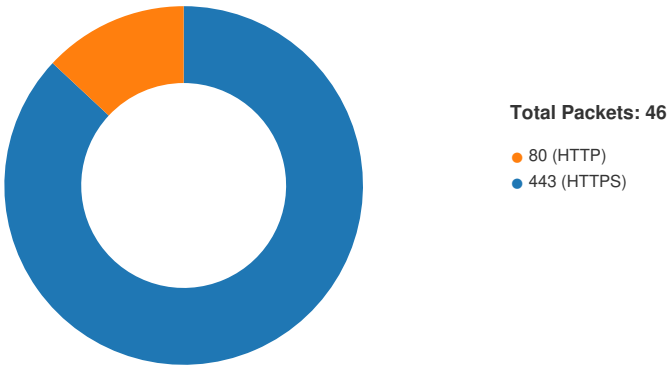
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:33:33.166982889 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.167025089 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.167115927 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.167412996 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.167429924 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.169287920 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:33.169342041 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.169414043 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:33.169785976 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:33.169807911 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.245448112 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.264004946 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.286587954 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.358562946 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:33.358592033 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.359050035 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.359069109 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.360526085 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.360616922 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.361423969 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.361468077 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:33.361552954 CET	49713	443	192.168.2.6	216.58.209.45

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:33:33.362787962 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:33.362867117 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:33.446656942 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:34.743302107 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:34.743344069 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.743457079 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:34.743465900 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.743688107 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.743868113 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:34.743896008 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.743989944 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:34.744000912 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.744288921 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.787349939 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.787502050 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:34.787532091 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.787642002 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:34.787708044 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:34.844183922 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:34.844204903 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.852360964 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.852437973 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:34.852459908 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.854250908 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:34.854321003 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:35.342459917 CET	49714	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.342628956 CET	49715	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.342941999 CET	49713	443	192.168.2.6	216.58.209.45
Feb 7, 2023 18:33:35.342986107 CET	443	49713	216.58.209.45	192.168.2.6
Feb 7, 2023 18:33:35.344928980 CET	49712	443	192.168.2.6	142.250.180.174
Feb 7, 2023 18:33:35.344960928 CET	443	49712	142.250.180.174	192.168.2.6
Feb 7, 2023 18:33:35.359853983 CET	80	49714	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.360008001 CET	80	49715	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.360358953 CET	49714	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.360493898 CET	49715	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.547180891 CET	49714	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.565646887 CET	80	49714	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.622087955 CET	80	49714	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.622123957 CET	80	49714	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.622248888 CET	49714	80	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.817929983 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.817981005 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.818083048 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.818526030 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.818536997 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.818595886 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.819037914 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.819052935 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.819432974 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.819443941 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.908215046 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.915977001 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.916012049 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.918231964 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.918351889 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.926538944 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.930469036 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.930495024 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.932845116 CET	443	49716	142.250.184.100	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:33:35.932923079 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.947518110 CET	49716	443	192.168.2.6	142.250.184.100
Feb 7, 2023 18:33:35.947540045 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.947801113 CET	443	49716	142.250.184.100	192.168.2.6
Feb 7, 2023 18:33:35.948615074 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.948627949 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.948883057 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:35.950275898 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:35.950294018 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.018942118 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019048929 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:36.019068956 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019139051 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019232988 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:36.019238949 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019257069 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019304991 CET	49717	443	192.168.2.6	23.227.38.65
Feb 7, 2023 18:33:36.019311905 CET	443	49717	23.227.38.65	192.168.2.6
Feb 7, 2023 18:33:36.019368887 CET	443	49717	23.227.38.65	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:33:33.077668905 CET	192.168.2.6	8.8.8.8	0x9419	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:33.082726955 CET	192.168.2.6	8.8.8.8	0xaf1d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:34.645457029 CET	192.168.2.6	8.8.8.8	0x50ac	Standard query (0)	linwoodfabric.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.725217104 CET	192.168.2.6	8.8.8.8	0x240	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.760725975 CET	192.168.2.6	8.8.8.8	0x2aeb	Standard query (0)	linwoodfabric.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.769531012 CET	192.168.2.6	8.8.8.8	0xdb20	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.291523933 CET	192.168.2.6	8.8.8.8	0x8b1f	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.306766987 CET	192.168.2.6	8.8.8.8	0xe2b0	Standard query (0)	shopapi.weldcode.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.329206944 CET	192.168.2.6	8.8.8.8	0x2817	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.331060886 CET	192.168.2.6	8.8.8.8	0x8a23	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.374933958 CET	192.168.2.6	8.8.8.8	0xdff	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.377284050 CET	192.168.2.6	8.8.8.8	0x3044	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.380359888 CET	192.168.2.6	8.8.8.8	0xc2e8	Standard query (0)	shopapi.weldcode.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.737082005 CET	192.168.2.6	8.8.8.8	0x7e6c	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.912437916 CET	192.168.2.6	8.8.8.8	0x57a	Standard query (0)	static.klaviyo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.912843943 CET	192.168.2.6	8.8.8.8	0x204	Standard query (0)	monorail-edge.shopifysvc.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.928584099 CET	192.168.2.6	8.8.8.8	0x7ca5	Standard query (0)	api.feefo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.810084105 CET	192.168.2.6	8.8.8.8	0x363a	Standard query (0)	shop.app	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.818582058 CET	192.168.2.6	8.8.8.8	0x29a	Standard query (0)	static-tracking.klaviyo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.941422939 CET	192.168.2.6	8.8.8.8	0xa7b4	Standard query (0)	register.feefo.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:33:38.078702927 CET	192.168.2.6	8.8.8.8	0x7f83	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.091425896 CET	192.168.2.6	8.8.8.8	0xf99b	Standard query (0)	www.clarity.ms	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.140795946 CET	192.168.2.6	8.8.8.8	0xb5cd	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.227977037 CET	192.168.2.6	8.8.8.8	0x21b9	Standard query (0)	monorail-edge.shopifysvc.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.238882065 CET	192.168.2.6	8.8.8.8	0xc54b	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.011166096 CET	192.168.2.6	8.8.8.8	0xd413	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.073864937 CET	192.168.2.6	8.8.8.8	0xdabf	Standard query (0)	static-forms.klaviyo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.074314117 CET	192.168.2.6	8.8.8.8	0x82dc	Standard query (0)	fast.a.klaviyo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.278861046 CET	192.168.2.6	8.8.8.8	0x27c1	Standard query (0)	cdn.linkedin.oribi.io	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.282202005 CET	192.168.2.6	8.8.8.8	0x2447	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:40.556746006 CET	192.168.2.6	8.8.8.8	0x2447	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:40.882417917 CET	192.168.2.6	8.8.8.8	0xe5d2	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:41.040585041 CET	192.168.2.6	8.8.8.8	0x5b9	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:41.124090910 CET	192.168.2.6	8.8.8.8	0x99e3	Standard query (0)	j.clarity.ms	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:41.558497906 CET	192.168.2.6	8.8.8.8	0x48c7	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:42.206218958 CET	192.168.2.6	8.8.8.8	0x8bc2	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:42.724828959 CET	192.168.2.6	8.8.8.8	0x1ed9	Standard query (0)	collect.feefo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.054617882 CET	192.168.2.6	8.8.8.8	0x5b2d	Standard query (0)	chimpstatic.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.055867910 CET	192.168.2.6	8.8.8.8	0xed89	Standard query (0)	easy-image-mapper.herokuapp.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.056624889 CET	192.168.2.6	8.8.8.8	0xdc9e	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.056863070 CET	192.168.2.6	8.8.8.8	0xf5bc	Standard query (0)	image-optimizer.salessquad.co.uk	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.057221889 CET	192.168.2.6	8.8.8.8	0x6a8b	Standard query (0)	searchserverapi.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.057306051 CET	192.168.2.6	8.8.8.8	0x2cc3	Standard query (0)	c.clarity.ms	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:46.229465961 CET	192.168.2.6	8.8.8.8	0x8b9b	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.749820948 CET	192.168.2.6	8.8.8.8	0x5dc1	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.753613949 CET	192.168.2.6	8.8.8.8	0xce32	Standard query (0)	searchanise-ef84.kxcdn.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.781361103 CET	192.168.2.6	8.8.8.8	0x9d1c	Standard query (0)	json.geoiplookup.io	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:54.561844110 CET	192.168.2.6	8.8.8.8	0x591c	Standard query (0)	telemetrics.klaviyo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:55.982872009 CET	192.168.2.6	8.8.8.8	0xdedb	Standard query (0)	d3k81ch9hvuctc.cloudfront.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:18.449441910 CET	192.168.2.6	8.8.8.8	0x7aa8	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:18.682183027 CET	192.168.2.6	8.8.8.8	0xe77f	Standard query (0)	api.feefo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:35.805069923 CET	192.168.2.6	8.8.8.8	0x2551	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:35.903580904 CET	192.168.2.6	8.8.8.8	0x718	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:34:36.435803890 CET	192.168.2.6	8.8.8.8	0xea4	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.489025116 CET	192.168.2.6	8.8.8.8	0x415d	Standard query (0)	monorail-edge.shopifysvc.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.632251978 CET	192.168.2.6	8.8.8.8	0xe135	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.711683989 CET	192.168.2.6	8.8.8.8	0x3b5	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.722903013 CET	192.168.2.6	8.8.8.8	0x22d0	Standard query (0)	linwoodfabric.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.915174007 CET	192.168.2.6	8.8.8.8	0x386f	Standard query (0)	register.feefo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.157099962 CET	192.168.2.6	8.8.8.8	0x43f2	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.708769083 CET	192.168.2.6	8.8.8.8	0x3028	Standard query (0)	api.feefo.com	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:44.664437056 CET	192.168.2.6	8.8.8.8	0xacb2	Standard query (0)	j.clarity.ms	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:49.462832928 CET	192.168.2.6	8.8.8.8	0x66a6	Standard query (0)	static.klaviyo.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 18:33:33.106153011 CET	8.8.8.8	192.168.2.6	0x9419	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:33.106153011 CET	8.8.8.8	192.168.2.6	0x9419	No error (0)	clients.l.google.com		142.250.180.174	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:33.123466969 CET	8.8.8.8	192.168.2.6	0xaf1d	No error (0)	accounts.google.com		216.58.209.45	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:34.677412987 CET	8.8.8.8	192.168.2.6	0x50ac	No error (0)	linwoodfabric.com		23.227.38.65	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.751247883 CET	8.8.8.8	192.168.2.6	0x240	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.787734985 CET	8.8.8.8	192.168.2.6	0xdb20	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:35.809433937 CET	8.8.8.8	192.168.2.6	0x2aeb	No error (0)	linwoodfabric.com		23.227.38.65	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.310857058 CET	8.8.8.8	192.168.2.6	0x8b1f	No error (0)	cdn.shopify.com		23.227.60.200	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.329494953 CET	8.8.8.8	192.168.2.6	0xe2b0	No error (0)	shopapi.wyldcode.com		172.67.184.153	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.329494953 CET	8.8.8.8	192.168.2.6	0xe2b0	No error (0)	shopapi.wyldcode.com		104.21.59.224	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.349786043 CET	8.8.8.8	192.168.2.6	0x8a23	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.349786043 CET	8.8.8.8	192.168.2.6	0x8a23	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.351917982 CET	8.8.8.8	192.168.2.6	0x2817	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:36.393059969 CET	8.8.8.8	192.168.2.6	0xdff	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:36.397120953 CET	8.8.8.8	192.168.2.6	0x3044	No error (0)	cdnjs.cloudflare.com		104.17.24.14	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 18:33:36.397120953 CET	8.8.8.8	192.168.2.6	0x3044	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.402023077 CET	8.8.8.8	192.168.2.6	0xc2e8	No error (0)	shopapi.wyldcode.com		104.21.59.224	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.402023077 CET	8.8.8.8	192.168.2.6	0xc2e8	No error (0)	shopapi.wyldcode.com		172.67.184.153	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.754992008 CET	8.8.8.8	192.168.2.6	0x7e6c	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:36.930082083 CET	8.8.8.8	192.168.2.6	0x204	No error (0)	monorail-edge.shopifysvc.com		185.146.173.20	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.931464911 CET	8.8.8.8	192.168.2.6	0x57a	No error (0)	static.klaviyo.com	klaviyo-onsite.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:36.931464911 CET	8.8.8.8	192.168.2.6	0x57a	No error (0)	klaviyo-onsite.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.931464911 CET	8.8.8.8	192.168.2.6	0x57a	No error (0)	klaviyo-onsite.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.931464911 CET	8.8.8.8	192.168.2.6	0x57a	No error (0)	klaviyo-onsite.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.931464911 CET	8.8.8.8	192.168.2.6	0x57a	No error (0)	klaviyo-onsite.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.948420048 CET	8.8.8.8	192.168.2.6	0x7ca5	No error (0)	api.feefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:36.948420048 CET	8.8.8.8	192.168.2.6	0x7ca5	No error (0)	api.feefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.827374935 CET	8.8.8.8	192.168.2.6	0x363a	No error (0)	shop.app		23.227.38.33	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.838288069 CET	8.8.8.8	192.168.2.6	0x29a	No error (0)	static-tracking.klaviyo.com	klaviyo-app.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:37.838288069 CET	8.8.8.8	192.168.2.6	0x29a	No error (0)	klaviyo-app.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.838288069 CET	8.8.8.8	192.168.2.6	0x29a	No error (0)	klaviyo-app.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.838288069 CET	8.8.8.8	192.168.2.6	0x29a	No error (0)	klaviyo-app.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.838288069 CET	8.8.8.8	192.168.2.6	0x29a	No error (0)	klaviyo-app.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.962094069 CET	8.8.8.8	192.168.2.6	0xa7b4	No error (0)	register.feefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:37.962094069 CET	8.8.8.8	192.168.2.6	0xa7b4	No error (0)	register.feefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.101443052 CET	8.8.8.8	192.168.2.6	0x7f83	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	www.clarity.ms	clarity.azurefd.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	clarity.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	shed.dual-low.part-0032.t-0009.fdv2-t-msedge.net	global-entry-afdthirdparty-fallback-first.trafficmanager.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 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	shed.dual-low.part-0032.t-0009.fb-t-msedge.net	part-0032.t-0009.fb-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	part-0032.t-0009.fb-t-msedge.net		13.107.253.60	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.119290113 CET	8.8.8.8	192.168.2.6	0xf99b	No error (0)	part-0032.t-0009.fb-t-msedge.net		13.107.226.60	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.173393011 CET	8.8.8.8	192.168.2.6	0xb5cd	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.173393011 CET	8.8.8.8	192.168.2.6	0xb5cd	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.248524904 CET	8.8.8.8	192.168.2.6	0x21b9	No error (0)	monorail-edge.shopifysvc.com		185.146.173.20	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:38.260521889 CET	8.8.8.8	192.168.2.6	0xc54b	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.260521889 CET	8.8.8.8	192.168.2.6	0xc54b	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:38.260521889 CET	8.8.8.8	192.168.2.6	0xc54b	No error (0)	dualstack.pinterest.map.fastly.net		146.75.120.84	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.029223919 CET	8.8.8.8	192.168.2.6	0xd413	No error (0)	stats.g.doubleclick.net		142.251.31.156	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.029223919 CET	8.8.8.8	192.168.2.6	0xd413	No error (0)	stats.g.doubleclick.net		142.251.31.154	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.029223919 CET	8.8.8.8	192.168.2.6	0xd413	No error (0)	stats.g.doubleclick.net		142.251.31.157	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.029223919 CET	8.8.8.8	192.168.2.6	0xd413	No error (0)	stats.g.doubleclick.net		142.251.31.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.091679096 CET	8.8.8.8	192.168.2.6	0xdabf	No error (0)	static-forms.klaviyo.com	klaviyo-onsite.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:39.091679096 CET	8.8.8.8	192.168.2.6	0xdabf	No error (0)	klaviyo-onsite.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.091679096 CET	8.8.8.8	192.168.2.6	0xdabf	No error (0)	klaviyo-onsite.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.091679096 CET	8.8.8.8	192.168.2.6	0xdabf	No error (0)	klaviyo-onsite.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.091679096 CET	8.8.8.8	192.168.2.6	0xdabf	No error (0)	klaviyo-onsite.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.093995094 CET	8.8.8.8	192.168.2.6	0x82dc	No error (0)	fast.a.klaviyo.com	klaviyo-onsite.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:39.093995094 CET	8.8.8.8	192.168.2.6	0x82dc	No error (0)	klaviyo-onsite.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.093995094 CET	8.8.8.8	192.168.2.6	0x82dc	No error (0)	klaviyo-onsite.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.093995094 CET	8.8.8.8	192.168.2.6	0x82dc	No error (0)	klaviyo-onsite.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.093995094 CET	8.8.8.8	192.168.2.6	0x82dc	No error (0)	klaviyo-onsite.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.299823999 CET	8.8.8.8	192.168.2.6	0x27c1	No error (0)	cdn.linkedin.oribi.io	d1ni990a184w7d.cloudfront.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 18:33:39.299823999 CET	8.8.8.8	192.168.2.6	0x27c1	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.7	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.299823999 CET	8.8.8.8	192.168.2.6	0x27c1	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.16	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.299823999 CET	8.8.8.8	192.168.2.6	0x27c1	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.41	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.299823999 CET	8.8.8.8	192.168.2.6	0x27c1	No error (0)	d1ni990a184w7d.cloudfront.net		13.224.103.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:39.315260887 CET	8.8.8.8	192.168.2.6	0x2447	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:39.315260887 CET	8.8.8.8	192.168.2.6	0x2447	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:40.578943014 CET	8.8.8.8	192.168.2.6	0x2447	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:40.578943014 CET	8.8.8.8	192.168.2.6	0x2447	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:40.909358978 CET	8.8.8.8	192.168.2.6	0xe5d2	No error (0)	www.google.co.uk		142.251.209.3	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:41.062252045 CET	8.8.8.8	192.168.2.6	0x5b9	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:41.143996000 CET	8.8.8.8	192.168.2.6	0x99e3	No error (0)	j.clarity.ms	vmss-clarity-ingest-eus2-d.eastus2.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:41.590423107 CET	8.8.8.8	192.168.2.6	0x48c7	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:41.590423107 CET	8.8.8.8	192.168.2.6	0x48c7	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:41.590423107 CET	8.8.8.8	192.168.2.6	0x48c7	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:42.226947069 CET	8.8.8.8	192.168.2.6	0x8bc2	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:42.226947069 CET	8.8.8.8	192.168.2.6	0x8bc2	No error (0)	star-mini.c10r.facebook.com		157.240.253.35	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:42.746944904 CET	8.8.8.8	192.168.2.6	0x1ed9	No error (0)	collect.fefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:42.746944904 CET	8.8.8.8	192.168.2.6	0x1ed9	No error (0)	collect.fefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.074522018 CET	8.8.8.8	192.168.2.6	0xf5bc	No error (0)	image-optimizer.salessquad.co.uk		167.114.156.181	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.217.135.136	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.216.219.248	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.217.36.30	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.217.49.6	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.217.230.48	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 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		54.231.199.184	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		52.216.108.197	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.076103926 CET	8.8.8.8	192.168.2.6	0xdc9e	No error (0)	s3.amazonaws.com		54.231.201.184	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.078604937 CET	8.8.8.8	192.168.2.6	0x6a8b	No error (0)	searchserverapi.com		184.164.145.37	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.082590103 CET	8.8.8.8	192.168.2.6	0x5b2d	No error (0)	chimpstatic.com		184.28.113.54	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.083681107 CET	8.8.8.8	192.168.2.6	0xed89	No error (0)	easy-image-mapper.herokuapp.com		54.205.8.205	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.083681107 CET	8.8.8.8	192.168.2.6	0xed89	No error (0)	easy-image-mapper.herokuapp.com		18.211.231.38	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.083681107 CET	8.8.8.8	192.168.2.6	0xed89	No error (0)	easy-image-mapper.herokuapp.com		54.235.77.118	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.083681107 CET	8.8.8.8	192.168.2.6	0xed89	No error (0)	easy-image-mapper.herokuapp.com		174.129.128.48	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:43.085827112 CET	8.8.8.8	192.168.2.6	0x2cc3	No error (0)	c.clarity.ms	c.msn.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:43.085827112 CET	8.8.8.8	192.168.2.6	0x2cc3	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:46.249597073 CET	8.8.8.8	192.168.2.6	0x8b9b	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.773791075 CET	8.8.8.8	192.168.2.6	0x5dc1	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:51.781979084 CET	8.8.8.8	192.168.2.6	0xce32	No error (0)	searchanise-ef84.kxcdn.com	p-chzh00.kxcdn.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:33:51.781979084 CET	8.8.8.8	192.168.2.6	0xce32	No error (0)	p-chzh00.kxcdn.com		94.126.16.223	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.802186012 CET	8.8.8.8	192.168.2.6	0x9d1c	No error (0)	json.geoiplookup.io		104.26.8.192	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.802186012 CET	8.8.8.8	192.168.2.6	0x9d1c	No error (0)	json.geoiplookup.io		172.67.68.68	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:51.802186012 CET	8.8.8.8	192.168.2.6	0x9d1c	No error (0)	json.geoiplookup.io		104.26.9.192	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:54.586947918 CET	8.8.8.8	192.168.2.6	0x591c	No error (0)	telemetrics.klaviyo.com		13.224.103.75	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:54.586947918 CET	8.8.8.8	192.168.2.6	0x591c	No error (0)	telemetrics.klaviyo.com		13.224.103.58	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:54.586947918 CET	8.8.8.8	192.168.2.6	0x591c	No error (0)	telemetrics.klaviyo.com		13.224.103.124	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:54.586947918 CET	8.8.8.8	192.168.2.6	0x591c	No error (0)	telemetrics.klaviyo.com		13.224.103.118	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:56.003906012 CET	8.8.8.8	192.168.2.6	0xdedb	No error (0)	d3k81ch9hvuctc.cloudfront.net		13.224.103.69	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:56.003906012 CET	8.8.8.8	192.168.2.6	0xdedb	No error (0)	d3k81ch9hvuctc.cloudfront.net		13.224.103.58	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:33:56.003906012 CET	8.8.8.8	192.168.2.6	0xdedb	No error (0)	d3k81ch9hvuctc.cloudfront.net		13.224.103.77	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 18:33:56.003906012 CET	8.8.8.8	192.168.2.6	0xdedb	No error (0)	d3k81ch9hvuctc.cloudfront.net		13.224.103.85	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:18.468684912 CET	8.8.8.8	192.168.2.6	0x7aa8	No error (0)	cdn.shopify.com		23.227.60.200	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:18.704304934 CET	8.8.8.8	192.168.2.6	0xe77f	No error (0)	api.feefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:18.704304934 CET	8.8.8.8	192.168.2.6	0xe77f	No error (0)	api.feefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:35.825032949 CET	8.8.8.8	192.168.2.6	0x2551	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:35.921663046 CET	8.8.8.8	192.168.2.6	0x718	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:36.455141068 CET	8.8.8.8	192.168.2.6	0xea4	No error (0)	cdn.shopify.com		23.227.60.200	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.506529093 CET	8.8.8.8	192.168.2.6	0x415d	No error (0)	monorail-edge.shopifysvc.com		185.146.173.20	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.654360056 CET	8.8.8.8	192.168.2.6	0xe135	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:38.654360056 CET	8.8.8.8	192.168.2.6	0xe135	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.740840912 CET	8.8.8.8	192.168.2.6	0x22d0	No error (0)	linwoodfabric.com		23.227.38.65	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.741636038 CET	8.8.8.8	192.168.2.6	0x3b5	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:38.741636038 CET	8.8.8.8	192.168.2.6	0x3b5	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:38.741636038 CET	8.8.8.8	192.168.2.6	0x3b5	No error (0)	dualstack.pinterest.map.fastly.net		146.75.116.84	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.937331915 CET	8.8.8.8	192.168.2.6	0x386f	No error (0)	register.feefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:38.937331915 CET	8.8.8.8	192.168.2.6	0x386f	No error (0)	register.feefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.187169075 CET	8.8.8.8	192.168.2.6	0x43f2	No error (0)	stats.g.doubleclick.net		142.251.31.155	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.187169075 CET	8.8.8.8	192.168.2.6	0x43f2	No error (0)	stats.g.doubleclick.net		142.251.31.154	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.187169075 CET	8.8.8.8	192.168.2.6	0x43f2	No error (0)	stats.g.doubleclick.net		142.251.31.156	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.187169075 CET	8.8.8.8	192.168.2.6	0x43f2	No error (0)	stats.g.doubleclick.net		142.251.31.157	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.726605892 CET	8.8.8.8	192.168.2.6	0x3028	No error (0)	api.feefo.com		104.16.75.76	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:39.726605892 CET	8.8.8.8	192.168.2.6	0x3028	No error (0)	api.feefo.com		104.16.138.15	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:44.683023930 CET	8.8.8.8	192.168.2.6	0xacb2	No error (0)	j.clarity.ms	vmss-clarity-ingest-eus2-d.eastus2.cloudapp.azure.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:34:49.481987953 CET	8.8.8.8	192.168.2.6	0x66a6	No error (0)	static.klaviyo.com	klaviyo-onsite.map.fastly.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 18:34:49.481987953 CET	8.8.8.8	192.168.2.6	0x66a6	No error (0)	klaviyo-onsite.map.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:49.481987953 CET	8.8.8.8	192.168.2.6	0x66a6	No error (0)	klaviyo-onsite.map.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:49.481987953 CET	8.8.8.8	192.168.2.6	0x66a6	No error (0)	klaviyo-onsite.map.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:34:49.481987953 CET	8.8.8.8	192.168.2.6	0x66a6	No error (0)	klaviyo-onsite.map.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)	false

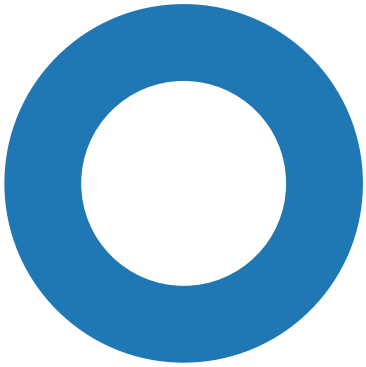
HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- linwoodfabric.com
- https:
  - cdn.shopify.com
  - static.klaviyo.com
  - api.feefo.com
  - shopapi.wyldcode.com
  - shop.app
  - static-tracking.klaviyo.com
  - register.feefo.com
  - www.clarity.ms
  - connect.facebook.net
  - monorail-edge.shopifysvc.com
  - s.pinimg.com
  - stats.g.doubleclick.net
  - fast.a.klaviyo.com
  - static-forms.klaviyo.com
  - cdn.linkedin.oribi.io
  - www.google.com
  - www.google.co.uk
  - www.facebook.com
  - collect.feefo.com
  - chimpstatic.com
  - image-optimizer.salessquad.co.uk
  - searchserverapi.com
  - s3.amazonaws.com
  - easy-image-mapper.herokuapp.com
  - searchanise-ef84.kxcdn.com
  - json.geoiplookup.io
  - telemetrics.klaviyo.com
  - d3k81ch9hvuctc.cloudfront.net
- a.nel.cloudflare.com

Statistics

Behavior

chrome.exe
chrome.exe
chrome.exe



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6092, Parent PID: 2588

General

Target ID:	0
Start time:	18:33:28
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" --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: 2148, Parent PID: 6092

General

Target ID:	1
Start time:	18:33:29
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=1948 --field-trial-handle=1772,i,16511072594903400105,15930520381033309042,131072 --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

Analysis Process: chrome.exe PID: **4732**, Parent PID: **2588**

General

Target ID:	2
Start time:	18:33:30
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" "http://mailto:Warrick@linwoodfabric.com
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