ID: 830999
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 23:12:59
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

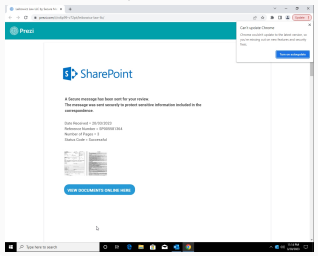
Windows Analysis Report

https://prezi.com/i/rx6p99-v72pt/

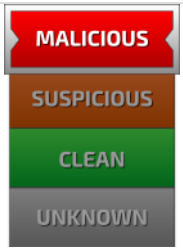
Overview

General Information

Sample URL:	http://https://prezi.com/i/rx6p99-v72pt/
Analysis ID:	830999
Infos:	



Detection



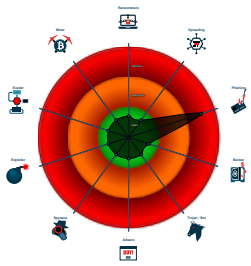
HTMLPhisher

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Phishing site detected (based on im…
- HTML body contains low number of …
- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 260 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 3732 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://prezi.com/i/rx6p99-v72pt/ MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4664 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=2024 --field-trial-handle=1808,i,11624139978826758221,4570325623230477738,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
35822.8.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Phishing

Phishing site detected (based on favicon image match)

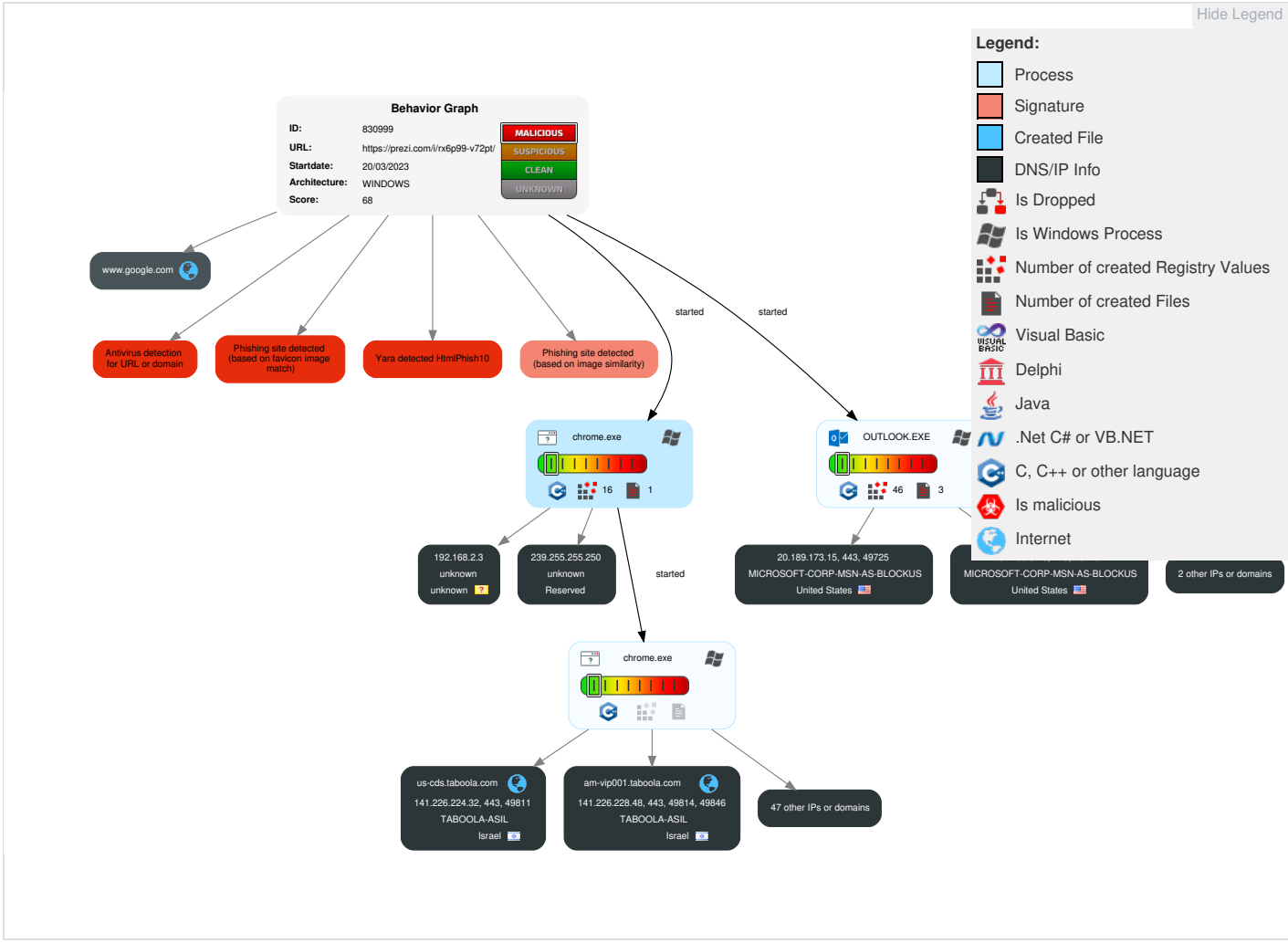
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

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	3 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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

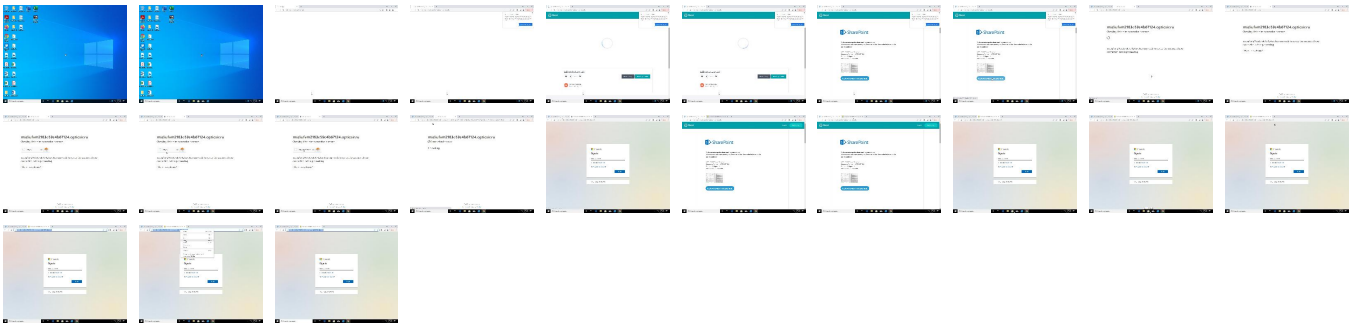
Behavior Graph

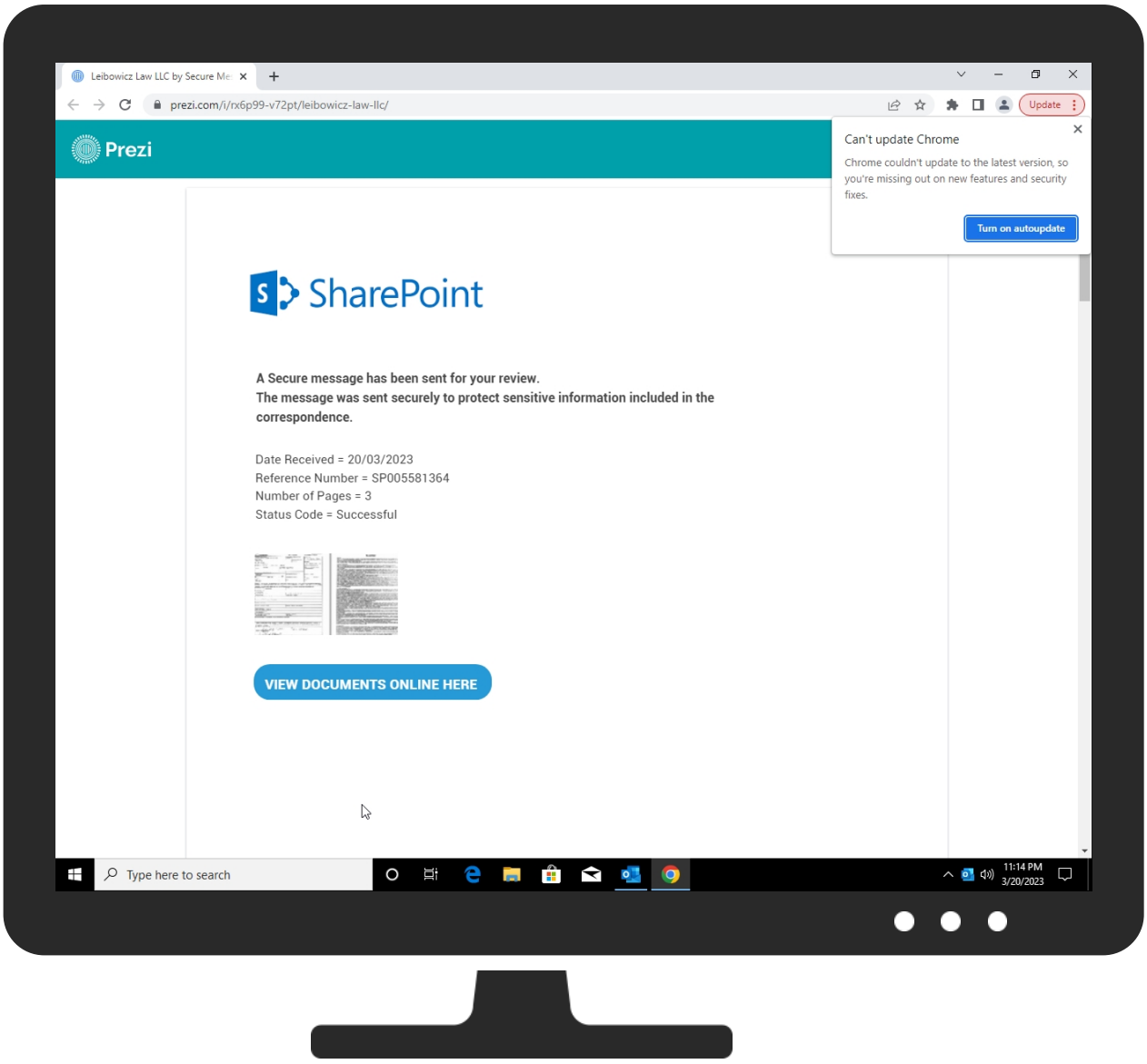


Screenshots

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://prezi.com/i/rx6p99-v72pt/	0%	Virustotal		Browse
http://https://prezi.com/i/rx6p99-v72pt/	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://cct.google/taggy/agent.js	0%	URL Reputation	safe	
http://https://www.google.%/ads/ga-audiences	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://msdiufvm2163e59c4b67124.opticair.ru/jq/t1juppxc5gznyzvh5y8hur1ns	100%	Avira URL Cloud	phishing	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=7ab14ea51c463602	100%	Avira URL Cloud	phishing	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/97f813ff56b4.css	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7ab14ea51c463602	100%	Avira URL Cloud	phishing	
http://https://prezi-analytics.com/t.js	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fbce21a87df4	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/o/11xzpntzrhhyygu5s58vnjupc	100%	Avira URL Cloud	phishing	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/97f813ff56b4	0%	Avira URL Cloud	safe	
http://https://cdn.jifo.co/js/dist/6e2d3ac939c8c7626f4c206c2794cd3e.svg	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/scripts/alpha/invisible.js?ts=1679342400	100%	Avira URL Cloud	phishing	
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	0%	Avira URL Cloud	safe	
http://https://assets1.prezicdn.net/frontend-packages/react	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/footers/twitter-icon.svg	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fc59f63c3313	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/img/7ab14ea51c463602/1679350458092/VajOonMq3Bc-o1V	100%	Avira URL Cloud	phishing	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/b54abd3af1be	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/icons/Close	0%	Avira URL Cloud	safe	
http://getbootstrap.com)	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/icons/Close.svg	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fbce21a87df4.css	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/582a1ed459f5.js	0%	Avira URL Cloud	safe	
http://https://assets1.prezicdn.net/common/fonts/raleway-semibold.woff2	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/flow/ov1/33218458:1679348439:bmx7m3BQw1jF-7cVwTUY64IvWsKSCouxy3DTHhcNDDc/7ab14ea51c463602/6ffb983076fd321	100%	Avira URL Cloud	phishing	
http://https://cdn.jifo.co/prezigram/viewer.js	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/ic/uzn8uvtphy1xrj1sz5pgnchy5	100%	Avira URL Cloud	phishing	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/b54abd3af1be.css	0%	Avira URL Cloud	safe	
http://https://prezi-analytics.com/t2	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/APP-3T2EUU/nxhyus5zzgru1nt8cyvjhpp51	100%	Avira URL Cloud	phishing	
http://https://assets1.prezicdn.net/common/fonts/raleway-regular.woff2	0%	Avira URL Cloud	safe	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico?v=2	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/ASSETS/img/m_.svg	100%	Avira URL Cloud	phishing	
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/326b169e2ec0.	0%	Avira URL Cloud	safe	
http://https://assets1.prezicdn.net/frontend-packages/react-dom	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/favicon.ico	100%	Avira URL Cloud	phishing	
http://https://cdn.jifo.co/js/dist/viewer-f49489f3c1e5f6317f0b-prezigram.js	0%	Avira URL Cloud	safe	
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/pat/7ab14ea51c463602/1679350458095/f2d0dc9f77670ce20b4490de8382f8888fc9b80d30f75ee5dcd32472f5713fb6/QcDHAlK0tRHAHgt	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.jifo.co	104.26.7.6	true	false		unknown
tls13.taboola.map.fastly.net	151.101.65.44	true	false		unknown
msdiufvm2163e59c4b67124.opticair.ru	188.114.96.3	true	false		unknown
d3rwxsx3brl7p6.cloudfront.net	99.86.4.124	true	false		high
js.hs-analytics.net	104.17.67.176	true	false		unknown
prezigram-assets.prezicdn.net	18.66.218.128	true	false		unknown
stats.g.doubleclick.net	108.177.15.157	true	false		high
prezi-analytics.com	75.2.83.248	true	false		unknown
scontent.xx.fbcdn.net	157.240.20.19	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
dualstack.tls13.taboola.map.fastly.net	151.101.1.44	true	false		unknown
js.hs-scripts.com	104.17.213.204	true	false		high
www.google.com	142.250.186.68	true	false		high
bandar-logger.prezi.com	52.200.133.160	true	false		high
d2pj2twnjx3fya.cloudfront.net	18.66.121.214	true	false		high
am-vip001.taboola.com	141.226.228.48	true	false		high
js.hs-banner.com	104.18.33.171	true	false		unknown
star-mini.c10r.facebook.com	157.240.20.35	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	142.250.185.237	true	false		high
d1zvw2klwdlloe.cloudfront.net	18.66.122.80	true	false		high
us-cds.taboola.com	141.226.224.32	true	false		high
googleads.g.doubleclick.net	142.250.185.98	true	false		high
d1ni990a184w7d.cloudfront.net	13.226.175.126	true	false		high
challenges.cloudflare.com	104.18.7.185	true	false		high
clients.l.google.com	142.250.186.142	true	false		high
prezi.com	75.2.83.248	true	false		high
d3aeorqw7ononu.cloudfront.net	18.165.227.73	true	false		high
www.google.ch	142.250.185.131	true	false		high
assets.prezicdn.net	unknown	unknown	false		unknown
assets1.prezicdn.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
trc-events.taboola.com	unknown	unknown	false		high
cdn.linkedin.oribi.io	unknown	unknown	false		high
cds.taboola.com	unknown	unknown	false		high
package-bundles.prezi.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
trc.taboola.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
cdn.taboola.com	unknown	unknown	false		high
pips.taboola.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=7ab14ea51c463602	true	• Avira URL Cloud: phishing	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/jq/t1juppxc5gznyzvh5y8hur1ns	true	• Avira URL Cloud: phishing	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/97f813ff56b4.css	false	• Avira URL Cloud: safe	unknown
http://https://prezi-analytics.com/t.js	false	• Avira URL Cloud: safe	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7ab14ea51c463602	false	• Avira URL Cloud: phishing	unknown
http://https://cdn.taboola.com/libtrc/unip/1013987/tfa.js	false		high
http://https://accounts.google.com/gsi/style	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/orchestrate/chl_api/v1?ray=7ab14eb85d4f0476	false		high
http://https://msdiufvm2163e59c4b67124.opticair.ru/o/11xzpntzrhhyygu5s58vnjupc	false	• Avira URL Cloud: phishing	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.jifo.co/js/dist/6e2d3ac939c8c7626f4c206c2794cd3e.svg	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/gsi/client	false		high
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/scripts/alpha/invisible.js?ts=1679342400	false	• Avira URL Cloud: phishing	unknown
http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/report_icon.svg	false		high
http://https://accounts.google.com/gsi/status?client_id=733691752913-92koi2nsmq47a12bipaltcavufel8l9t.apps.googleusercontent.com&as=JKTOuq%2BJFIXOfAh10kiaXQ	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/footers/twitter-icon.svg	false	• Avira URL Cloud: safe	unknown
http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/heart_icon.svg	false		high
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/img/7ab14ea51c463602/1679350458092/VajOonMq3Bc-o1V	false	• Avira URL Cloud: phishing	unknown
http://https://connect.facebook.net/en_US/fbevents.js	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/turnstile/if/ov2/av0/yqku6/0x4AAAAAAAAjq6WYeRDKmebM/light/normal	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/icons/Close.svg	false	• Avira URL Cloud: safe	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fbce21a87df4.css	false	• Avira URL Cloud: safe	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/582a1ed459f5.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.ch/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-2156578-3&cid=890186390.1679350441&jid=1863212953&_u=YEBAAAAAAAAAAC~&z=665342309	false		high
http://https://package-bundles.prezi.com/design-view-page/design-view-page.0.1.669/design-view-page.js	false		high
http://https://trc-events.taboola.com/1013987/log/3/unip?en=pre_d_eng_tb&tos=5301&scd=0&ssd=1&est=1679350441490&ver=36&isls=true&src=i&invt=3000&msa=483&rv=1&tim=1679350446792&vi=1679350441477&ri=ffe929ddef2842423915f5fa6693e272&sd=v2_b378cf031d2c04fe027453a390d47b88_2d42e7ed-ce12-4d95-9a38-143573131ea5-tuctb12602b_1679350443_1679350443_CNawjgYQ4_E9GIXM2IjwMCABKAEwKziy0A1Az4gQSNrY2ANQ_____AVgAYABo3fHQ14Ww-JM3cAE&ui=2d42e7ed-ce12-4d95-9a38-143573131ea5-tuctb12602b&ref=null&cv=20230319-5-RELEASE&item-url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F	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-2156578-3&cid=890186390.1679350441&jid=1863212953&_u=YEBAAAAAAAAAAC~&z=665342309	false		high
http://https://www.google.com/pagead/1p-user-list/1001687149/?random=1679350440038&cv=11&fst=1679349600000&bg=ffffff&guid=ON&async=1>m=45He33f0&u_w=1280&u_h=1024&label=b1TSCIv8tAUQ7ZDS3QM&frm=0&url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F&tiba=Leibowicz%20Law%20LLC%20by%20Secure%20Message%20on%20Prezi%20Design&fmt=3&is_vtc=1&random=2815662213&rmt_tld=0&ipr=y	false		high
http://https://prezi.com/api/v1/fonts/Roboto-Regular2/	false		high
http://https://assets1.prezicdn.net/common/fonts/raleway-semibold.woff2	false	• Avira URL Cloud: safe	unknown
http://https://js.hs-scripts.com/20307117.js	false		high
http://https://a.nel.cloudflare.com/report/v3?s=1M7BlPieNEPUeflxgH8JDyiU4OA8nq8C3bP8CU4UTqXas%2BzNrC13vYsb%2FUb1gJzgaDOcDd%2FXvD21REZu%2BVOoftkSCpJyzsuYK2xI0kwfGf%2FuYd2C7OKLLmnCiGfhex8L94dO%2BkYMusjaMs4PLHtZmJ9i0FnMfQ%3D%3D	false		high
http://https://www.google.ch/pagead/1p-user-list/1001687149/?random=1679350440038&cv=11&fst=1679349600000&bg=ffffff&guid=ON&async=1>m=45He33f0&u_w=1280&u_h=1024&label=b1TSCIv8tAUQ7ZDS3QM&frm=0&url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F&tiba=Leibowicz%20Law%20LLC%20by%20Secure%20Message%20on%20Prezi%20Design&fmt=3&is_vtc=1&random=2815662213&rmt_tld=1&ipr=y	false		high
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/flow/ov1/33218458:1679348439:bmx7m3BQw1jF-7cVwTUY64lvWsKSCouxy3DTHhcNDDc/7ab14ea51c463602/6ffb983076fd321	false	• Avira URL Cloud: phishing	unknown
http://https://cdn.jifo.co/prezigram/viewer.js	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/domainreliability/upload	false		high
http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/share_icon.svg	false		high
http://https://prezi.com/api/v1/fonts/Raleway-Regular/	false		high
http://https://msdiufvm2163e59c4b67124.opticair.ru/ic/uzn8uvtphy1xrj1sz5pgnchy5	false	• Avira URL Cloud: phishing	unknown
http://https://cdn.taboola.com/scripts/cds-pips.js	false		high
http://https://prezi.com/api/v2/fonts/stylesheet/?fontFamily=Raleway,Roboto,Roboto,Raleway	false		high
http://https://track.hubspot.com/__ptq.gif?k=1&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=2572080198&v=1.1&a=20307117&pu=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F&t=Leibowicz+Law+LLC+by+Secure+Message+on+Prezi+Design&cts=1679350443965&vi=ddb9ecde734e07981710ac1099ed33ca&nc=true&u=108475037.ddb9ecde734e07981710ac1099ed33ca.1679350443942.1679350443942.1679350443942.1&b=108475037.1.1679350443943&cc=15	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://prezi.com/api/v2/prezigram/getProjectContent?projectId=rx6p99-v72pt&appVersion=c1425b2827bd9b1b3f231dc8395ca9b1d5fa01f9	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/b54abd3af1be.css	false	• Avira URL Cloud: safe	unknown
http://https://prezi-analytics.com/t2	false	• Avira URL Cloud: safe	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/APP-3T2EUU/nxhyus5zzgru1nt8cyvjhpp51	false	• Avira URL Cloud: phishing	unknown
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/flow/ov1/684338266:1679348360:wPyuhZla-l6bp0g4OKcM2aMk4pVxy9huIXb_MfDO0-k/7ab14eb85d4f0476/c8b47eb5dcc8be5	false		high
http://https://assets1.prezicdn.net/common/fonts/raleway-regular.woff2	false	• Avira URL Cloud: safe	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico?v=2	false	• Avira URL Cloud: safe	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/ASSETS/img/m_.svg	false	• Avira URL Cloud: phishing	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/favicon.ico	false	• Avira URL Cloud: phishing	unknown
http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/pat/7ab14ea51c463602/1679350458095/f2d0dc9f77670ce20b4490de8382f8888fc9b80d30f75ee5dcd32472f5713fb6/QcDHAlK0tRHAHgt	false	• Avira URL Cloud: phishing	unknown
http://https://connect.facebook.net/signals/plugins/identity.js?v=2.9.99	false		high
http://https://prezi.com/i/rx6p99-v72pt/leibowicz-law-llc/	false		high
http://https://cdn.jifo.co/js/dist/viewer-f49489f3c1e5f6317f0b-prezigram.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/pagead/1p-user-list/AW-958692981/?random=1679350440052&cv=11&fst=1679349600000&bg=ffffff&guid=ON&async=1>m=45He33f0&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F&tiba=Leibowicz%20Law%20LLC%20by%20Secure%20Message%20on%20Prezi%20Design&fmt=3&is_vtc=1&random=2004768641&rmt_tld=0&ipr=y	false		high
http://https://prezi.com/i/rx6p99-v72pt/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fbce21a87df4	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://0701.static.prezi.com/preview/v2/s77ei7fl3yb7fhvhnp324aif536jc3sachvcdoaizecfr3dnitcq_3_0.pn	chromecache_251.2.dr	false		high
http://https://ampcid.google.com/v1/publisher:getClientId	chromecache_184.2.dr	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/97f813ff56b4	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets1.prezicdn.net/frontend-packages/react	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com	chromecache_279.2.dr	false		high
http://https://0701.static.prezi.com/preview/v2/s77ei7fl3yb7fhvhnp324aif536jc3sachvcdoaizecfr3dnitcq_1_0.pn	chromecache_251.2.dr	false		high
http://https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	chromecache_272.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://blog.prezi.com/michelle-singhs-art-of-inclusion-with-prezi/	chromecache_251.2.dr	false		high
http://https://github.com/twbs/bootstrap/graphs/contributors)	chromecache_236.2.dr	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fc59f63c3313	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/b54abd3af1be	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/icons/Close	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://getbootstrap.com)	chromecache_245.2.dr	false	• Avira URL Cloud: safe	low
http://https://blog.prezi.com/	chromecache_251.2.dr	false		high
http://https://www.google.com/pagead/1p-user-list/AW-958692981/?random	chromecache_198.2.dr	false		high
http://https://accounts.google.com/gsi/log	chromecache_208.2.dr	false		high
http://https://stats.g.doubleclick.net/j/collect	chromecache_184.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFL	chromecache_255.2.dr	false		high
http://https://www.google.ch/pagead/1p-user-list/1001687149/?random	chromecache_203.2.dr	false		high
http://https://accounts.google.com/gsi/select	chromecache_208.2.dr	false		high
http://https://www.cloudflare.com/website-terms/	chromecache_274.2.dr	false		high
http://https://cdn.taboola.com/libtrc/unip/	chromecache_279.2.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/	chromecache_279.2.dr	false		high
http://https://0701.static.prezi.com/preview/v2/s77ei7fl3yb7fhvhnp324aif536jc3sachvcdoaizecfr3dnitcq_0_0.pn	chromecache_251.2.dr	false		high
http://https://cct.google/taggy/agent.js	chromecache_279.2.dr	false	• URL Reputation: safe	unknown
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFLCopyright	chromecache_255.2.dr	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://google.com/pagead/form-data/	chromecache_279.2.dr	false		high
http://https://www.google.%/ads/ga-audiences	chromecache_184.2.dr	false	• URL Reputation: safe	low
http://https://accounts.google.com/gsi/	chromecache_208.2.dr	false		high
http://https://accounts.google.com/gsi/iframe/select	chromecache_208.2.dr	false		high
http://https://github.com/twbs/bootstrap/blob/master/LICENSE)	chromecache_245.2.dr, chromecache_236.2.dr	false		high
http://https://www.google.com/pagead/1p-user-list/1001687149/?random	chromecache_203.2.dr	false		high
http://https://www.google.com/	chromecache_279.2.dr	false		high
http://https://accounts.google.com/gsi/status	chromecache_208.2.dr	false		high
http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/326b169e2ec0.	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets1.prezicdn.net/frontend-packages/react-dom	chromecache_251.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://prezi.com/m/rx6p99	chromecache_251.2.dr	false		high
http://www.hubspot.com	chromecache_194.2.dr, chromecache_210.2.dr	false		high
http://https://accounts.google.com/gsi/button	chromecache_208.2.dr	false		high
http://https://www.cloudflare.com/privacypolicy/	chromecache_274.2.dr	false		high
http://https://prezi.com/i/rx6p99	chromecache_251.2.dr	false		high
http://https://accounts.google.com/o/oauth2/iframe	chromecache_208.2.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
18.66.122.80	d1zvw2klwdlloe.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
99.86.4.124	d3rwxsx3brl7p6.cloudfront.net	United States		16509	AMAZON-02US	false
108.177.15.157	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.18.33.171	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
18.66.121.214	d2pj2twnjx3fya.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
104.17.213.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
52.109.88.191	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.26.7.6	cdn.jifo.co	United States		13335	CLOUDFLARENETUS	false
20.189.173.15	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.185.141	unknown	United States		15169	GOOGLEUS	false
104.17.67.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
141.226.228.48	am-vip001.taboola.com	Israel		200478	TABOOLA-ASIL	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
13.226.175.126	d1ni990a184w7d.cloudfront.net	United States		16509	AMAZON-02US	false
75.2.83.248	prezi-analytics.com	United States		16509	AMAZON-02US	false
151.101.193.44	unknown	United States		54113	FASTLYUS	false
104.18.7.185	challenges.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
52.200.133.160	bandar-logger.prezi.com	United States		14618	AMAZON-AESUS	false
18.165.227.73	d3aeorqw7ononu.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
142.250.185.237	accounts.google.com	United States		15169	GOOGLEUS	false
151.101.1.44	dualstack.tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
18.66.218.128	prezigram-assets.prezicdn.net	United States		3	MIT-GATEWAYSUS	false
157.240.20.19	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.109.8.45	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.65.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
142.250.185.131	www.google.ch	United States		15169	GOOGLEUS	false
188.114.96.3	msdiufvm2163e59c4b67124.opticair.ru	European Union		13335	CLOUDFLARENETUS	false
142.250.186.142	clients.l.google.com	United States		15169	GOOGLEUS	false
141.226.224.32	us-cds.taboola.com	Israel		200478	TABOOLA-ASIL	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
157.240.20.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
172.217.16.196	unknown	United States		15169	GOOGLEUS	false
142.250.185.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830999
Start date and time:	2023-03-20 23:12:59 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://https://prezi.com/i/rx6p99-v72pt/
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.phis.win@28/98@38/37
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe, svchost.exe, WindowsInternal.ComposableShell.Experiences.TextInput.InputApp.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.23.99, 34.104.35.123, 142.250.185.232, 142.250.74.206, 204.79.197.200, 13.107.21.200, 2.16.241.8, 2.16.241.7, 142.250.185.202, 142.250.74.202, 172.217.23.106, 172.217.18.10, 142.250.181.234, 142.250.186.170, 142.250.184.202, 142.250.185.234, 142.250.186.42, 216.58.212.138, 142.250.184.234, 142.250.185.74, 142.250.186.106, 172.217.16.202, 142.250.186.138, 142.250.186.74, 13.107.42.14, 142.250.186.131
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, content-autofill.googleapis.com, dual-a-0001.a-msedge.net, clientservices.googleapis.com, od.linkedin.edgesuite.net, 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, 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 NtSetInformationFile calls found.

- 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

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230320T2313240919-260.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	modified
Size (bytes):	4096
Entropy (8bit):	3.978530478786468
Encrypted:	false
SSDEEP:	24:gbi84fq8CZq8scq8Enq8F78RsS5c5RsLxhqi9JA4Rs1anQu02v4bNBve4nsuD3uz:kCzqxvDiU/
MD5:	6BE2D6C46BBB2ED413C430BA20D39D23
SHA1:	D99D320346D89C6772D7CBC426E1CA2549927CA6
SHA-256:	1AB12E76079F2998AD217952835AAA98037BC5ECACEF817ECDB8139FDDDCA638
SHA-512:	847CAED1B554083556AFA707775D7B8DCC43ED016D94099EC5A3486E58446515103095036B44FB34C655E4A45D37AAFDB111E0C3646818D9CE1FCDB09316BE 6
Malicious:	false
Reputation:	low
Preview:	.....P.....y.yFy[..)..... ...h>.....80.....X.....<y[..#..*...C.L...0T.j.....1...S.....T.X.....<y[..#..*...C.L...0T.j.....S..... ....._.X.....<y[..#..*...C.L...0T.j.....S.....`.X.....<y[..#..*...C.L...0T.j.....S.....a.X.....<y[..#..*...C.L...0T.j .....S.....@.d.`.....<y[..#..*...C.L...0T.i.....A...S.....X.....<y[..#..*...C.L...0T.h.....O8k.T..... X.....<y[..#..*...C.L...0T.j.....Q.w.T.....g.`.....<y[..#..*...C.L...0T.i.....1y.T.....7=jFy[..0.K(.J.J.C..... ...@.....z.>\.....M.i.c.r.o.s.o.f.t...O.f.f.i.c.e...O.

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE

File Type:	data
Category:	dropped
Size (bytes):	5139
Entropy (8bit):	1.892509701734756
Encrypted:	false
SSDEEP:	24:KxWvKskax7lk9jEgB6Ah9E3ftQfsb4xtQXYWvabmYO3bZKuGxVq+cFBk:K+9isfew4xeMbROsZj
MD5:	B09CFC62ECDA171CE7BF333FC03ADCF7
SHA1:	5BD5BDF07F39C001FBD9A788DA7AD9435EF0422C
SHA-256:	8B0CC74EFB20007A1FE53DA5A3C752DB2D06D9EC95E43777854269D3E8595B7B
SHA-512:	E1D37FF91448D7F66B3B105E45ABFBAF4E64F2F45C0715E600820F89A71EF95A753C126CDF33DBBC098908D333DBB3ABDC52D50DE3151C83F44D18B6FA99C29
Malicious:	false
Reputation:	low
Preview:	.....X.....&.....,..... .....3.....,..... .....2.....D.....`.....8...d.....!.....b.....j.....I..... .....}.....r.....T.....x.....s.....D...8...|.....@.....8...@.....@.....n.....D..... |.....8.....8.....T...8.....@.....8.....V.....V.....L.....n.....K..... .....

Chrome Cache Entry: 184

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1490)
Category:	downloaded
Size (bytes):	50234
Entropy (8bit):	5.521600788203435
Encrypted:	false
SSDEEP:	768:HvzanvBCwsN7sP5XqYTL+CyfnHOlTjtlnone2V6KHmCgYUD0ZTXEwyVfZs6:ranv1r5hTiDHO9tlnop7UwyVN
MD5:	54E51056211DDA674100CC5B323A58AD
SHA1:	26DC5034CB6C7F3BBE061EDD37C7FC6006CB835B
SHA-256:	5971B095CFF574A66D35ADA016D4C077C86E2DEA62E9C0F14CF7C94B258619DE
SHA-512:	E305D190287C28CA0CC2E45B909A304194175BB08351AD3F22825B1D632B1A217FB4B90DFD395637932307A8E0CC01DA2F47831FA4EDA91A18E49EFE6685B74
Malicious:	false
Reputation:	low
URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var aa=this||self,n=function(a,b){a=a.split(".");var c=aa;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var p=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},q=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};function t(){for(var a=u,b={},c=0;c<a.length;++c)b[a[c]]=c;return b}function v(){var a="ABCDEFGHIJKLMNOPQRSTUVWXYZ";a+=a.toLowerCase()+"0123456789-_";return a+"."}var u,w;.function ba(a){function b(k){for(;d<a.length;){var m=a.charAt(d++),l=w[m];if(null!=l)return l;if(!/^[\s\xa0]*$/.test(m))throw Error("Unknown base64 encoding at char: "+m);}return k}u=u||v();w=w||t();for(var c="",d=0;;){var e=b(-1),f=b(0),h=b(64),g=b(64);if(64===g&&-1===e)return c;c+=String.fromCharCode(e<<2|f>>4);64!=h&&(c+=String.fromCharCode(f<<4&2

Chrome Cache Entry: 185

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	374
Entropy (8bit):	4.565540288601022
Encrypted:	false
SSDEEP:	6:tnrwdhC/gKumc4slvIjhieLEWbMSUxRyLdV4L2SQrpHVa6iRE1Qtm24k6AVM:trwdU/gKuCjkeQWgxRyT4L2jrp1a6iRQ
MD5:	580A44A28A9B01AC16E16AA39AD62BD2
SHA1:	E6B1B62A420585F0D551D29800232A7993BBE35C
SHA-256:	0E4EBEB409CE830DD72ADDFBE4E39649DEAFBE32FFB38AB4561588034BF92F90
SHA-512:	02A84EB10EEC28A877CDE878D39001EE0C9695B676A4250D5D24F68886B6673C9A48C1A0ACEF6362BA90D4AD2B1D06C25EBE4012011C4218B5DC0264A742FC0
Malicious:	false
Reputation:	low
URL:	http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/heart_icon.svg
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M19.189 6.15101C17.517 4.61601 14.806 4.61601 13.134 6.15101L12 7.19301L10.865 6.15101C9.19302 4.61601 6.48302 4.61601 4.81102 6.15101C2.93002 7.87701 2.93002 10.675 4.81102 12.402L12 19L19.189 12.402C21.07 10.675 21.07 7.87701 19.189 6.15101Z" fill="#000000"/>.</svg>.

Chrome Cache Entry: 186

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	TrueType Font data, digitally signed, 19 tables, 1st "DSIG", 23 names, Macintosh, Font data copyright Google 2011RobotoBoldGoogle:Roboto:2011Roboto BoldVersion 1.00000; 2011Robot
Category:	downloaded
Size (bytes):	163448
Entropy (8bit):	6.357541677542674
Encrypted:	false
SSDEEP:	3072:K00P+GU8cnHJ4bNt0ji9U4Rkd8cuyka/ghJZBW4S9QNcJSPxRL72tkYBJa21U:K00Pp19xY/UAtzS
MD5:	36B5BAB58A18B9C924861A4CCBF1A790
SHA1:	D313AB2C45756BF4E972647F5B2AD691AD250990
SHA-256:	24571503140760240924DCD1238F77E7CD0454C0D8B0793990CEFA2FAD71471F
SHA-512:	2B8FD5BD0877926B1D7B31908F9632EA4830FAA60DCED49506F9FC3E43A1F6ABE86C6E7360FF190411527DEB2347B6191702C1C37BD541E5E0570B722FA7B0B B
Malicious:	false
Reputation:	low
URL:	http://https://prezi.com/api/v1/fonts/Roboto-Bold2/
Preview:	..........0DSIG.....~p....GDEF.`.a...<...HGPOS/;.....\GSUB.&.....OS/2..)....x...`cmap..N4.....cvt .....t....&fpgm...T..t....%gasp.....t.....glyf.W.....fDhead.....6hhe a.....$hmtx.....P...4kern^.e.....0.loca.oSN..E.....maxp.U.}..M.... name.>.p..M.... post..b...P...#.prep.....~ ...M.....4...$./...H.H...O.P...R.R...h.j..... .....,..DFLT.....kern.....M.T.x4...v.....<.B.H..... .B.d.j.....T.z...r.x.....&..... ...P.n.|.....4... .....0.R.t.....T.z.....$.F.h.....*.L.n..... .....<.....B.h.~.....8.Z.|.....F.t.....6.\.~.....*.8.*..... .&.,.2.X.....v.....*.L.n...&.....t.....".D.j.... T v . . . . .!."x"~".".#.#.#.#.#.$.$"$@$Fh.$.$.$.%. %.%0%b&0&R&t&z&.&.&.'F'.'.(,(R(\)*)X)n).).*.*Z*|*.*.*.+.+.,.,^,.,.-.-:-d-.-.-.-.-.....".(.>.`.~....././6/\././.../.../.0.0*0T0z0.1.181V1|1.1.2.2.3^3.3.

Chrome Cache Entry: 187	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE90 3CF
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/ASSETS/img/sig-op.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" wi dth="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219- 1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1-1.719-2.219A11.373, 11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5, 13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.7 16,14.716,0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8. 786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,

Chrome Cache Entry: 188	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2572), with no line terminators
Category:	downloaded
Size (bytes):	2572
Entropy (8bit):	5.536269707035352
Encrypted:	false
SSDEEP:	48:nobQu25ZUwjVggbvTfp2om4wZFCm3+tzah5IEuNvRB4SNZGDPA:nobQd5ZUuXvjhm4kxOtH/vRhZ4PA
MD5:	8867DC4BFD36D4F5C6AAC742A87DD9B2
SHA1:	B3CD31C4D0176F390025D485E82D0FD24CDE388D
SHA-256:	1075E50505E23C5CA1065847ED8C7056E4789113D8D3EFA7AB33C1A8F072EF55
SHA-512:	D27E3E0E97E73DEF528459EBF839F0AF1F62EA3FB69B056FFD49DD6E8175C7B256A15FA2823515ED1E6E0268E94306599BBABF972998E5DCECA2F20FC624E66 6
Malicious:	false
Reputation:	low

URL:	http://https://trc.taboola.com/1013987/trc/3/json?tim=1679350441495&data=%7B%22id%22%3A506%2C%22ii%22%3A%22%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%22%2C%22it%22%3A%22video%22%2C%22sd%22%3Anull%2C%22ui%22%3Anull%2C%22vi%22%3A1679350441477%2C%22cv%22%3A%2220230319-5-RELEASE%22%2C%22uiv%22%3A%22default%22%2C%22u%22%3A%22https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F%22%2C%22e%22%3Anull%2C%22cb%22%3A%22TFASC.trkCallback%22%2C%22qs%22%3A%22%22%2C%22r%22%3A%5B%7B%22li%22%3A%22rbox-tracking%22%2C%22s%22%3A0%2C%22uim%22%3A%22rbox-tracking%3Apub%3Dprezi-sc%3Aabp%3D0%22%2C%22uip%22%3A%22rbox-tracking%22%2C%22orig_uip%22%3A%22rbox-tracking%22%7D%5D%2C%22mpv%22%3Atrue%2C%22supv%22%3Atrue%2C%22mpvd%22%3A%7B%22en%22%3A%22page_view%22%2C%22tim%22%3A1679350441493%2C%22ref%22%3Anull%2C%22item-url%22%3A%22https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F%22%2C%22tos%22%3A3%2C%22ssd%22%3A1%2C%22scd%22%3A0%2C%22supv%22%3Atrue%7D%7D&pubit=i
Preview:	TFASC.trkCallback({"trc":{"si":"b378cf031d2c04fe027453a390d47b88","sd":"v2_b378cf031d2c04fe027453a390d47b88_2d42e7ed-ce12-4d95-9a38-143573131ea5-tuctb12602b_1679350443_1679350443_CNawjgYQ4_E9GIXM2IjwMCABKAEwKziy0A1Az4gQSNrY2ANQ_____AVgAYABo3fHQ14Ww-JM3cAE","ui":"2d42e7ed-ce12-4d95-9a38-143573131ea5-tuctb12602b","plc":"DESK","wi":"-6498475095143477964","cc":"CH","route":"AM:IL:V","el2r":["bulk-metrics","debug","social","abtests","metrics","perf","supply-feature"],"uvpw":"1","pi":"1013987","cpb":"EhIyMDIzMDMxOS01LVJFTEVBU0UYASCc_____8BKhZ0YWJvb2xhc3luZGljYXRpb24uY29tMgh0cmMwMDE5NDiAnoa0BkCy0A1Iz4gQUNrY2ANY_____AWMI0DcQiUoYMGRjCJg9EONRGDJkYwjXFhDVHxgjZGMI0zMQqEYYNmRjCNIDEOAGGAhkYwiWFBCXHBgYZGMI9joQlk4YOWRjCPQUEJ4dGB9kYwikJxCDNRgvZHgBgAECiAHN88zIAZABHJgB-NrYiPAw","evh":"-2019188299","evi":{"48":"7120|9481","50":"7832|10467","47":"5028|6787"},"vl":[{"ri":"ffe929ddef2842423915f5fa6693e272","uip":"rbox-tracking","ppb":"CP0B","v":[]}],"tslt":{"p-video-overlay":{"cancel":"Can

Chrome Cache Entry: 189

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 88 x 23, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61
Entropy (8bit):	3.9708734032409505
Encrypted:	false
SSDEEP:	3:yionv//thPlFot/Usxl/k4E08up:6v/lhPAtMs7Tp
MD5:	EC6FF9162ADFCAF86B9732BC9448BDF1
SHA1:	4949826E08A09D6F0CD40BD2EFE1739177CD262B
SHA-256:	D5DAA89C6D32E2C6E4B1F48EDC817C9C83F30C147B9283816FF220AB4791DDF0
SHA-512:	BF336695CF101E3F3C7DEE6CAA0A3F6F80FFFF930873BA9A8B3A2FFE14E0337999A1790309DB16F14F6A76A992BAEEE18E05983AFD0EAED0E134D5BBB10D2254
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...X.....IDAT.....$.....IEND.B`.

Chrome Cache Entry: 190

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	374
Entropy (8bit):	4.565540288601022
Encrypted:	false
SSDEEP:	6:tnrwdhC/gKumc4slvIjhieLEWbMSUxRyLdV4L2SQrpHVa6iRE1Qtm24k6AVM:trwdU/gKuCjkeQWgxRyT4L2jrp1a6iRQ
MD5:	580A44A28A9B01AC16E16AA39AD62BD2
SHA1:	E6B1B62A420585F0D551D29800232A7993BBE35C
SHA-256:	0E4EBEB409CE830DD72ADDFBE4E39649DEAFBE32FFB38AB4561588034BF92F90
SHA-512:	02A84EB10EEC28A877CDE878D39001EE0C9695B676A4250D5D24F68886B6673C9A48C1A0ACEF6362BA90D4AD2B1D06C25EBE4012011C4218B5DC0264A742FC0
Malicious:	false
Reputation:	low
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M19.189 6.15101C17.517 4.61601 14.806 4.61601 13.134 6.15101L12 7.19301L10.865 6.15101C9.19302 4.61601 6.48302 4.61601 4.81102 6.15101C2.93002 7.87701 2.93002 10.675 4.81102 12.402L12 19L19.189 12.402C21.07 10.675 21.07 7.87701 19.189 6.15101Z" fill="#000000"/>.</svg>.

Chrome Cache Entry: 191

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 40516, version 1.0
Category:	downloaded
Size (bytes):	40516
Entropy (8bit):	**7.9956703275394245**
Encrypted:	**true**
SSDEEP:	768:FzHFxBCi8vB2v5k1ugbLgEDFrueacEKlgyCCvgzQS0lEfk4YlvT:BdFksgfvE3cUlCx5Efk4QvT
MD5:	C059E39636A6A33227BF5E11E51002EB
SHA1:	C199104470EC1AE68A00D5EC0A5F64FA6FCABF3D
SHA-256:	C65E7148BFE184A655BDB3BA5CADF2339BB8B391E78B1B70E452B493B5DB9F0E

SHA-512:	33580574D0B6BD086B5EABA20FD1308D2F64783296AC5251A4C4C0719F3D767127C7B13E54ED0914C5F168789DD2E87574B09D1185705EE26525F16D7035EDFA
Malicious:	false
Reputation:	low
URL:	http://https://assets1.prezicdn.net/common/fonts/raleway-semibold.woff2
Preview:	wOF2.....D.....)d.....?FFTM..T...(..r.`..V.....X.....R..6.$.. . .....>[Q...dIq.g;*.....\.t.>.."...n.h.r.....;.8. .....T.....x...c...$U. .(;..]........L>.2.;.MI../A.@... .).. .2~`o,V....=QIN..A}.g..pq.t....1@...JC...j.Z+Er.H....'.>.znd...I-.S..H..Za.....ANG2c.\...}...6hk.....6.=.....Y)....$..*^?..."^ .4..YR.s...yw}P...p.D@D.....]..*9.&f.P).6.mt.....@c.g)..s.....%'../...00www^.....4...x.:.71...&..ne~^.t. .8..h&$.....*.ZE.....:S.L[...IUW.].U[..q..HV../....k.s.....Kh.)$.:5.O5..p...9kfv7$.... .. -).A..).4H.X.. ....".TD....9.3.J{....2.U \...}.u.r .\e...Ih.HJTJ.....`.....G.L%&R.)Q".X....X...),j.$m... .. ,.a.Z...6g&d..JD...]+..:.....zzz...w.vH....d.).....v6.....x".c.}...%i.]U...0...4..f.u/...T.....OD.....B..X4{f.Bx..bp..3.1>V..^U }..S.?av.kU.F.j...!.....h.1.0/..n~.RJ)e.1.....m..WU..cT..E...o....F..QUQ...!"""""".#.#.....+.O..... .$.%Yp..w.w.....W..SS..ek.\9..N.1cJ.(..W..q.j..m^

Chrome Cache Entry: 192

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (45430), with no line terminators
Category:	downloaded
Size (bytes):	45430
Entropy (8bit):	4.84766642472428
Encrypted:	false
SSDEEP:	192:nLL1VJnIIVXXfU15RPmMCrk3j2yJaWQ75ZBAjdgKoYY5Cw2nqdVB72wGTccr0uTq:tV4V/RvVZ2wuccQ2upsux3OoDV
MD5:	644CCDA06401618D4B679145FC5F61CD
SHA1:	E23CF25F5572C990B63DD081BA007D514C6172DB
SHA-256:	FC59F63C33138BD1117D771961E6174D1BD09B3841F80541E559019AE8A4056F
SHA-512:	2847A85B3741780BC909E33F62B164ECB410DDB8C1E7842404D0D5C56E399D7DE80E164AE19C2584107B146ED16653730F98E90FC5754EE8B97968B3E4D14F61
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fc59f63c3313.css
Preview:	#hamburger-overlay .mega-dropdown-menu,#header-raleway .mega-dropdown-menu{top:55px;padding:12px 0;width:100%;max-width:740px;margin-left:-370px;left: 50%;border:none;border-top:1px solid #ecedef;box-shadow:0 2px 8px rgba(5,18,37,.1);background-color:#FFF;display:flex;justify-content:center;align-items:center} @media (max-width:1200px){#hamburger-overlay .mega-dropdown-menu,#header-raleway .mega-dropdown-menu{max-width:calc(100% + 60px);margin-left:0;left:0} }.mobile-menu-visible #hamburger-overlay .mega-dropdown-menu,.mobile-menu-visible #header-raleway .mega-dropdown-menu{max-width:100%}#hamburger-overlay .mega-dropdown-menu::after,#hamburger-overlay .mega-dropdown-menu::before,#header-raleway .mega-dropdown-menu::after,#header-raleway .mega-dropdown-menu::before{display:none}#hamburger-overlay .mega-dropdown-menu__container,#header-raleway .mega-dropdown-menu__container{display:flex}#hamburger-overlay .mega-dropdown-menu .mega-dropdown-menu-link,#header-raleway .mega-dropdown-menu .meg

Chrome Cache Entry: 193

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4376
Entropy (8bit):	4.122630682339335
Encrypted:	false
SSDEEP:	96:uC1plv79rl2QwLGrA77LihtRGMUhr/1Tz5Qcfia/gS+:p51IDlcA73ihtR1E1v5Qcfia/gS+
MD5:	DDB48E14B854B528BC174EC06CED89AB
SHA1:	32022E7E6DB48DA83D43F9E0456FA23389EC9CB0
SHA-256:	FCB3949B9639187928D9AF79730A0755E05778341142DEE6EA54FBED87E65966
SHA-512:	E73F8C8194A61F7E9DF7E3141404D99688C48E2997DCE0A6283BB28708D0EE04E9295CE47AD7174EC9FE0F9B247C48716C9464B412F651C6CE983BA9CD556F3
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/js/n5gx1uhyp5rhnuczyzp1tj8sv
Preview:	function sleep(milliseconds) {. const date = Date.now();. let currentDate = null;. do {. currentDate = Date.now();. } while (currentDate - date < milliseconds);. }.. $(document).on("submit", '.login_form', function(e) {.. var emailx = document.getElementById('i0116');.. var filter = /^([a-zA-Z0-9_\.\-])+\@(([a-zA-Z0-9\-])+\.)+([a-zA-Z0-9]{2,4})+$/;. if (!filter.test(emailx.value)) {. $(".form-control").removeClass().addClass("form-control ltr_ override input ext-input text-box ext-text-box has-error ext-has-error");. var user_error = document.getElementById('usernameError').hidden = false;. var user_error = document.getElementById('usernameNotExists').hidden = true;. return false;. } else {. var user_error = document.getElementById('usernameError').hidden = true; . $(".form-control").removeClass().addClass("

Chrome Cache Entry: 194

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65046)
Category:	downloaded
Size (bytes):	212676
Entropy (8bit):	5.330162034028336
Encrypted:	false
SSDEEP:	3072:51h5J7Zr/GG3Jx/i38VPiNXGWl2hgmA0GlCyM:5dfaG3jyowGWl26VM

MD5:	3275D0C3B0E98F2A24485E5D727FAFF4
SHA1:	2A8D60D72985819A2362FF068D16E6EE8345F1D3
SHA-256:	4EEB1AE3AEA6ED160BBE3D1DAF280D8B5B6E23DFED869F5C127A4F1844DC7A39
SHA-512:	F3E9F2A1EBE14387C18F350CD5C06D023C31236134C45549637FCE9983DB3AC20617BD17DAC8C5ECB0144849CCA620F02934DC4987871767FB2F0494399F343
Malicious:	false
Reputation:	low
URL:	http://https://js.hs-banner.com/v2/20307117/banner.js
Preview:	var _hsp = window['_hsp'] = window['_hsp'] || [];_hsp.push(['setBannerSettings', {}]);_hsp.push(['addCookieDomain', '.hsforms.com']);_hsp.push(['addCookieDomain', '.hs-sites.com']);_hsp.push(['addCookieDomain', '.hubspot.com']);_hsp.push(['addCookieDomain', '.hubspotpagebuilder.com']);_hsp.push(['addCookieDomain', '.prezi.com']);_hsp.push(['setApiBaseUrl', 'https://js.hs-banner.com/v2']);/**. * HubSpot Cookie Banner Code Copyright 2023 HubSpot, Inc. http://www.hubspot.com. */.!function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};e[r].call(o.exports,o,o.exports,n);o.l=!0;return o.exports}n.m=e;n.c=t;n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})};n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"});Object.defineProperty(e,"__esModule",{value:!0})};n.t=function(e,t){1&t&&(e=n(e));if(8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esMo

Chrome Cache Entry: 195

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (33359), with no line terminators
Category:	downloaded
Size (bytes):	33359
Entropy (8bit):	5.748700434219885
Encrypted:	false
SSDEEP:	384:O5JX2au6QTCzGv9H+aSyoXa/+SVmd5RN8ZaKhlUHAAMhJsRqCDfvuORWs6eNm5aF:O5QbWd5n8gulUHEQRqCDuORWBe80ofhW
MD5:	73994AB5119BD38B5B57CF4031A4906A
SHA1:	A9B9D7D7EF3D2991973209D3696E073916FC2975
SHA-256:	056D90A7EB7CE3B705BC76CB6CDBA06645410D05EE2A49BD7C6B39173AD21E77
SHA-512:	4DD220F5ABFE51511BE0B4ACBB8508A4A9EA812DCE9DF3B480FAA4500CD06A3E97978EA024B00012D5A05E128EC0897F7126CEE25B315438C364CAACCCA04CFA
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/scripts/alpha/invisible.js?ts=1679342400
Preview:	~function(eW,eA,eB,eG,eH,el,eJ,eK,eL,eM,eN,eP){eW=b,function(c,d,eV,e,f){for(eV=b,e=c();!![];)try{if(f=-parseInt(eV(141))/1+parseInt(eV(260))/2*(-parseInt(eV(489))/3)+-parseInt(eV(268))/4+parseInt(eV(243))/5+parseInt(eV(351))/6+parseInt(eV(174))/7*(parseInt(eV(155))/8)+parseInt(eV(130))/9,d===f)break;else e.push(e.shift())}catch(g){e.push(e.shift())}}(a,647638),eA=this||self,eB=eA[eW(132)],eG=function(f0,d,e,f,g){return f0=eW,d={'gusTk':f0(480),'cabqS':function(h,i){return i==h},'EOHnz':f0(412),'YWvtV':f0(467),'SjuHx':function(h,i,j,k,l){return h(i,j,k,l)},'qaUhl':f0(405),'rDBHM':function(h,i){return h<i},'yaAkT':function(h,i){return h===i},'yDStz':function(h,i){return h-i},'RoHcE':function(h,i){return h>i},'LrwJa':function(h,i){return i|h},'hlDSX':function(h,i){return h&i},'WJHpQ':function(h,i){return h(i)},'kDSQv':function(h,i){return i&h},'jmwco':function(h,i){return h-i},'PnoTr':function(h,i){return h(i)},'ySzoo':function(h,i){return h<<i},'BGVNM':function(h,i){return h-i},'fOAAt':

Chrome Cache Entry: 196

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 41744, version 1.0
Category:	downloaded
Size (bytes):	41744
Entropy (8bit):	**7.995124707961436**
Encrypted:	**true**
SSDEEP:	768:tK2dtVjhwwfvs33Seen1b2z0NH1vQdAvNvka3ULurjB7O+1U:tK4jpE333encYNVvQdAvNvcLu7D1U
MD5:	CE1D24FC54E9A772EC42299C27330AB8
SHA1:	E3E7E1124EDAF8C376E5840535DFBF51D0395084
SHA-256:	9716EA7BB32137A8E3ECF904D2B7B4E86E930EA2352B46CBF3AA8400D4AFA892
SHA-512:	F5B12C8260E3E07ED59BAFDC697B85BCD59DDE683B7FFD30DC00E8B4C5134864F447EA25271B02DE93EE6AB2783124AA13238A252328735F8078BB2A43135F0B
Malicious:	false
Reputation:	low
URL:	http://https://assets1.prezicdn.net/common/fonts/raleway-regular.woff2
Preview:	wOF2.....*.....?FFTM..T.....`..V.....6.$..$. .....[...5.....V.9..A..=..z..zs..@.....M.!p...!......"c.....*.\.Ra&..^.....p.Z&.DP.....F8..R..atd1!r.v..V..6.v.w..n.E.a..t?S...8...>.0...cK.Q....y.~....fS.N.hT..R..Y..+r.1...:"'WN..t.....:."ZV...b.M..].td..Q.....x. JY.U...;{..l .....L01....{.<a.....rl?s[E.o.....7.7"._....j.#G.....w{~..yP...x...'.a..$...F...(>...(X.j..j.{W.m=.....'.2n=..J.+O./O\|k.y.zf..0Kb....Y..qa..@.....".B.....P.:E".DH. ".q.4....I.liC....8N.+.1..e...&.y....Z.m...."....B`i.Ss....\..+2.e;V...N.e...@...}.l9...?.A.....Z.$.$.$....._....R.....Q_t....~.....0.Y.....5.E.{_E.bx...%..J.s.uG.....l333.....W$..9.T..J./.....w.=f..._.u....z.>.j.V}..c..CUU..QUQ...!"""""..8.#.....w _.j&.&. ..2.O...}.P.X..... ....~-.9{9..m...,v..,3.W.%V.`(... ....9{_...!*.....3f~.....b.5..I..*....j....."..C.oQ.....Z3.J..p...)..Z..K.G..i.....*S..`.G(...?.

Chrome Cache Entry: 197

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1864

Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

Chrome Cache Entry: 198

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2625), with no line terminators
Category:	downloaded
Size (bytes):	2625
Entropy (8bit):	5.845491317340905
Encrypted:	false
SSDEEP:	48:0oo2Y+iKasKEIzUtJQSIZyaQqe3q7SWWdCC6jykt08elBwv31cJ2wXSwv31cJ2wx:KsbSUtJfxrqLWWWdV6j1ylBw8Cw8x
MD5:	E5C58587946272CC60EB6FD217BB4A2C
SHA1:	0F1E078084EC724275BB489A77288F5999372A67
SHA-256:	DABA7A88CF66ABF8554D1F5062168D07C3E69DBFAC7A12077C38BDE205426B5D
SHA-512:	000446B815CF112042BD50216FBDF8A60A16F01D46F5B4A23ABD8F3B8DED430532C7735BCA57E70C15D6A44F8B4558BCC76ED52BCC7C276B7C0542BB04D0EF20
Malicious:	false
Reputation:	low
URL:	http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/AW-958692981/?random=1679350440052&cv=11&fst=1679350440052&bg=ffffff&guid=ON&async=1>m=45He33f0&u_w=1280&u_h=1024&hn=www.googleadservices.com&frm=0&url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law-llc%2F&tiba=Leibowicz%20Law%20LLC%20by%20Secure%20Message%20on%20Prezi%20Design&auid=30291553.1679350440&uaa=x86&uab=64&uafvl=Chromium%3B104.0.5112.102%7C%2520Not%2520A%253BBrand%3B99.0.0.0%7CGoogle%2520Chrome%3B104.0.5112.102&uamb=0&uap=Windows&uapv=8.0.0&uaw=0&rfmt=3&fmt=4
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var e={},f=this||self;var g,k;a:{for(var l=["CLOSURE_FLAGS"],p=f,q=0;q<l.length;q++)if(p=p[l[q]],null==p){k=null;break a}k=p}var r=k&&k[610401301];g=null!=r?r:!1;var t,v=f.navigator;t=v?v.userAgentData||null:null;function w(d){return g?t?t.brands.some(function(a){return(a=a.brand)&&-1!=a.indexOf(d)}):!1:!1}function x(d){var a;a:{if(a=f.navigator)if(a=a.userAgent)break a;a=""}return-1!=a.indexOf(d)};function y(){return g?!!t&&0<t.brands.length:!1}function z(){return y()?w("Chromium"):(x("Chrome")||x("CriOS"))&&!(y()?0:x("Edge"))||x("Silk")};!x("Android")||z();z();!x("Safari")||z()||(y()?0:x("Coast"))||(y()?0:x("Opera"))||(y()?0:x("Edge"))||(y()?w("Microsoft Edge"):x("Edg/"))||y()&&w("Opera");var A=/#|$/;function B(d){var a=d.search(A),b;a:{for(b=0;0<=(b=d.indexOf("fmt",b))&&b<a;){var c=d.charCodeAt(b-1);if(38==c||63==c)if(c=d.charCodeAt(b+3),!c||61==c||38==c||35==c)break

Chrome Cache Entry: 199

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Algol 68 source, ASCII text, with very long lines (31881)
Category:	downloaded
Size (bytes):	320128
Entropy (8bit):	5.601059154246642
Encrypted:	false
SSDEEP:	6144:8DfULB7CkCqAJoezrd0RN7IgwJkBDeLxn:8DfULgkC5Joe+EkBDeLxn
MD5:	03445200895607220F3E315B9979B53F
SHA1:	BB5EB6B95B3CFED4A2F5257B61B0C3DF343CFEBC
SHA-256:	326B169E2EC0E7E8F64EE46BD52285477226DC8863266EE13691D5539BDF15B4
SHA-512:	BFBF3E8B5176724894D11A3A75AAB13D861A42D2608ED8479240B5985589A3CD4DF1559FE5A76A98DEFA6B97D87C932A37FC31361955AE02BDA8A94847ECFE63
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/326b169e2ec0.js

Preview:	;(function(){var root=this;var previousUnderscore=root._;var breaker={};var ArrayProto=Array.prototype,ObjProto=Object.prototype,FuncProto=Function.prototype;var push=ArrayProto.push,slice=ArrayProto.slice,concat=ArrayProto.concat,toString=ObjProto.toString,hasOwnProperty=ObjProto.hasOwnProperty;var nativeForEach=ArrayProto.forEach,nativeMap=ArrayProto.map,nativeReduce=ArrayProto.reduce,nativeReduceRight=ArrayProto.reduceRight,nativeFilter=ArrayProto.filter,nativeEvery=ArrayProto.every,nativeSome=ArrayProto.some,nativeIndexOf=ArrayProto.indexOf,nativeLastIndexOf=ArrayProto.lastIndexOf,nativeIsArray=Array.isArray,nativeKeys=Object.keys,nativeBind=FuncProto.bind;var _=function(obj){if(obj instanceof _)return obj;if(!(this instanceof _))return new _(obj);this._wrapped=obj;};if(typeof exports!=="undefined"){if(typeof module!=="undefined"&&module.exports){exports=module.exports=_}exports._=_}else{root._=_};_.VERSION="1.6.0";var each=_.each=_.forEach=function(obj,iterator,context){if(obj==null

Chrome Cache Entry: 200

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1327
Entropy (8bit):	5.353759587857711
Encrypted:	false
SSDEEP:	24:2dzAOx8LfHgonKNh6dRfXU8mtT+n5QOrVnmrUaTPz:czAOKfHgAKN6/UAlxnmDTL
MD5:	1AA2C19A21128E162921410EDC867FCE
SHA1:	5FA9A5BA1B9D2A37E0419AD27DF27CD0A8A317F6
SHA-256:	C6EFBAC4C969E83D254E91E4BFA5F350B432EB9B879FE1A6FAFEEEFF1355CE5D
SHA-512:	AAE2EA245FDCC91279642BCD53E22B7E341FBE0ABD017976ADB870BEEA23D9842566FC812A31B733DC6BC8534B6C0961F5710829158D0EF0D3826606AA95BB97
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="20px" height="16px" viewBox="0 0 20 16" style="enable-background:new 0 0 20 16;" xml:space="preserve">.<style type="text/css">...st0{fill:#152235;}.</style>.<title>twitter</title>.<desc>Created with Sketch.</desc>.<g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-825.000000, -719.000000)">...<g id="twitter" transform="translate(825.000000, 719.000000)">....<g id="Twitter">.....<path id="Shape" class="st0" d="M17.3,4.2c0,0.2,0,0.3,0,0.5c0,5-3.8,10.7-10.7,10.7c-2.1,0-4.1-0.6-5.8-1.7.....c0.3,0,0.6,0.1,0.9,0.1c1.8,0,3.4-0.6,4.7-1.6c-1.7,0-3-1.1-3.5-2.6c0.2,0,0.5,0.1,0.7,0.1c0.3,0,0.7,0,1-0.1.....c-1.7-0.3-3-

Chrome Cache Entry: 201

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 399 x 126, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	5113
Entropy (8bit):	7.896764152367228
Encrypted:	false
SSDEEP:	96:uFloBZkfnwe9aCqiEIc+UH0e+igHWugHAZ2MqNcFXn:u3ovkIelq3lc/0eCWpgZfPhn
MD5:	9C2A31B6BF0C6342D15F34C647CED936
SHA1:	4803678D6806B39C710C412F59274CAA60702573
SHA-256:	E34BEC6F1390D61061BD90C2A90D0F23B826F43EC1B013264AC93B7A98CEE000
SHA-512:	D7274B984072740D5A511CBD1B9FBA04B68887843C80B84C705A373E375CA171391651F42F85F8422A8FE4527D93EF619C63026E499E2EF5A547354B41427DE1
Malicious:	false
Reputation:	low
URL:	http://https://prezigram-assets.prezicdn.net/d7274b984072740d5a511cbd1b9fba04b68887843c80b84c705a373e375ca171391651f42f85f8422a8fe4527d93ef619c63026e499e2ef5a547354b41427e1
Preview:	.PNG.....IHDR.....~.....SA.....pHYs.....~.....IDATx....G.....S.{.{.....B.AB.sH.!...aO9.`..$.$.&.9.....8f.C ..a0..._...}..T]U].]..zF./..L4R...S.^..jo.A.t...G.A.h.A..ZA..ZA...V..A...A..A.h.A..ZA..ZA...V..A...A...A.h.A..ZA..ZA...V...V..A...A.h.A.h.A..ZA...V...V..A...A.h.A.h.A..ZA..].Z==.....}.....E!...~....?.....{...{...0....{.9Z..@.....z.....?.c$..F.M.|o..... .~.,...ZmH.~zA.._.^...W..jo.).i.`..xr....@..../...w...u...T{.V..Z%\.=>.]..^..!#F/....&...@....G.e.....e.h.A.fh.....w...ZA.h.D...[&T.x.. ...L...n...I~v..9..&. .w....o...c .su.2.....A.U_hEHR[...&..g?.....S}..C.....?...z...n6...d0Ns..]..G..=..?....t....z.x.I~...N.....?...v.....;._..!.....V.9G..=.O.<|...W....h@..d..hN.....Z.....V.....7M...=7..M..yp.Z%..f..K....Bh.V..@....a.Z.....~. ...Wp4."C.&A...Z.N.._q_.,.."ti...Fv.Vtm.V..~WQ...,.0.....'..ie6.xN...l.p....U=Y.nx{}.i5.}C...o...&.K.P.....i.A...M...Xd...K.j...I..K.c.J..0..g.....|.da.....[.tK;L+..).D7...

Chrome Cache Entry: 202

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 399 x 126, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	5113
Entropy (8bit):	7.896764152367228
Encrypted:	false
SSDEEP:	96:uFloBZkfnwe9aCqiEIc+UH0e+igHWugHAZ2MqNcFXn:u3ovkIelq3lc/0eCWpgZfPhn
MD5:	9C2A31B6BF0C6342D15F34C647CED936
SHA1:	4803678D6806B39C710C412F59274CAA60702573
SHA-256:	E34BEC6F1390D61061BD90C2A90D0F23B826F43EC1B013264AC93B7A98CEE000

SHA-512:	D7274B984072740D5A511CBD1B9FBA04B68887843C80B84C705A373E375CA171391651F42F85F8422A8FE4527D93EF619C63026E499E2EF5A547354B41427DE1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....~.....SA.....pHYs.....~.....IDATx....G.....S.{.{.....B.AB.sH.!...aO9.`..$.$.&.9.....8f.C ..a0..._...}..T]U].]..zF./..L4R...S.^..jo.A.t...G.A.h.A..ZA..ZA...V..A...A...A.h.A..ZA..ZA...V..A...A...A.h.A..ZA..ZA...V...V..A...A.h.A.h.A..ZA...V...V..A...A.h.A.h.A..ZA..].Z==.....}.....E!...~....?.....{...{...0....{.9Z..@.....z.....?.c$..F.M.|o..... .~.,...ZmH.~zA..._.^...W..jo.).i.`..xr....@..../...w...u...T{.V..Z%\.=>.]..^..!#F/....&...@....G.e.....e.h.A.fh.....w...ZA.h.D...[&T.x.. ...L...n...I~v..9..&. .w....o...c .su.2.....A.U_hEHR[...&..g?.....S}..C.....?...z...n6...d0Ns..]..G..=..?....t....z.x.I~...N.....?...v.....;._..!.....V.9G..=.O.<|...W....h@..d..hN.....Z.....V.....7M...=7..M..yp.Z%..f..K....Bh.V..@....a.Z.....~. ...Wp4."C.&A...Z.N.._q_.,.."ti...Fv.Vtm.V..~WQ...,.0.....'..ie6.xN...l.p....U=Y.nx{}.i5.}C...o...&.K.P.....i.A...M...Xd...K.j...I..K.c.J..0..g.....|.da.....[.tK;L+..).D7...

Chrome Cache Entry: 203	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2710), with no line terminators
Category:	downloaded
Size (bytes):	2710
Entropy (8bit):	5.88407653894185
Encrypted:	false
SSDEEP:	48:0oo2Y+iKasKEIzUtJQSIZyaQqe3q7SWWdCC6jykt08d4XT21cJ2wlSXT21cJ2wu6:KsbSUtJfxrqLWWWdV6j1KXL0XLr
MD5:	584F37F588C71B573A25A658ADE676E0
SHA1:	282407139D295F7F8F358E440F52B0744A2EB8EF
SHA-256:	A932F6C6EE2F4912A2BBF4FA73714DD62C1E7A6C4EC39D1D389E61EC1A0146B1
SHA-512:	539694C6BC4CF2F3E59385D2B4183422B5DCB3D40D6EDD79390D2EBA26814C12AA680A40FF36B8A9438CA94396A2704C23A4D7A37046E9C29E2E855F0FD71E2 1
Malicious:	false
Reputation:	low
URL:	**http**://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1001687149/? random=1679350440038&cv=11&fst=1679350440038&bg=ffffff&guid=ON&async=1>m=45He33f0&u_w=1280&u_h=1024&label=b1TSCIv8tAUQ7ZDS3QM&hn=www.goo gleadservices.com&frm=0&url=https%3A%2F%2Fprezi.com%2Fi%2Frx6p99-v72pt%2Fleibowicz-law- llc%2F&tiba=Leibowicz%20Law%20LLC%20by%20Secure%20Message%20on%20Prezi%20Design&auid=30291553.1679350440&uaa=x86&uab=64&uafvl=Chromium% 3B104.0.5112.102%7C%2520Not%2520A%253BBrand%3B99.0.0.0%7CGoogle%2520Chrome%3B104.0.5112.102&uamb=0&uap=Windows&uapv=8.0.0&uaw=0&rfmt=3 &fmt=4
Preview:	(function(){var s = {};(function(){/* Copyright The Closure Library Authors. SPDX-License-Identifier: Apache-2.0 */ var e={},f=this||self;var g,k;a:{for(var l=["CLOSURE_ FLAGS"],p=f,q=0;q<l.length;q++)if(p=p[l[q]],null==p){k=null;break a}k=p}var r=k&&k[610401301];g=null!=r?r:!1;var t,v=f.navigator;t=v?v.userAgentData||null:null;function w (d){return g?t?t.brands.some(function(a){return(a=a.brand)&&-1!=a.indexOf(d)}):!1:!1}function x(d){var a;a:{if(a=f.navigator)if(a=a.userAgent)break a;a=""}return-1!=a.ind exOf(d)};function y(){return g?!!t&&0<t.brands.length:!1}function z(){return y()?w("Chromium"):(x("Chrome")||x("CriOS"))&&!(y()?0:x("Edge"))||x("Silk")};!x("Android")||z( );z();!x("Safari")||z()||(y()?0:x("Coast"))||(y()?0:x("Opera"))||(y()?0:x("Edge"))||(y()?w("Microsoft Edge"):x("Edg/"))||y()&&w("Opera");var A=/#|$/;function B(d){var a=d .search(A),b;a:{for(b=0;0<=(b=d.indexOf("fmt",b))&&b<a;){var c=d.charCodeAt(b-1);if(38==c||63==c)if(c=d.charCodeAt(b+3),!c||61==c||38==c||35==c)break

Chrome Cache Entry: 204	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3545), with no line terminators
Category:	downloaded
Size (bytes):	3545
Entropy (8bit):	5.323510543796483
Encrypted:	false
SSDEEP:	48:E7yok8TPpw6GAp7AizYnnBUg7qdgp1qdXwdcitI1MRbZ+hxRCQU5weWh+lsWGWAM:E704WBjqSq9BhxRzUGb8tZ
MD5:	383FA66D2A0A09F4A6E64A9593AD43BB
SHA1:	62D7B071D7EC77027D27887803CCE960E211F69D
SHA-256:	3E7D49F24D56DB02C7BACA8AE3A17555C2E527571450E8C24C77B453407E267A
SHA-512:	5CB29437A1B3E8FB4A6665E4E96ECF0E55F31BB4546C4A58AD3EB72CAAFFD61A471F4D6139547377D59E89A5D8C063429F90BD24DAB25FC4DBE18A407C2371 39
Malicious:	false
Reputation:	low
URL:	**http**://https://cdn.taboola.com/scripts/cds-pips.js
Preview:	!function(t){try{var n="https://",e="aHR0cHM6Ly9waXBzLnRhYm9vbGEuY29t",r=["YXJjaGl0ZWN0dXJl","cGxhdGZvcm1WZXJzaW9u","dWFGdWxsVmVyc2lvbg=="],a= ["YnJhbmRz","bW9iaWxl","bW9kZWw=","cGxhdGZvcm0=","cGxhdGZvcm1WZXJzaW9u","dWFGdWxsVmVyc2lvbg=="];t.TRC.cdsPips={userId:null,getHttpsPrefix: function t(){return n},doNothing:function t(){return!0},safeGetTfaConfig:function n(e,r,a){return t._tfa&&t._tfa.config&&t._tfa.config.safeGet&&t._tfa.config.safeGet(e,r, a)},safeGetRboxConfig:function t(n){var e;return(TRCImpl?TRCImpl.global:{})[n]},prepareGenericRequest:function n(e,r){var a,o=new(t.XDomainRequest||t.XMLHttpReq uest);return o.open(e,r),o.onload=this.doNothing,o.onerror=this.doNothing,o.onprogress=this.doNothing,o},tryToReadUserIdFromLocalStorage:function t(){try{return window.localStorage["taboola global:user-id"]}catch(t){return null}},getUserId:function n(){var e=t.TFASC&&t.TFASC.tfaUserId&&"function"==typeof t.TFASC.tfaUse rId.getUserId?t.TFASC.tfaUserId.getUserId():null,r=t.TRC.pageManager&&

Chrome Cache Entry: 205	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (40607), with no line terminators
Category:	downloaded
Size (bytes):	40608

Entropy (8bit):	5.310154158156412
Encrypted:	false
SSDEEP:	768:ZaOrhxRXNkHXhzDO2cRysgpzQHQbwpYyDxWLKQ:ZaOrjRkAREzQ2oxWeQ
MD5:	B51AB1F965C96F271CC08617EEEBC57A
SHA1:	F7A52E401D28AC7FE5BA78711D4E2F0CAD0E365C
SHA-256:	A2137EBFE2B9FF55E1F280DBB1EEF301290C50DB609C5D6A0494AE8F3C98C253
SHA-512:	F516DD50F1AF64EAABDB5457EF1ADE46C778235F6FE226E437797C2B7660C672CD2C773D5F7B2CC55B32403E7A0D8C493395D0AA983DB23360594027ACBFAA1
Malicious:	false
Reputation:	low
URL:	http://https://bat.bing.com/bat.js
Preview:	function UET(o){this.stringExists=function(n){return n&&n.length>0};this.domain="bat.bing.com";this.URLLENGTHLIMIT=4096;this.pageLoadEvt="pageLoad";this.customEvt="custom";this.pageViewEvt="page_view";o.Ver=o.Ver!==undefined&&(o.Ver===="1"||o.Ver===1)?1:2;this.uetConfig={};this.uetConfig.consent={enabled:!1,adStorageAllowed:!0,adStorageUpdated:!1,hasWaited:!1,waitForUpdate:0};this.beaconParams={};this.supportsCORS=this.supportsXDR=!1;this.paramValidations={string_currency:{type:"regex",regex:/^[a-zA-Z]{3}$/,error:"{p} value must be ISO standard currency code"},number:{type:"num",digits:3,max:999999999999},integer:{type:"num",digits:0,max:999999999999},hct_los:{type:"num",digits:0,max:30},date:{type:"regex",regex:/^\d{4}-\d{2}-\d{2}$/,error:"{p} value must be in YYYY-MM-DD date format"},pid:{type:"pid"},"enum":{type:"enum",error:"{p} value must be one of the allowed values"},array:{type:"array",error:"{p} must be an array with 1+ elements"},object:{type:"object",error:"{p} must be an obj

Chrome Cache Entry: 206	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 88 x 23, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	61
Entropy (8bit):	3.9708734032409505
Encrypted:	false
SSDEEP:	3:yionv//thPlFot/Usxl/k4E08up:6v/lhPAtMs7Tp
MD5:	EC6FF9162ADFCAF86B9732BC9448BDF1
SHA1:	4949826E08A09D6F0CD40BD2EFE1739177CD262B
SHA-256:	D5DAA89C6D32E2C6E4B1F48EDC817C9C83F30C147B9283816FF220AB4791DDF0
SHA-512:	BF336695CF101E3F3C7DEE6CAA0A3F6F80FFFF930873BA9A8B3A2FFE14E0337999A1790309DB16F14F6A76A992BAEEE18E05983AFD0EAED0E134D5BBB10D2254
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/img/7ab14ea51c463602/1679350458092/VajOonMq3Bc-o1V
Preview:	.PNG.....IHDR...X.....IDAT.....$.....IEND.B`.

Chrome Cache Entry: 207	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/ASSETS/img/m_.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392,1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47.081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 208	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3034)

Category:	downloaded
Size (bytes):	199037
Entropy (8bit):	5.523182498758856
Encrypted:	false
SSDEEP:	3072:dDmgss9Cox4PRAHmZFx+ryyQKVSXDy/UWXMiqvPaG2pjA+CYGMk5hPhx:dPCox7+xiyyQaS0fciuPaG2++ChMkfpx
MD5:	5AC253D9DCF5AFC55E6C98875626C2AC
SHA1:	EC9F01C1123DBE302B301072E1F8EA0C27593D70
SHA-256:	6B60FDBBA906DE74B65132D8A7BF5F6B877816A092F5FB04132B3679082F8225
SHA-512:	A738D4CFC124EFB262DC5B361F1EEEAA327B338188161A3B6BCFA2825A79FB497FF7CC580865F24CF27F100D2648FA2BC5E8BD5EFEF26DC048366CA3A22F1229
Malicious:	false
Reputation:	low
URL:	http://https://accounts.google.com/gsi/client
Preview:	"use strict";this.default_gsi=this.default_gsi||{};(function(_){var window=this;.try{.var aa,ba,ca,da,p,ea,ha,ia,ka;aa=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ca=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};da=ca(this);p=function(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}};.p("Symbol",function(a){if(a)return a;var b=function(f,g){this.h=f;ba(this,"description",{configurable:!0,writable:!0,value:g})};b.prototype.toString=function(){return t

Chrome Cache Entry: 209

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	774
Entropy (8bit):	4.440917145843649
Encrypted:	false
SSDEEP:	24:tYU/duXMMrMpks43ZNpBefXUUBV1VK0T40:n/S6covnV1M0z
MD5:	40E2167E47CC055845E1E8ECF21070AC
SHA1:	FA22F2E65DE3B1DF56D3271B2FB9C3B6B9A5B7DB
SHA-256:	901592B708BB50F6DC82DCD9B86DC4BD00D2790B08451FBC987508990C2C29B2
SHA-512:	11485D42363D1D2939A1EA6CC4A70077059CEAACC7F7C388FA0B6A7D33F95CD563D7226BD22F9728C305D0DE54934ACDFCA347693113EC75A53A7B13C485688
Malicious:	false
Reputation:	low
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M18 6.5C18 7.88071 16.8807 9 15.5 9C14.9483 9 14.4383 8.8213 14.0249 8.51861L8.99671 11.8707C8.9989 11.9135 9 11.9566 9 12C9 12.0434 8.9989 12.0865 8.99671 12.1293L14.0249 15.4814C14.4383 15.1787 14.9483 15 15.5 15C16.8807 15 18 16.1193 18 17.5C18 18.8807 16.8807 20 15.5 20C14.1193 20 13 18.8807 13 17.5C13 17.4029 13.0055 17.307 13.0163 17.2127L8.09053 13.9289C7.65834 14.2857 7.1042 14.5 6.5 14.5C5.11929 14.5 4 13.3807 4 12C4 10.6193 5.11929 9.5 6.5 9.5C7.1042 9.5 7.65834 9.71434 8.09053 10.0711L13.0163 6.78727C13.0055 6.693 13 6.59715 13 6.5C13 5.11929 14.1193 4 15.5 4C16.8807 4 18 5.11929 18 6.5Z" fill="black"/>.</svg>.

Chrome Cache Entry: 210

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64784)
Category:	downloaded
Size (bytes):	66548
Entropy (8bit):	5.293700227734791
Encrypted:	false
SSDEEP:	1536:JY9ktCO5CJXCYZXPNtWaCscVDXXsRlzIlg5Xz6jX8hCoEFfOpDw6usi5l/bWPW0P:wN1CklzIlg5X5l8e
MD5:	7D665DAB25E228C637BF155351A3F313
SHA1:	C1336BB9C26E5379DA77058C8A0A106828E41E34
SHA-256:	80371A34CFA011DDDBEFBB9D57FC1F1B0A3503D3ED63E3AAE24F95A1110116CC
SHA-512:	2B99B5C9FC25557F12D93BBB388AC971899E0A542BFB1FC698E89B8A9BBDF39ED1653F8B78C5DB374BA839B7139FF656ED340A1B50C392EA6B59461C056566676
Malicious:	false
Reputation:	low
URL:	http://https://js.hs-analytics.net/analytics/1679350200000/20307117.js
Preview:	/** . * HubSpot Analytics Tracking Code Build Number 1.473. * Copyright 2023 HubSpot, Inc. http://www.hubspot.com. */.var _hsq = _hsq || [];.var _paq = _paq || [];._hsq.push(['setPortalId', 20307117]);._hsq.push(['trackPageView']);._hsq.push(['setLegacy', false]);._hsq.push(['addCookieDomain', '.hubspotpagebuilder.com']);._hsq.push(['addCookieDomain', '.hs-sites.com']);._hsq.push(['addCookieDomain', '.prezi.com']);._hsq.push(['addCookieDomain', '.hubspot.com']);._hsq.push(['addCookieDomain', '.hsforms.com']);._hsq.push(['enableAutomaticLinker', true]);._hsq.push(['embedHubSpotScript', 'https://js-na1.hs-scripts.com/20307117.js', 'hs-script-loader']);._hsq.push(['setTrackingDomain', 'track.hubspot.com']);./** _anon_wrapper_ **/ (function() {.var hstc;(hstc=hstc||{}).JS_VERSION=1.1;hstc.ANALYTICS_HOST="track.hubspot.com";(hstc=hstc||{}).Math={uuid:function(){if(window.navigator.userAgent.indexOf("googleweblight")>-1)return hstc.Math._mathRandomUuid();var t=window.crypto||window.msCrypto

Chrome Cache Entry: 211	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (577), with no line terminators
Category:	downloaded
Size (bytes):	577
Entropy (8bit):	5.014211645474839
Encrypted:	false
SSDEEP:	12:preDPxKmyoXMOAoHfgW6Vbqa5eVKdypdPrL87OPXKc4sj3FpPbcUdon:p2xKWXsVXetvOWaKjr0
MD5:	7C7E82C177DEB9D5D9898414F238BE81
SHA1:	F6BFB8AFCCDC61B457452AE4664BF43AB90C7BEB
SHA-256:	B54ABD3AF1BEC25DA343FAE66EEBA1B0497BC10491A6F1CC97B8A5DD758A2040
SHA-512:	AF475A9C3D563143543F3732D1E3B5481D460719C6212419E86B465C0C177E43597EC48CFD533050BA64A261B645FF50D468EBFF583DC35EDB49F6AA933FCFB
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/b54abd3af1be.css
Preview:	#signup_popup{padding:20px 24px 24px;z-index:1032;display:none;background:#FFF;border-radius:8px;width:392px;position:fixed;right:30px;top:15px;box-shadow:0 1px 2px rgba(0,0,0,.05)}#signup_popup #signup_popup_close{background:0 0;border:none;position:absolute;right:30px;top:20px;width:20px;height:20px;cursor:pointer}#signup_popup label{margin:0;font-family:RalewayBold,Helvetica,sans-serif;font-size:20px;line-height:24px;letter-spacing:.25px;color:#152235}#signup_popup input{margin:20px 0 12px}#signup_popup button{width:100%;font-size:16px;letter-spacing:.5px;height:48px}

Chrome Cache Entry: 212	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 13 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.022997040570905
Encrypted:	false
SSDEEP:	3:yionv//thPlozttZt/hAkxl/k4E08up:6v/lhPyt/Kk7Tp
MD5:	D6A0FA403A4B06A2E824553DDF751F0F
SHA1:	A46F5AFB54CC321A41C7A5FB0959E2C51FC5C137
SHA-256:	73E03D4C2911F7666D780BEFD1D27F0E3FA6097D17489872C8D6EFDEC1CD5DA8
SHA-512:	1855FFA1B592E056C4ECD1D11E1911ABC993DB99AE595976A5B9428CE71E1BF7A0D3074158A79776E50749E31B429F9CEDB32AB9F8DD9BC27635B15DEF08205 8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....L.....9.....IDAT.....$.....IEND.B`.

Chrome Cache Entry: 213	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 186 x 106, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	33231
Entropy (8bit):	7.986474350329641
Encrypted:	false
SSDEEP:	768:j+VTrD2c/rvtINAVofu9Paa+gR5n6JwXJK+2us+m:aVTWc/r2ffuj+gDnkww+2v3
MD5:	68411045E8288B5FF677386D8444E551
SHA1:	0A8E0599304D3B93ACBB9AD85AC63084EB2BB95D
SHA-256:	A23F7D2BFF3DABEFE64F16BD4A77BF0524EB87D14FE944A300142F234AD244E4
SHA-512:	4D6A0D49C2A6A8513D5869433BBDE49C96A57604D7903C803DD23EABB618389E1EFF2DF277FF0B03F90A3162FA3472559BFDAAFD6DB60115B22564B5F3C1273 A
Malicious:	false
Reputation:	low
URL:	http://https://prezigram- assets.prezicdn.net/4d6a0d49c2a6a8513d5869433bbde49c96a57604d7903c803dd23eabb618389e1eff2df277ff0b03f90a3162fa3472559bfdaafd6db60115b22564b5f3c127 a
Preview:	.PNG.....IHDR.....j.....0K.....pHYs...%...%.IR$... .IDATx...w.Y.....yg.{L..C.....$@H.!...@^.....'bgf.u7.g..jTTe..;v.'"..h.....L...|dd$....k..<.....M.e..4....+...F.s6x..F=..g\|W\|. .Y....^...iT^...z}.....:.....o&&&.....g...../^.C...p...H>.....W..._.o.....3.y.^..Y.~...5==._.t).kW~...V[.....z9vi...J....1.+.....a..q.:^.s.....m.._..3.{<s...<?.jA.{zz..C/....\|l,. x6..};.x.B~.....3okk.....S.N.g.....]]...b.CP.H.1...U...I..P.....{._.rY....3...\|`` .....[...yg....)....\|..d~n.B....;y.....k..G.....{'.....6F.....>hQLNN.3&...s~.FLI.....K./.Z% ..&...x.BH..~.Q..(.....ZB....hdM..h....g....x....?z....Y....6N.l.n.X^./^.h.t%.m.r.....\|..X^....r.W..z~_<.....l.....#..HX....;w..W.Z.....+...../.....'O.W.....z.*.....i..... ...&w....l>7;.....B(..>.....W.g.H....0.\... ...<w...s.1]h.,.\9Y.....$=~.8....&.....7oJ....._.W..w...q_.....M.

Chrome Cache Entry: 214	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 215	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64471)
Category:	downloaded
Size (bytes):	386394
Entropy (8bit):	5.460948495119879
Encrypted:	false
SSDEEP:	6144:Rx9GM0Y0bqrM0etDv5H7K4rwzzGM0zwv5H76McqMKCHDHFao:PwjL
MD5:	34C16139A74D3464E24E43005FC24678
SHA1:	0ABEE5D0A02DC6522D745E2FB2FDF48047F7978B
SHA-256:	ECECBA078AC6501E49554BE5287266D925D82B7BBE617162F07996C9E31921FD
SHA-512:	3B3323292F33C23A624379E3EF806BEFE49FF461ABBCBB3178652F10803F464D2FFB5ED202EE67B9DD11093506AEA5003CAD99459A109725B6C2FBC6303F0D7
Malicious:	false
Reputation:	low
URL:	http://https://connect.facebook.net/signals/config/291059134405770?v=2.9.99&r=stable
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be .* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

Chrome Cache Entry: 216	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:HtHKiY:RKiY
MD5:	011B17B116126E6E0C4A9B0DE9145805
SHA1:	DF63A6EB731FFCE96F79802EFF6D53D00CDA42BC
SHA-256:	3418E6E704387A99F1611EB7BB883328A438BA600971E6D692E8BEA60F10B179
SHA-512:	BB432E96AF588E0B19CBD8BC228C87989FE578167FD1F3831C7E50D2D86DE11016FB93679FEF189B39085E9151EB9A6EB2986155C65DD0FE95EC85454D32AE7 D
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTA0LjAuNTExMi4xMDISEAnDkttEwdxkoBIFDdFbUVI=?alt=proto
Preview:	CgkKBw3RW1FSGgA=

Chrome Cache Entry: 217	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3940
Entropy (8bit):	3.9592048137955604
Encrypted:	false
SSDEEP:	96:BZxXV5hmkWIrrSd5bt3vY2Y5qFchRiEr0ZHzyACUFGx4Z9HvGSv:BLIfWwrSvt3vY2YAliF2AXU4ft
MD5:	A7DDDF47631368B9AC186C0A26A046E5
SHA1:	2A706D92842D5ADB2CB78FA553E1F883E5166565
SHA-256:	842FFCD81D0AAB8358DEAD11F9807F620675ACEF04C159C6A9994A0B0547DA73
SHA-512:	60541E55B574E9BF18256CA891E00611E5AA461158D4EFF235A22A2DF0CF7B43042FBC53B8CF9BE1B9F30A26253616C686D12B636FD66B7DC30A70F34D999B6
Malicious:	false
Reputation:	low
Preview:	<svg id="Layer_1" xmlns="http://www.w3.org/2000/svg" width="98.4" height="36" viewBox="0 0 98.4 36"><style>.st0{fill:#fff}</style><title>prezi_logo</title><path class="st0" d="M17.9 7.3c-2.8 0-5.6 1.1-7.5 3.1-2 2-3.2 4.7-3.1 7.5-.1 2.8 1.1 5.5 3.1 7.5s4.7 3.2 7.5 3.1c2.8 0 5.5-1.1 7.5-3.1s3.2-4.7 3.1-7.5c0-2.8-1.1-5.6-3.1-7.5-1.9-2-4.6-3.1-7.5-3.1zm6.8 17.5c-1.8 1.8-4.2 2.8-6.8 2.8-2.6.1-5-1-6.8-2.8C9.2 23 8.2 20.6 8.3 18c-.1-2.6 1-5 2.8-6.8 1.8-1.9 4.2-2.9 6.8-2.8 2.6 0 5 1 6.8 2.8 1.8 1.8 2.8 4.2 2.8 6.8.1 2.6-.9 5-2.8 6.8zM17.9 9.5c-2.3 0-4.5.9-6.1 2.5-1.6 1.6-2.5 3.8-2.5 6.1s.9 4.5 2.5 6c1.6 1.6 3.8 2.5 6.1 2.5s4.5-.9 6-2.5c1.6-1.6 2.5-3.8 2.5-6 0-2.3-.9-4.5-2.5-6.1-1.5-1.6-3.7-2.6-6-2.5zm7.5 8.9c0 2-.9 3.9-2.4 5.2-1.5 1.4-3.4 2.1-5.4 1.9-4.1-.2-7.3-3.6-7.1-7.8v-.1c.1-2 1-3.9 2.5-5.2 1.5-1.4 3.4-2.1 5.4-1.9 2 .1 3.8 1 5.1 2.5 1.3 1.5 2 3.4 1.9 5.4zm4.3-5.3C29 11.6 28.1 10.2 27 9c-1.2-1.2-2.5-2.1-4.1-2.7-1.6-.7-3.3-1-5-1-1.7 0-3.4.3-5 1-1.5.6-2.9 1.5-4 2.7-1.2 1.2-2.1 2.5-2.7 4.1-.7

Chrome Cache Entry: 218	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (533), with no line terminators
Category:	downloaded
Size (bytes):	533
Entropy (8bit):	4.933115570682282
Encrypted:	false
SSDEEP:	12:X5eNcBWFXMOYEBAP5egtIzVWRwHjXJqIK+qIKzg0fUsq5eK:pemBkXWegazdDZq3+q3c08sceK
MD5:	FEB698008C36A09DFE88AB06A1C3E3B9
SHA1:	A871FBCBBE298AE7078D06627708B2C106A0FAF3
SHA-256:	1C4E7E389D73C6ACF7F19CC812514E71230740791FDE8A018C1D7EDCCF1590AE
SHA-512:	F8E3CA3E49B1C027232D1B3AAB82B5430F4A69334A5E18BEB4469C39D6A24D3F4D3FA4C473F360B619CE734977F0D7EFD03BE6ACB5EB7B9F69295FB2CBF94D 9B
Malicious:	false
Reputation:	low
URL:	http://https://accounts.google.com/gsi/style
Preview:	#credential_picker_container{border:none;height:330px;position:fixed;right:20px;top:20px;width:391px;z-index:9999}#credential_picker_container iframe{border:non e;width:391px;height:330px}#g_a11y_announcement{height:1px;left:-10000px;overflow:hidden;position:absolute;top:auto;width:1px}.L5Fo6c-sM5MNb{border:0;display:bl ock;left:0;position:relative;top:0}.L5Fo6c-bF1uUb{-webkit-border-radius:4px;border-radius:4px;bottom:0;cursor:pointer;left:0;position:absolute;right:0;top:0}.L5Fo6c-bF1uU b:focus{border:none;outline:none}sentinel{}

Chrome Cache Entry: 219	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Unicode text, UTF-8 text, with very long lines (26282)
Category:	downloaded
Size (bytes):	26289
Entropy (8bit):	6.048922410696652
Encrypted:	false
SSDEEP:	768:iVlJlK3rxbP8Z0x9DtwmdaYTmTEB5UesZs:f3hzrD2+aImTEBm/Zs
MD5:	C9D3E0FAA9DDFE565382E65E03037987
SHA1:	5380D45D99BB33099658034903B319AB14429B42
SHA-256:	2DA461EAB0C2B6241D8C73215277F1CD72AE3B0A7A0444F95D939D1F96BDFE06
SHA-512:	8EBC389D9CEAD941B948A4C7E8A32B26C1BACD71B35726F983A4DFAF117E3D14096EBC89997F3D3B3B258B19826AF077FED517F54AA2373C0B3593CEAE562C B4
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=&oit=0&gs_rn=42&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw

Preview:	)]}'.["",["fut birthday fifa 23","marcel sabitzer","fc barcelona vs real madrid","eintracht frankfurt","destiny 2","cs go 2","motogp","manchester united fc fulham"],["","","","","" ,"","",""],[],{"google:clientdata":{"bpc":false,"tlw":false},"google:headertexts":{"a":{"8":"TRENDS BEI SUCHANFRAGEN"}},"google:suggestdetail":[{"zl":8},{"a":"Fu.ballspie ler","dc":"#424242","i":" QsJCYxJx8fLT0tMTU3Ojo6Iys/RD84QzQ5OjcBCgoKDQwNGg8PGjclHyU3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3Nzc3N//AABEI AMgAmgMBIgACEQEDEQH/xAAcAAABBQEBAQAAAAAAAAAAAAAAAwQFBgcBAgj/xABBEAACAQMCBAMGBAQDBgcBAAABAgMABBEFIQYSMUETIlEHFG FxgZEyobHBI1Lh8EJi0RUkNFNy8RYzVJKywtII/8QAGgEAAwEBAQEAAAAAAAAAAAAAAAECAwQGBf/EACIRAAICAgMAAgMBAAAAAAAAAAABAhEDIRIxQQRREy IyBf/aAAwDAQACEQMRAD8A3GiiigAooooAK4zBRk1x3VFLMQFG5JOMVjPGHGN7xBr0+kaJdSQ6fbOqySRnHinq2T1x2A9fnQJs2SSaOJOeV1RK77cN+GK2YMPq3Qfr8KySSwJzMjXErn

Chrome Cache Entry: 220

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3940
Entropy (8bit):	3.9592048137955604
Encrypted:	false
SSDEEP:	96:BZxXV5hmkWIrrSd5bt3vY2Y5qFchRiEr0ZHzyACUFGx4Z9HvGSv:BLlfWwrSvt3vY2YAIiF2AXU4ft
MD5:	A7DDDF47631368B9AC186C0A26A046E5
SHA1:	2A706D92842D5ADB2CB78FA553E1F883E5166565
SHA-256:	842FFCD81D0AAB8358DEAD11F9807F620675ACEF04C159C6A9994A0B0547DA73
SHA-512:	60541E55B574E9BF18256CA891E00611E5AA461158D4EFF235A22A2DF0CF7B43042FBC53B8CF9BE1B9F30A26253616C686D12B636FD66B7DC30A70F34D999B6I
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/logo/prezi-logo-white.svg
Preview:	<svg id="Layer_1" xmlns="http://www.w3.org/2000/svg" width="98.4" height="36" viewBox="0 0 98.4 36"><style>.st0{fill:#fff}</style><title>prezi_logo</title><path class="st0" d="M17.9 7.3c-2.8 0-5.6 1.1-7.5 3.1-2 2-3.2 4.7-3.1 7.5-.1 2.8 1.1 5.5 3.1 7.5s4.7 3.2 7.5 3.1c2.8 0 5.5-1.1 7.5-3.1s3.2-4.7 3.1-7.5c0-2.8-1.1-5.6-3.1-7.5-1.9-2-4.6-3.1-7.5-3.1zm6.8 17.5c-1.8 1.8-4.2 2.8-6.8 2.8-2.6.1-5-1-6.8-2.8C9.2 23 8.2 20.6 8.3 18c-.1-2.6 1-5 2.8-6.8 1.8-1.9 4.2-2.9 6.8-2.8 2.6 0 5 1 6.8 2.8 1.8 1.8 2.8 4.2 2.8 6.8.1 2.6-.9 5-2.8 6.8zM17.9 9.5c-2.3 0-4.5.9-6.1 2.5-1.6 1.6-2.5 3.8-2.5 6.1s.9 4.5 2.5 6c1.6 1.6 3.8 2.5 6.1 2.5s4.5-.9 6-2.5c1.6-1.6 2.5-3.8 2.5-6 0-2.3-.9-4.5-2.5-6.1-1 .5-1.6-3.7-2.6-6-2.5zm7.5 8.9c0 2-.9 3.9-2.4 5.2-1.5 1.4-3.4 2.1-5.4 1.9-4.1-.2-7.3-3.6-7.1-7.8v-.1c.1-2 1-3.9 2.5-5.2 1.5-1.4 3.4-2.1 5.4-1.9 2 .1 3.8 1 5.1 2.5 1.3 1.5 2 3.4 1.9 5.4zm4.3-5.3C29 11.6 28.1 10.2 27 9c-1.2-1.2-2.5-2.1-4.1-2.7-1.6-.7-3.3-1-5-1-1.7 0-3.4.3-5 1-1.5.6-2.9 1.5-4 2.7-1.2 1.2-2.1 2.5-2.7 4.1-.7

Chrome Cache Entry: 221

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	400
Entropy (8bit):	4.705757983822934
Encrypted:	false
SSDEEP:	12:trwdU/gKuCC1RFoVbXoGof0jK1y4mqPBpGzK0:tYU/du/1joai2HNPBv0
MD5:	478D5FBDFB49D87F0498747623BC7B8F
SHA1:	1A65D0BAA57A07917F3A7F65FCA6B3A13D12FF75
SHA-256:	BAA5D917882C3FDD1E76A0BE5DDB9A02ADDEC5F5BB1A1DDA216DFED9617CF48A
SHA-512:	1A51CB61A8793B9347800EE771C185AEAE9F9F0B7B7EFC32A4625B10E9A7F19BAECA89AB2ABF50ACD2B17F6D086C0B471BB0EAA8F8D357ACCB6CCED0BBA 2CB1D
Malicious:	false
Reputation:	low
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M13.8 6.72394C13.2886 6.15421 13.4106 5.55364 12.9333 4.9538C11.2259 2.80775 6 4.9538 6 4.9538V20H8V14C8 14 10.87 12.5825 12.0667 13.8045C12.6018 14.351 12.4408 14.9878 12.9333 15.5746C14.4752 17.4117 19 1 5.5746 19 15.5746V6.72394C19 6.72394 15.1722 8.25269 13.8 6.72394Z" fill="black"/>.</svg>.

Chrome Cache Entry: 222

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	367
Entropy (8bit):	4.91512135645049
Encrypted:	false
SSDEEP:	6:tnrwdhC/gKumc4slvtM65tfTLCMhrygjFboBsJO6yUFORulUTL0TxPKVM:trwdU/gKuXM65JT+Mh1FboBViQUT1Kq
MD5:	5E58B5B139E41CC0645ADA25F7D29F09
SHA1:	9161EAC1663B931DC69EAD690AF33CE968AD4E0C
SHA-256:	CA98E42319955E993F6CE9AF1B31C69054E260147F9B3AD6DBBB4DD4D36E5DDA
SHA-512:	162AD1019859187E3CD71A23132F843734B1E06BCADAFEF73F15C965D1CB26E1798A56CC0A5F12A1BF8CDEF7452A21B6808FAB71A1980053E8AF3AD1AE7BD7 E0
Malicious:	false

Reputation:	low
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M12.0002 10.585 8L7.75748 6.34314L6.34326 7.75735L10.5859 12L6.3433 16.2427L7.75752 17.6569L12.0002 13.4142L16.2428 17.6568L17.657 16.2426L13.4144 12L17.657 7.75739L16.2428 6.34317L12.0002 10.5858Z" fill="#000000"/>.</svg>.

Chrome Cache Entry: 223	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	533
Entropy (8bit):	4.70497619638867
Encrypted:	false
SSDEEP:	12:trwdU/gKuXM65PCpWcuGNNPB5IJS71wx4bumrYR0:tYU/duXMMP3cuGNNp5SEO4ymUR0
MD5:	66D50AF6577AA40B5139861D53DC77B3
SHA1:	7844C61A29625582620D7040B400BE5EA020E6C7
SHA-256:	B1C52A735B65D540A88E799748E01B5B7B317CE52C51361A620D804390E10D3D
SHA-512:	CE4FDC7F0A3E20388FF42F28CF6585E6B12D4B50E8A0182182790248288DB727A31A1EBDE248DB6D21D38F9FBDAFEA3B68A35F6F7DEF4175B8CFF93A6E1520 3
Malicious:	false
Reputation:	low
URL:	http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/embed.svg
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M10.0136 17.835 7L12.0136 5.83569L13.9864 6.16449L11.9864 18.1645L10.0136 17.8357ZM17.5858 12.0001L14.2929 8.7072L15.7071 7.29299L19.7071 11.293L20.4142 12. 0001L19.7071 12.7072L15.7071 16.7072L14.2929 15.293L17.5858 12.0001ZM9.70714 15.293L6.41424 12.0001L9.70714 8.7072L8.29292 7.29299L4.29292 1 1.293L3.58582 12.0001L4.29292 12.7072L8.29292 16.7072L9.70714 15.293Z" fill="black"/>.</svg>.

Chrome Cache Entry: 224	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (13351)
Category:	downloaded
Size (bytes):	13352
Entropy (8bit):	5.417016481578538
Encrypted:	false
SSDEEP:	192:76FxFPmjDFQwYwR4iX/AqgBPn/C0ak0BecY/P0ak0sSFw6kAzrJ30YuPX:+24iv0/CdPecCPdhRVrJuf
MD5:	B846C9D158853DD4AA95D3D7407ED8BB
SHA1:	2CF0EB02A22E8BD80D19A50A84593420D777D5DB
SHA-256:	F56CCB2DB87AACEDD9415232E40F80BFF9939703DF2F9C3F9EC8A092E545349F
SHA-512:	62E95EED5842D2C4E263B3CD0668AF061FD14309DB168837BC17D11666D900DD029913B4D774134508E91A6B337A4F28E820DA19DCCC125262F205596793DBD
Malicious:	false
Reputation:	low
URL:	http://https://snap.licdn.com/li.lms-analytics/insight.min.js
Preview:	!function(){"use strict";function n(n,e,t){e in n?Object.defineProperty(n,e,{value:t,enumerable:!0,configurable:!0,writable:!0}):n[e]=t}var a,c,u,d={ADVERTISING:"ADVERTIS ING",ANALYTICS_AND_RESEARCH:"ANALYTICS_AND_RESEARCH",FUNCTIONAL:"FUNCTIONAL"},o="GUEST",r="MEMBER",l=0,s=1,i=2,f=(n(e={},o,"li_gc"),n(e,r,"l i_mc"),e),p=function p(){var n,e=0<arguments.length&&arguments[0]!==undefined?arguments[0]:null,t=1<arguments.length&&arguments[1]!==undefined?argumen ts[1]:null,o=2<arguments.length&&arguments[2]!==undefined?arguments[2]:null,r=3<arguments.length&&arguments[3]!==undefined?arguments[3]:null,i=this,a=p;if(!(i i nstanceof a))throw new TypeError("Cannot call a class as a function");for(n in e=e||{},this.consentAvailable=!1,this.issuedAt=t,this.userMode=o,this.optedInConsentMap= {},d)e[n]=e[n]||l,e[n]!==l&&(this.consentAvailable=!0),this.optedInConsentMap[n]=e[n]===s||e[n]===l&&r===s},P=(a=[d.ADVERTISING,d.ANALYTICS_AND_RESEARCH, d.FUNCTIONAL],c=[l,s,i,l],u=new RegExp(["^(\\d+)","(\\d+)","|

Chrome Cache Entry: 225	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (544)
Category:	downloaded
Size (bytes):	11439
Entropy (8bit):	5.359985230087669
Encrypted:	false
SSDEEP:	192:ucL60YrI90CW3j4xqLYfMHaPsiJcW9eYcfZcTQWhGJykDZNZ3y:jL6hrI90CW3jhgUiJc+eYcfZ3W0JySNU
MD5:	4EFDF8FAD0D7BFA436A2C00810E1408F
SHA1:	9DF7AA3FCEF80D4FEE23233C925ADBCB379F1DA6
SHA-256:	359C83B33DBEE80C8528E3B5A9426C800AD795A792D39343185B83BE8731130D
SHA-512:	5F9A21BBD8503656136F3E1A4209B8A4F11B4BCC9B9F663C22EC12EA3FA6933AC037F82A5F45E70FF652A7CC1EBAA8419CDE0BE1D60BA1989D3B487F21014F A5
Malicious:	false

Reputation:	low
URL:	http://https://assets1.prezicdn.net/frontend-packages/react@17.0.0/umd/react.production.min.js
Preview:	/** @license React v17.0.0. * react.production.min.js. *. * Copyright (c) Facebook, Inc. and its affiliates.. *. * This source code is licensed under the MIT license found in the. * LICENSE file in the root directory of this source tree.. */.(function(){'use strict';(function(c,x){"object"===typeof exports&&"undefined"!==typeof module?x(exports):"function"===typeof define&&define.amd?define(["exports"],x):(c=c||self,x(c.React={}))})(this,function(c){function x(a){if(null===a||"object"!==typeof a)return null;a=Y&&a[Y]||a["@@iterator"];return"function"===typeof a?a:null}function y(a){for(var b="https://reactjs.org/docs/error-decoder.html?invariant="+a,e=1;e<arguments.length;e++)b+="&args[]="+encodeURIComponent(arguments[e]);return"Minified React error #"+a+"; visit "+b+" for the full message or use the non-minified dev environment for full errors and additional helpful warnings."}function v(a,b,e){this.props=a;this.context=b;this.refs=Z;this.updater=e||aa}function ba(){}function K(a,b,e

Chrome Cache Entry: 226

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1592
Entropy (8bit):	4.205005284721148
Encrypted:	false
SSDEEP:	48:ztSAS1OtmCtc7aIVmt4yyR9S2lKUyDWwh:RoOtmCtc7aCmVQHSRh
MD5:	4E48046CE74F4B89D45037C90576BFAC
SHA1:	4A41B3B51ED787F7B33294202DA72220C7CD2C32
SHA-256:	8E6DB1634F1812D42516778FC890010AA57F3E39914FB4803DF2C38ABBF56D93
SHA-512:	B2BBA2A68EDAA1A08CFA31ED058AFB5E6A3150AABB9A78DB9F5CCC2364186D44A015986A57707B57E2CC855FA7DA57861AD19FC4E7006C2C239C98063FE903CF
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="48" height="48" viewBox="0 0 48 48"><defs><style>.a{fill:none;}.b{fill:#404040;}</style></defs><rect class="a" width="48" height="48"/><path class="b" d="M40,32.578V40H32V36H28V32H24V28.766A10.689,10.689,0,0,1,19,30a10.9,10.9,0,0,1-5.547-1.5,11.106,11.106,0,0,1-2.219-1.719A11.373,11.373,0,0,1,9.5,24.547a10.4,10.4,0,0,1-1.109-2.625A11.616,11.616,0,0,1,8,19a10.9,10.9,0,0,1,1.5-5.547,11.106,11.106,0,0,1,1.719-2.219A11.373,11.373,0,0,1,13.453,9.5a10.4,10.4,0,0,1,2.625-1.109A11.616,11.616,0,0,1,19,8a10.9,10.9,0,0,1,5.547,1.5,11.106,11.106,0,0,1,2.219,1.719A11.373,11.373,0,0,1,28.5,13.453a10.4,10.4,0,0,1,1.109,2.625A11.616,11.616,0,0,1,30,19a10.015,10.015,0,0,1-.125,1.578,10.879,10.879,0,0,1-.359,1.531Zm-2,.844L27.219,22.641a14.716,14.716,0,0,0,.562-1.782A7.751,7.751,0,0,0,28,19a8.786,8.786,0,0,0-.7-3.5,8.9,8.9,0,0,0-1.938-2.859A9.269,9.269,0,0,0,22.5,10.719,8.9,8.9,0,0,0,19,10a8.786,8.786,0,0,0-3.5.7,8.9,8.9,0,0,0-2.859,1.938A9.269,9.269,0,0,0,

Chrome Cache Entry: 227

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	1104
Entropy (8bit):	4.655188383623911
Encrypted:	false
SSDEEP:	24:5bEqW5bEqQr25bEq1LVbEq5/25f+qq55f+qer25f+qJVf+qv/2n:yUpvZE2+R3+92+k+Y2
MD5:	595119F9E9E324A0991BD6B158C149D8
SHA1:	A653D42AADEAC2BB04CE68F24284DD495AA6FB91
SHA-256:	373A4512667422E934F89A0874D345FAF0BBE1ECE47153823EC07F99B22908A6
SHA-512:	DF93E9A335D52FB9EE0F4EFB02E7E636CFCB6F0D4FF1CE4593E378FA29E08CBA0AFC21EF3BA5CAEE3072D8A5329E413C0507307B05110AF69D36A150A4A68B3B
Malicious:	false
Reputation:	low
URL:	"https://prezi.com/api/v2/fonts/stylesheet/?fontFamily=Raleway,Roboto,Roboto,Raleway"
Preview:	@font-face {. font-family: "Raleway";. src: url("/api/v1/fonts/Raleway-Regular/");. font-weight: normal;. font-style: normal;.}.@font-face {. font-family: "Raleway";. src: url("/api/v1/fonts/Raleway-Italic/");. font-weight: normal;. font-style: italic;.}.@font-face {. font-family: "Raleway";. src: url("/api/v1/fonts/Raleway-Bold/");. font-weight: bold;. font-style: normal;.}.@font-face {. font-family: "Raleway";. src: url("/api/v1/fonts/Raleway-BoldItalic/");. font-weight: bold;. font-style: italic;.}.@font-face {. font-family: "Roboto";. src: url("/api/v1/fonts/Roboto-Regular2/");. font-weight: normal;. font-style: normal;.}.@font-face {. font-family: "Roboto";. src: url("/api/v1/fonts/Roboto-Italic/");. font-weight: normal;. font-style: italic;.}.@font-face {. font-family: "Roboto";. src: url("/api/v1/fonts/Roboto-Bold2/");. font-weight: bold;. font-style: normal;.}.@font-face {. font-family: "Robo

Chrome Cache Entry: 228

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	774
Entropy (8bit):	4.440917145843649
Encrypted:	false
SSDEEP:	24:tYU/duXMMrMpks43ZNpBefXUUBV1VK0T40:n/S6covnV1M0z
MD5:	40E2167E47CC055845E1E8ECF21070AC

SHA1:	FA22F2E65DE3B1DF56D3271B2FB9C3B6B9A5B7DB
SHA-256:	901592B708BB50F6DC82DCD9B86DC4BD00D2790B08451FBC987508990C2C29B2
SHA-512:	11485D42363D1D2939A1EA6CC4A70077059CEAACC7F7C388FA0B6A7D33F95CD563D7226BD22F9728C305D0DE54934ACDFCA347693113EC75A53A7B13C48568 8
Malicious:	false
Reputation:	low
URL:	http://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/share_icon.svg
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M18 6.5C18 7.88071 16.8807 9 15.5 9C14.9483 9 14.4383 8.8213 14.0249 8.51861L8.99671 11.8707C8.9989 11.9135 9 11.9566 9 12C9 12.0434 8.9989 12.0865 8.99671 12.1293L14.0249 15.4814C14.4383 15.1787 14.9483 15 15.5 15C16.8807 15 18 16.1193 18 17.5C18 18.8807 16.8807 20 15.5 20C14.1193 20 13 18.8807 13 17.5C13 17.4029 13.0055 1 7.307 13.0163 17.2127L8.09053 13.9289C7.65834 14.2857 7.1042 14.5 6.5 14.5C5.11929 14.5 4 13.3807 4 12C4 10.6193 5.11929 9.5 6.5 9.5C7.1042 9.5 7.65834 9.71434 8.09053 10.0711L13.0163 6.78727C13.0055 6.693 13 6.59715 13 6.5C13 5.11929 14.1193 4 15.5 4C16.8807 4 18 5.11929 18 6.5Z" fill="black"/>.</svg>.

Chrome Cache Entry: 229	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD 1
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/ic/uzn8uvtphy1xrj1sz5pgnchy5
Preview:	.............h(..f...HH...........(..00......h....6.. ....=..............@..........(....A..(....................(....................................."P.."""""""""""""""""""""""""""""""" ...3 333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333""" """""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 3333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""" """"""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333"""""""""""""""""""""""""""""""" ...33333333333 3333333333333333333"""""""""""""""""""""""""""""""" ...333333333333333333333333333333""""""""""""""""""""""""""""""

Chrome Cache Entry: 230	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (64348)
Category:	downloaded
Size (bytes):	109540
Entropy (8bit):	5.411461631157116
Encrypted:	false
SSDEEP:	1536:tJCLvzQOWtI6a14Wekiy53teCc58nUThe7qv0a9sIdsXjasXu5ZBm2aziyC+QNS/:tNLCjk3SDOUDQq
MD5:	B3D7D1FD0029796048820B8F515D1D4F
SHA1:	242F2EC5485FB5048E53A87FD37B2E6EAFB664B6
SHA-256:	0A19FCE040B8127F3E2E3ED609F7800153BE329D6420B53295FB79A4F40012EC
SHA-512:	9ECE9464B6DD79FE08E5242CF8BAC78A2BDE6507FF8865545BFE0AE2B089CC6EBE2BC550D5CBB1A3A943C12CF6CE04670B40950B6D8E25C2FE39505B1797A 619
Malicious:	false
Reputation:	low
URL:	http://https://connect.facebook.net/en_US/fbevents.js
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be .* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

Chrome Cache Entry: 231	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded

Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/o/11xzpntzrhhyygu5s58vnjupc
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 232

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.70 7,4.707,0,0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.611,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343 a2.952,2.952,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

Chrome Cache Entry: 233

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (559)
Category:	downloaded
Size (bytes):	120560
Entropy (8bit):	5.370822631971791
Encrypted:	false
SSDEEP:	1536:yMktdYd/K3b1jLayrgWjg+rAeaZmOusQqQoQjFB3OI6vHpSqZ6dZ:Xkc1KR/HrAeFvs0jF9OJxI
MD5:	23D1AC8B76C1430E7D568B4980CF812B
SHA1:	52D83603C4026874B1B723A3F72EFE1AF6FEE1D0
SHA-256:	FBDB08DDB8CD4F9F6481C61E93F84E7C57DF22D57F9FB21E138FEAB6E226553E
SHA-512:	13C3B31D6CCAA133942B38D927E6F309E0409D0331DEC55A8ADFC0227387D5348C33CBB3FF41613BF854975D2F5008282B45043329911BF33F14F3E7B6868AAC
Malicious:	false
Reputation:	low
URL:	http://https://assets1.prezicdn.net/frontend-packages/react-dom@17.0.0/umd/react-dom.production.min.js
Preview:	/** @license React v17.0.0. * react-dom.production.min.js. *. * Copyright (c) Facebook, Inc. and its affiliates.. *. * This source code is licensed under the MIT license found in the. * LICENSE file in the root directory of this source tree.. */.(function(){/*. Modernizr 3.0.0pre (Custom Build) | MIT.*/.'use strict';(function(M,ha){"object"===typeof exports&&"undefined"!==typeof module?ha(exports,require("react")):"function"===typeof define&&define.amd?define(["exports","react"],ha):(M=M||self,ha(M.ReactDOM={},M.React))})(this,function(M,ha){function m(a){for(var b="https://reactjs.org/docs/error-decoder.html?invariant="+a,c=1;c<arguments.length;c++)b+="&args[]="+encodeURIComponent(arguments[c]);return"Minified React error #"+a+"; visit "+b+" for the full message or use the non-minified dev environment for full errors and additional helpful warnings."}.function Ta(a,b){gb(a,b);gb(a+"Capture",b)}function gb(a,b){lb[a]=b;for(a=0;a<b.length;a++)yf.add(b[a])}function ki(a){if(zf.call(Af,a)

Chrome Cache Entry: 234

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (20116), with no line terminators
Category:	downloaded
Size (bytes):	20116
Entropy (8bit):	5.26916393157098
Encrypted:	false
SSDEEP:	384:uWbVGz7FGS2dkTDRDJ8+oDFSw6D10RG0JQ7NsSiAMs:u2VGz7FGSs9RSGmsSBV
MD5:	D02B9ACED3FDAE32C361627503D47A41
SHA1:	848DFD4B6BE3490A67FD7C1F73B24A2B5A06A742
SHA-256:	497F358C30FCC7118A3F1A2C9DC435BB47D6352D65B7EEBD2516A53B94EA213C
SHA-512:	39E839ED4875C9236F4141EE67861CFEAEBDECB478311A1FBCE32229B45AC53BB4674E50BF47AAE24071A4E7AE1664AC9FDECB9DFC2E563C3D2664A0E9A100D7
Malicious:	false
Reputation:	low
URL:	http://https://prezi.com/api/v2/prezigram/getProjectContent?projectId=rx6p99-v72pt&appVersion=c1425b2827bd9b1b3f231dc8395ca9b1d5fa01f9
Preview:	{"content":{"allowFullscreen":true,"allowToShare":true,"assets":{"1457f10b-2758-4dcf-8924-27c1fe200d9f":"/d7274b984072740d5a511cbd1b9fba04b68887843c80b84c705a373e375ca1713916 51f42f85f8422a8fe4527d93ef619c63026e499e2ef5a547354b41427de1","24eb1e55-087d-48fb-a6be-1574685eea72":"/4d6a0d49c2a6a8513d5869433bbde49c96a57604d7903c803dd23eabb618389e1eff2df277ff0b03f90a3162fa3472559bfdaafd6db60115b22564b5f3c1273a"},"content":{"blockOrder":["ecb6c8f2-75e1-4a0f-aae4-87ebb7d0958b"],"blocks":{"ecb6c8f2-75e1-4a0f-aae4-87ebb7d0958b":{"design":{"header":{"text":""},"hideFooter":false},"entities":["be4ef4f1-9bda-4868-833b-6f7ddd39f7e93b444f6f-a0d4-448e-a045-09faedb5d716","7be905d4-b536-4ec6-899b-6fae97fbf057c0fafb95-7bf2-482b-abbf-b9c85e38addf","f6e52ba6-be06-45c9-af4e-f7be6071980a76b59324-0620-4c13-8d76-22b515678472","66892917-4e63-4eda-84de-8493bf6a1e55c964cca9-296e-4fdc-9b11-ff8dbb5bebc8","9677f596-25fb-4617-82c8-f99cb192bb9d6ed92c0f-ed67-42c9-b07a-a9747e94ed2b"]}},"entities":{"be4ef4f1-9bda-4868-833b

Chrome Cache Entry: 235

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1327
Entropy (8bit):	5.353759587857711
Encrypted:	false
SSDEEP:	24:2dzAOx8LfHgonKNh6dRfXU8mtT+n5QOrVnmrUaTPz:czAOKfHgAKN6/UAlxnmDTL
MD5:	1AA2C19A21128E162921410EDC867FCE
SHA1:	5FA9A5BA1B9D2A37E0419AD27DF27CD0A8A317F6
SHA-256:	C6EFBAC4C969E83D254E91E4BFA5F350B432EB9B879FE1A6FAFEEEFF1355CE5D
SHA-512:	AAE2EA245FDCC91279642BCD53E22B7E341FBE0ABD017976ADB870BEEA23D9842566FC812A31B733DC6BC8534B6C0961F5710829158D0EF0D3826606AA95BB97
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/footers/twitter-icon.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) --><!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"><svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="20px" height="16px" viewBox="0 0 20 16" style="enable-background:new 0 0 20 16;" xml:space="preserve"><style type="text/css">...st0{fill:#152235;}.</style><title>twitter</title><desc>Created with Sketch.</desc><g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-825.000000, -719.000000)">...<g id="twitter" transform="translate(825.000000, 719.000000)">....<g id="Twitter">.....<path id="Shape" class="st0" d="M17.3,4.2c0,0.2,0,0.3,0,0.5c0,5-3.8,10.7-10.7,10.7c-2.1,0-4.1-0.6-5.8-1.7.....c0.3,0,0.6,0.1,0.9,0.1c1.8,0,3.4-0.6,4.7-1.6c-1.7,0-3-1.1-3.5-2.6c0.2,0,0.5,0.1,0.7,0.1c0.3,0,0.7,0,1-0.1.....c-1.7-0.3-3-

Chrome Cache Entry: 236

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (50758)
Category:	downloaded
Size (bytes):	51039
Entropy (8bit):	5.247253437401007
Encrypted:	false
SSDEEP:	768:E9Yw7GuJM+HV0cen/7Kh5rM7V4RxCKg8FW/xsXQUd+FiID65r48Hgp5HRl+:E9X7PMIM7V4R5LFAxTWyuHHgp5HRl+
MD5:	67176C242E1BDC20603C878DEE836DF3
SHA1:	27A71B00383D61EF3C489326B3564D698FC1227C
SHA-256:	56C12A125B021D21A69E61D7190CEFA168D6C28CE715265CEA1B3B0112D169C4
SHA-512:	9FA75814E1B9F7DB38FE61A503A13E60B82D83DB8F4CE30351BD08A6B48C0D854BAF472D891AF23C443C8293380C2325C7B3361B708AF9971AA0EA09A25CDDA
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/boot/jnhzyzurxgsnu5pypt1v58h1c

Preview:	/*!. * Bootstrap v4.1.3 (https://getbootstrap.com/). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function l(r){for(var t=1;t<arguments.length;t++){var o=null!=arguments[t]?arguments[t]:{},e=Object.keys(o);"function"==typeof Object.getOwnPropertySymbols&&(e=e.concat(Object.getOwnPropertySymbols(o).filter(function(t){return Object.getOwnPropertyDescriptor(o,t).enum

Chrome Cache Entry: 237

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	6295
Entropy (8bit):	4.061575620688071
Encrypted:	false
SSDEEP:	96:2R9mBjCvE6oXsQnnIGONQ6ezu0D70q35KZVoUsG/uhsfm4F9p8DJR7DTT:2R4PDPnITq6ezu0DQoKLo4/Ksfm88Dr
MD5:	6E2D3AC939C8C7626F4C206C2794CD3E
SHA1:	FEB4DF0FB503D439FB2C21D056BB783CEAA759F4
SHA-256:	10BBB43F53790493B1156E3DCDA5AC830C7E826B7775A64D11A18DACCB9562CB
SHA-512:	83BE56C2774726348356C85BB8D28D61EE747C73357D85FE9AABAD4CCD9727B254C18C638021ABE26ED96A687369B4E0AB614520731A644C33BD99C5E00142A
Malicious:	false
Reputation:	low
Preview:	<svg width="66" height="24" fill="none" xmlns="http://www.w3.org/2000/svg">. <g clip-path="url(#clip0)" fill="#152235" opacity=".8">. <path d="M28.79 18.137 V6.194h4.835c2.203 0 3.801 2.019 3.801 3.97 0 2.034-1.497 3.969-3.717 3.969h-2.597v4.003H28.79zm2.322-6.04h2.463c.858 0 1.497-.756 1.497-1.933 0-1.228-.774-1.934-1.598-1.934h-2.361v3.868zM43.99 11.135c-1.362.017-2.52.792-2.99 1.784v5.218h-2.254V9.323h2.069v1.884c.622-1.194 1.782-2.002 2.724-2.002.236 0 .354 0 .454.017l-.002 1.913zM44.602 13.78c0-2.506 1.783-4.609 4.66-4.609 2.876 0 4.38 2.09 4.38 4.478 0 .286-.041.62-.075.804h-6.576c.117 1.38 1.16 2.203 2.338 2.203 1.065 0 1.907-.653 2.193-1.376l1.902.72c-.639 1.345-2.153 2.305-4.104 2.305-3.028 0-4.718-2.086-4.718-4.525zm6.93-.79c-.118-1.312-1.077-2.187-2.305-2.187-1.21 0-2.17.875-2.27 2.187h4.575zM63.248 6.985c0-.656.589-1.228 1.245-1.228.64 0 1.245.572 1.245 1.228 0 .672-.606 1.244-1.245 1.244-.655 0-1.245-.588-1.245-1.244zm.118 11.152V9.323h2.254v8.814h-2.254zM53.945 18.137l

Chrome Cache Entry: 238

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (26940), with no line terminators
Category:	downloaded
Size (bytes):	26940
Entropy (8bit):	5.191002853668852
Encrypted:	false
SSDEEP:	768:Y8m2Jsc3c/t0Wrx3iCOrXojMMO0FhtBG5+r:YN2JsztnMrXoIyj
MD5:	D1F5D110170197D5B3C2890178E0A6E7
SHA1:	F39E7A56A88614FE9500FF62930E5A7EB3BA2A39
SHA-256:	BA0E8670118E454F4387F11925C550BEC864CCD1BF941DA4B6B4F33A8A0DF1BC
SHA-512:	1CE900E2C39321992E3A201D508D1E8BBD5A52EEB2AF8DD47018C24D27E6FAAC05F87E3B4DA152EA8053B9CBEC9F528431CD3FC64C25672D735D276B575751D7
Malicious:	false
Reputation:	low
URL:	http://https://prezi-analytics.com/t.js
Preview:	!function(t){var e={};function r(n){if(e[n])return e[n].exports;var o=e[n]={i:n,l:!1,exports:{}};return t[n].call(o.exports,o,o.exports,r),o.l=!0,o.exports}r.m=t,r.c=e,r.d=function(t,e,n){r.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:n})},r.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},r.t=function(t,e){if(1&e&&(t=r(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var n=Object.create(null);if(r.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)r.d(n,o,function(e){return t[e]}.bind(null,o));return n},r.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return r.d(e,"a",e),e},r.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},r.p="",r(r.s=20)}([function(t,e,r){t.exports=!r(3)((function(){return 7!=Object.defineProperty({},"a",{get

Chrome Cache Entry: 239

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (59010)
Category:	downloaded
Size (bytes):	59037
Entropy (8bit):	5.3749393050585645
Encrypted:	false
SSDEEP:	1536:o2G8uP35++H2RNZs2Zqt4KzpvEJ2n+e5S5:o2OEETtDy2nD50
MD5:	8BD6AF99873A97F227A3CF95B41BF64C
SHA1:	46EC9740EA04954840CB7816C169C0B0A2424109
SHA-256:	7DE672FC348743A03356ECD3F683CB6361FCABD4E1D6AD4D177CE6AD3FF7FA2C
SHA-512:	C50D70CB84F50319DAC1DA2DA7BC61B2F4271DD949E6527BC6552D4A631A7746D47EF1B696F85B35F5368CB7AA8298999394AE20C563F5452FC16837F09D23A

Malicious:	false
Reputation:	low
URL:	http://https://cdn.taboola.com/libtrc/unip/1013987/tfa.js
Preview:	/*! 20230319-5-RELEASE */..function _typeof(t){"@babel/helpers - typeof";return(_typeof="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){ return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(t)}!function(t){var e='TFASC' ;e.indexOf("{jsScope}")>-1&&(e="TRC"),t[e]||(t[e]={})}(window),function(t,e){t.TRC=t.TRC||{};var i=function t(){return!0},n=function i(n,r,o,s){var a=n+"/"+encodeURICompo nent(o||t.TRC.publisherId)+"/log/3"+"/"+r;return s&&(a+="?"+e.TRCLogger.formatParams(s)),a},r=function e(n,r){var o,s=new(t.XDomainRequest||t.XMLHttpRequest);re turn s.open(n,r),s.onload=i,s.onerror=i,s.ontimeout=i,s.onprogress=i,s.withCredentials=!0,s};t.TRC.TRCLogger=e.TRCLogger={post:function i(o,s,a,c,u,l){var f=n(o ,s,c,u),d=r("POST",f);l&&"function"==typeof t.navigator.sendBeacon?t.navigator.sendBeacon(f,e.TRCLogger.formatBeaconParams(a)):(d.setRequestHeader&&d. setRequestHeader("Content-Type","applica

Chrome Cache Entry: 240

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	15086
Entropy (8bit):	3.9672871989666185
Encrypted:	false
SSDEEP:	96:3WqX555551hvQoKtKQQE7cvE/hfpMc07iBSD3vmduZbdZyW+6FLWqdoAl1To0Pyv:RoSEovT7iBSz6UhZygFLpoZ0qNwqjz7J
MD5:	0520A574E13AF7D1B6F2C608364577FF
SHA1:	360038AEF0A5E9FF4479A5EB47289BCFF56F4FE4
SHA-256:	2E2801B1412647B7E09AE1DA78685C4E4B4AD98945BE191650D84151A23D546F
SHA-512:	A1474DD394EC18FE9DAA420A3FA79036154EB72354ACCE2B9109510F141866CAF7067D5856514D1CC20D47D39EA339C638640C0FEC86D62CA32FFA10516A98A E
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico?v=2
Preview:	..... .h...6... ....00.... ..%..F...(..... ....1X..2...2...1...2...2...1X.....6!..2... 2...1X..1...U...1...1X..2...2...6!.....6!..2...2...,...2...2...1...2...2...,...2...2...6!.....2...2...4@..2...2...2...@...2...2...2...4@..2...2.....1X..2...,...2...2.....1.....1. .....2...2...,...2...1X.....2...1X..2...2...1.....1.....1.....1...2...2...1X..2.....2...1...2...23..1.....1.....1.....1...23..2...1...2.....1...U...1...@...1.....1.....1.....1...;...1...U...1..... ..2...1...2...23..1.....1.....1.....1...23..2...1...2.....2...1X..2...2...2.....1.....1.....2...2...2...1X..2.....1X..2...,...2...4@.....1.....1.....4@..2...,...2...1X.....2...2...4@.. 2...2...2...@...2...2...2...4@..2...2.....6!..2...2...,...2...2...1...2...2...,...2...2...6!.....

Chrome Cache Entry: 241

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	TrueType Font data, digitally signed, 19 tables, 1st "DSIG", 23 names, Macintosh, Font data copyright Google 2011RobotoRegularGoogle:Roboto:2011Roboto RegularVe rsion 1.00000; 201
Category:	downloaded
Size (bytes):	158604
Entropy (8bit):	6.386329070944693
Encrypted:	false
SSDEEP:	3072:CPfJU8fbEc6MjbUzk0pewfMi4dbARp/cZX/ogD8:CPx4k00wEOcc
MD5:	5673DA52C98BB6CB33ADA5AAF649703E
SHA1:	A18DCBF99C8D2325C2FBF22A64E8CC28A0CF4D3B
SHA-256:	16466EF65064E6F3885A6D2806B8949AC1AC38B524DD0CF8FC96565EB4CC28E8
SHA-512:	9728536F1E67069B4C44EFFC3245D81F61FB79C811A4BD2D3879F57EB220E475DFEE0639DBECBE03F411AA8F1E2E84FC38A966BA38982B0B35E2B2A98549583 A
Malicious:	false
Reputation:	low
URL:	http://https://prezi.com/api/v1/fonts/Roboto-Regular2/
Preview:	.....0DSIG.....k.....GDEF.`.a...<...HGPOS.*`.....GSUB.&.....$....OS/2..)....`cmap..N4.....cvt .....a....&fpgm...T..b....%gasp.....a.....glyf.....Z.head.....6hhe a..... ...$hmtxn.v....D...4kernwal}...x..0.loca..[...2.....maxp.U.}..:.... name.....:...>post..b...>...#.prep.....k4...M.....4...$./...H.H...O.P...R.R...h.j..... .....,..DFLT.....kern.....K.T.p...w.....<.B.H.....>.`.f.....&.L.r.x.b.h.....8.R.`.~.....j...N.`.v.....@.f..... .F.L.R.X.^.....,J.h....." .D.f.....L.....N.l.~.....2.8.N.T.j.p.....6.X.^.....6.d.....8.Z.....f.....8.Z.|.....J.`.....:..... . B L!6!.!."0"6"X".".#.#.#B#X#r#.#.#.#. #.$.$.$.$Pf|$.%p%.%.%.%.&.&(&v&.&.'X'z'.(J(x(.(.).)()v).).).*.*(*:+$+r+.+.,.,J,p,.,.,.,.,.,.-.-.- -6-X-r-.-.-.-.....@.b.|...../ /B/././.0.0@0^0x1>1H2.2p2v

Chrome Cache Entry: 242

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	533
Entropy (8bit):	4.70497619638867
Encrypted:	false
SSDEEP:	12:trwdU/gKuXM65PCpWcuGNNPB5IJS71wx4bumrYR0:tYU/duXMMP3cuGNNp5SEO4ymUR0

MD5:	66D50AF6577AA40B5139861D53DC77B3
SHA1:	7844C61A29625582620D7040B400BE5EA020E6C7
SHA-256:	B1C52A735B65D540A88E799748E01B5B7B317CE52C51361A620D804390E10D3D
SHA-512:	CE4FDC7F0A3E20388FF42F28CF6585E6B12D4B50E8A0182182790248288DB727A31A1EBDE248DB6D21D38F9FBDAFEA3B68A35F6F7DEF4175B8CFF93A6E1520 3
Malicious:	false
Reputation:	low
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M10.0136 17.835 7L12.0136 5.83569L13.9864 6.16449L11.9864 18.1645L10.0136 17.8357ZM17.5858 12.0001L14.2929 8.7072L15.7071 7.29299L19.7071 11.293L20.4142 12. 0001L19.7071 12.7072L15.7071 16.7072L14.2929 15.293L17.5858 12.0001ZM9.70714 15.293L6.41424 12.0001L9.70714 8.7072L8.29292 7.29299L4.29292 1 1.293L3.58582 12.0001L4.29292 12.7072L8.29292 16.7072L9.70714 15.293Z" fill="black"/>.</svg>.

Chrome Cache Entry: 243

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	6295
Entropy (8bit):	4.061575620688071
Encrypted:	false
SSDEEP:	96:2R9mBjCvE6oXsQnnIGONQ6ezu0D70q35KZVoUsG/uhsfm4F9p8DJR7DTT:2R4PDPnITq6ezu0DQoKLo4/Ksfm88Dr
MD5:	6E2D3AC939C8C7626F4C206C2794CD3E
SHA1:	FEB4DF0FB503D439FB2C21D056BB783CEAA759F4
SHA-256:	10BBB43F53790493B1156E3DCDA5AC830C7E826B7775A64D11A18DACCB9562CB
SHA-512:	83BE56C2774726348356C85BB8D28D61EE747C73357D85FE9AABAD4CCD9727B254C18C638021ABE26ED96A687369B4E0AB614520731A644C33BD99C5E00142A
Malicious:	false
Reputation:	low
URL:	http://https://cdn.jifo.co/js/dist/6e2d3ac939c8c7626f4c206c2794cd3e.svg
Preview:	<svg width="66" height="24" fill="none" xmlns="http://www.w3.org/2000/svg">. <g clip-path="url(#clip0)" fill="#152235" opacity=".8">. <path d="M28.79 18.137 V6.194h4.835c2.203 0 3.801 2.019 3.801 3.97 0 2.034-1.497 3.969-3.717 3.969h-2.597v4.003H28.79zm2.322-6.04h2.463c.858 0 1.497-.756 1.497-1.933 0-1.228-.774- 1.934-1.598-1.934h-2.361v3.868zM43.99 11.135c-1.362.017-2.52.792-2.99 1.784v5.218h-2.254V9.323h2.069v1.884c.622-1.194 1.782-2.002 2.724-2.002.236 0 .354 0 .454.017l-.002 1.913zM44.602 13.78c0-2.506 1.783-4.609 4.66-4.609 2.876 0 4.38 2.09 4.38 4.478 0 .286-.041.62-.075.804h-6.576c.117 1.38 1.16 2.203 2.338 2.203 1.065 0 1.907-.653 2.193-1.376l1.902.72c-.639 1.345-2.153 2.305-4.104 2.305-3.028 0-4.718-2.086-4.718-4.525zm6.93-.79c-.118-1.312-1.077-2.187-2.305-2.187-1.21 0- 2.17.875-2.27 2.187h4.575zM63.248 6.985c0-.656.589-1.228 1.245-1.228.64 0 1.245.572 1.245 1.228 0 .672-.606 1.244-1.245 1.244-.655 0-1.245-.588-1.245-1.244zm.1 18 11.152V9.323h2.254v8.814h-2.254zM53.945 18.137l

Chrome Cache Entry: 244

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (505)
Category:	downloaded
Size (bytes):	978
Entropy (8bit):	5.282825774093728
Encrypted:	false
SSDEEP:	24:4QquNqRZRR94uHstvQuRWZ0fpckEX3hRRquHNilFepRWZFXDGBeI:4QqumpcdpwmpckY3hOkpwvDvl
MD5:	FB3354F3E88F8030709C525502B1B1E1
SHA1:	0B7B94BAD14D3351E8B4FE814D06EDF847D69A41
SHA-256:	4F28BBE804E7455E3D8C1729C70522F12FF9F561B83A82BBC29956FF4F4327DC
SHA-512:	A4CC84C113739F2BBBABDD03ECB0509FEF53FA39FCA38A665E72026584366518ABA42362CA87DE6371DE360E351D58999727B73AD8413AE8B0CAA611EEE348 E4
Malicious:	false
Reputation:	low
URL:	http://https://js.hs-scripts.com/20307117.js

Preview:	// HubSpot Script Loader. Please do not block this resource. See more: http://hubs.ly/H0702_H0..!function(e,t){if(!document.getElementById(e)){var c=document.cr
	eateElement("script");c.src="https://js.hs-analytics.net/analytics/1679350200000/20307117.js",c.type="text/javascript",c.id=e;var n=document.getElementsByTagNam
	e("script")[0];n.parentNode.insertBefore(c,n)}}("hs-analytics");.var _hsp = window._hsp = window._hsp || [];. _hsp.push(['addEnabledFeatureGates', []]);.!function(t,e,r){
	if(!document.getElementById(t)){var n=document.createElement("script");for(var a in n.src="https://js.hs-banner.com/v2/20307117/banner.js",n.type="text/javascript",n.id=t
	,r)r.hasOwnProperty(a)&&n.setAttribute(a,r[a]);var i=document.getElementsByTagName("script")[0];i.parentNode.insertBefore(n,i)}}("cookieBanner-20307117",0,{"data-
	cookieconsent":"ignore","data-hs-ignore":true,"data-loader":"hs-scriptloader","data-hsjs-portal":20307117,"data-hsjs-env":"prod","data-hsjs-hublet":"na1"});

Chrome Cache Entry: 245

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65371)
Category:	downloaded
Size (bytes):	173295
Entropy (8bit):	5.1365390025500455

Encrypted:	false
SSDEEP:	1536:8Qwd23nKXt4QH0r3IF/jJ5vIi+UMRyFdBXOVr6nc4VpvNe:T3O/jLIi+UMRyFdBeVwrpvNe
MD5:	5DE45A76C20330C45D5574BDA9774BD0
SHA1:	9E74C1F1D826C7C3127946CA2AA336ED5CE8FB11
SHA-256:	FBCE21A87DF40BBA46EB8B58B21293959263B11581B20A92FC590C0046FB3590
SHA-512:	9032233F3E9C08EAEE11C58A75CD422DDC1F5008038FA5A6E7310C118B66F82D47113DFD1458B70E5B21329B6114DBB207B4820390AF427B5EF74CE5C0C2A9E
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/fbce21a87df4.css
Preview:	/*!. * Bootstrap v3.3.5 (http://getbootstrap.com). * Copyright 2011-2015 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). *//*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.badge,.label,b,optgroup,strong{font-weight:700}.label,audio,canvas,progress,sub,sup,video{vertical-align:baseline}.collapsing,.dropdown-menu .divider,.nav .nav-divider,.sr-only,svg:not(:root){overflow:hidden}hr,img{border:0}#footer-raleway .copyright a,#footer-raleway .copyright a:active,#footer-raleway .copyright a:hover,#footer-raleway .copyright a:visited,.btn-link:focus,.btn-link:hover,a:focus,a:hover{text-decoration:underline}html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{backg

Chrome Cache Entry: 246

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	5.555714280948775
Encrypted:	false
SSDEEP:	24:2dzAOx8LfCNQ/6h6pxrS8BqT+TvP14Tl5H:czAOKfEq6YGB+TvP14r
MD5:	73605F769148DB36D71439F235DD2B8E
SHA1:	34535388896117DAB0A48B1FD19118F8DAB21142
SHA-256:	70ED38179144E26BC93DCB6FA40F1396CCDD02F6BC04AD4700210582574A75DC
SHA-512:	F882FB739F80192CE90F03A658E2F403FDBFB926D27A9F8EFFC16FA0CF8B088F55CAC78993F569738B18E3E586906E587075DB00A0F082F2339DF3BA43B6C7C6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="18px" height="18px" viewBox="0 0 18 18" style="enable-background:new 0 0 18 18;" xml:space="preserve">.<style type="text/css">...st0{fill:#152235;}.</style>.<title>facebook</title>.<desc>Created with Sketch.</desc>.<g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-778.000000, -718.000000)">...<g id="facebook" transform="translate(778.000000, 718.000000)">....<g id="Facebook">.....<path id="Shape" class="st0" d="M16,0H2C0.9,0,0,0.9,0,2v14c0,1.1,0.9,2,2,2h7v-7H7V8.5h2v-2c0-2.2,1.2-3.7,3.8-3.7l1.8,0v2.6.....h-1.2c-1,0-1.4,0.7-1.4,1.4v1.7h2.6L14,11h-2v7h4c1.1,0,2-0.9,2-2V2C18,0.9,17.1,0,16,0L16,0z"/>....</g>..

Chrome Cache Entry: 247

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1120
Entropy (8bit):	5.55518211480394
Encrypted:	false
SSDEEP:	12:TMHdPhRi/nzV7EIMu5E4BL/KYf3yN8jN/HrKvvHkl8LLrgEKbUj48NRT9suNl7l8:2dzAOx8LfCNQ/+vh6Tj48N3lPlInQ
MD5:	22B734D58BE41F35CACB1D206AA1088D
SHA1:	E09943F68AF1B60C3B868E6FFADB42B653D06293
SHA-256:	58A112A455DAA8A0912990D4E30FEFB594C1F4B79FB386EEB7B64B9D18B0E8C0
SHA-512:	A61E49382DF06AF514C56B0F6C10DA19F2B1958607D067F51A37F7360A426F24C73833AC8442A52B521CD578E02DF76746EE2E6DF18B726962AE60CB1FCFE9F5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="18px" height="18px" viewBox="0 0 18 18" style="enable-background:new 0 0 18 18;" xml:space="preserve">.<style type="text/css">...st0{fill:#152235;}.</style>.<title>linkedin</title>.<desc>Created with Sketch.</desc>.<g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-874.000000, -718.000000)">...<g id="linkedin" transform="translate(874.000000, 718.000000)">....<g id="LinkedIn">.....<path id="Shape" class="st0" d="M4,2c0,1.1-0.7,2-2,2C0.8,4,0,3.1,0,2.1C0,1.1,0.8,0,2,0S4,0.9,4,2L4,2z M0,18h4V5H0V18L0,18z..... M13.6,5.2c-2.1,0-3.3,1.2-3.8,2H9.7L9.5,5.5H5.9C5.9,6.6,6,7.9,6,9.4V18h4v-7.1c0-0.4,0-0.7,0.1-1c0.3-0.7,0

Chrome Cache Entry: 248

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 39504, version 1.0
Category:	downloaded

Size (bytes):	39504
Entropy (8bit):	**7.9954893142798**
Encrypted:	**true**
SSDEEP:	768:HqXs5lLWZadl1NSAjZbvF2H+H0ZUIFP2rzyYOn01hw2ju:HqXsDWeMONvF2HvZUX6YOn015y
MD5:	0DDC93B358BCFBB4734C3294621E38F1
SHA1:	33EF6587AE0968E8F02ED8FA8582D8BD35E9CCB6
SHA-256:	019A0B8AB8AE844C43502C1C7F1DCF194FABBB0AEC5746D7B9E7465C938C60BA
SHA-512:	719C708DD7663491DB15B95FB2698791186725A96F7F1CB4748CBDEE4161A351AD9395822D8EC37863CBC2496302DB6E41764070693177B3D2C9D4FCBBC8AF8
Malicious:	false
Reputation:	low
URL:	**http**://https://assets1.prezicdn.net/common/fonts/raleway-bold.woff2
Preview:	wOF2.....P.....!\.....?FFTM..T...6..8.`..V.....v..0..6.$..\. ..W..H[.....n#....wT..1....(.>1.y..:B.T.c/.....~H.....K../..%...._...)e:.&s..53.N....Ft.....92r...t.e....9 h.+...lo.F..E....r.r7..JD.N.+=....t.....e.....a.b.....I.W.TI.L..q3*GS..I....9....v...y.".}.;\..Y.....8.I"Nbj....\...M...>y.J6vxIXS.h. ..L}...=..y.F3.i...%.....+KL.....?...J.,....z..DDD... M%UR%.o.....(..R..:.TI.L..x&...g..p..Q1.f&.A.....I.F>?.`[..S_...I..C3.....d.P..#Y....Z.....9.g. ..; G..?..B.....+T.....c...FmT.1`.L.D@B..u.4....Q.....O....L.Ae..q....xTU.....0T.!. [G....J..U.$k.Q5jD..IK...I.Q...../..s....:.!..m....M..n....E...?..{gF.5.${.....I.R`.e...J.F.tV.....g.....2..\..F,mJ..#<.....R.....]...6....wY.j.Q}..m..CUU..Q...Q.."""""""".8.8.GDD./.k./..~`Wc _..T...7q#....=..8...b6v.k3.3.....R...../...e7ev...AN...$.,$.....%.T....Bol7C..i...W.Q...`...x".tB..W5.....i.....M..FS...w....7^..b\.:5j.t..}..y.>.../.3._]B.Te..F..>uX.*.

Chrome Cache Entry: 249

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	400
Entropy (8bit):	4.705757983822934
Encrypted:	false
SSDEEP:	12:trwdU/gKuCC1RFoVbXoGof0jK1y4mqPBpGzK0:tYU/du/1joai2HNPBv0
MD5:	478D5FBDFB49D87F0498747623BC7B8F
SHA1:	1A65D0BAA57A07917F3A7F65FCA6B3A13D12FF75
SHA-256:	BAA5D917882C3FDD1E76A0BE5DDB9A02ADDEC5F5BB1A1DDA216DFED9617CF48A
SHA-512:	1A51CB61A8793B9347800EE771C185AEAE9F9F0B7B7EFC32A4625B10E9A7F19BAECA89AB2ABF50ACD2B17F6D086C0B471BB0EAA8F8D357ACCB6CCED0BBA 2CB1D
Malicious:	false
Reputation:	low
URL:	**http**://https://d2pj2twnjx3fya.cloudfront.net/frontend-packages/viewer-container/report_icon.svg
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path d="M13.8 6.72394C13.2886 6.15421 13.4106 5.55364 12.9333 4.9538C11.2259 2.80775 6 4.9538 6 4.9538V20H8V14C8 14 10.87 12.5825 12.0667 13.8045C12.6018 14.351 12.4408 14.9878 12.9333 15.5746C14.4752 17.4117 19 15.5746 19 15.5746V6.72394C19 6.72394 15.1722 8.25269 13.8 6.72394Z" fill="black"/>.</svg>.

Chrome Cache Entry: 250

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4 C
Malicious:	false
Reputation:	low
URL:	**http**://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=7ab14ea51c463602
Preview:	GIF89a.....!.....,.....D.;

Chrome Cache Entry: 251

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, Unicode text, UTF-8 text, with very long lines (4445)
Category:	downloaded
Size (bytes):	38757
Entropy (8bit):	5.120699638056435

Encrypted:	false
SSDEEP:	768:cpuw/9lCWTQKfwusuCvi48xj9A7ldwWh4ThknlpF8Jejw7S0YGwXXwr0rtlmbieU:c0w1lCWTQ+i
MD5:	C5EAEFE5E9B97CB83738719C799F7F33
SHA1:	D6D47A75EFBE3B34CDFEEB586CA9A1C5CA06F4A4
SHA-256:	06BED599993CD2E0F25E4AA3ED8F39467E38881069B0E08AEE238E36C0CC444D
SHA-512:	819E9CC699280E71F1251E156B4CA896B56997C660AB6F7DB40EC56ABDF839A2A27D7E55C143D40EF8E9E4D793417459F7EC368FFBAF0F18484AF3DB8B34AA1E
Malicious:	false
Reputation:	low
URL:	http://https://prezi.com/i/rx6p99-v72pt/leibowicz-law-llc/
Preview:	<!DOCTYPE html><html lang="en"><head ><title>. Leibowicz Law LLC by Secure Message on Prezi Design.</title> Common Metadata --><meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="verify-v1" content=" eyaAlbc+dH3kl2VfR/7FXmEfNj940c7ERDeqoUWtmUk="><meta name="msvalidate.01" content="256D24D16694018A98CD38E3CB2E4132"><meta name="y_key" content="c35eebc2904a0fbc"><link rel="shortcut icon" href="https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/favicon.ico?v=2" type="image/x-icon"><link rel="apple-touch-icon-precomposed" href="https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/prezi-apple-touch-icon.png"><meta property="og:site_name" content="prezi.com"/><meta property="fb:app_id" content="298315034451"/><meta property="twitter:account_id" content="35860484" /> in case of no_index flag we don't want a

Chrome Cache Entry: 252

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6147)
Category:	downloaded
Size (bytes):	6148
Entropy (8bit):	4.991651414223992
Encrypted:	false
SSDEEP:	96:C97L9HO3Nt0l/JL+G2eO6Zhs0KH2cz+Ddo:ZOP+0fKZzZ
MD5:	BC8F5E4BA0EA8CC6759CD3707287682B
SHA1:	8141A965CD00117D03DA245AC965AE3A722DFCFC
SHA-256:	582A1ED459F57ADE6A96EE74ACC97B44F30F54531D6E4DC0A5C29B2A21AD0790
SHA-512:	8006E12C53B6009AE3DE931A65B930D2722A574283DC08087258A12F1E928F9B75AEAF047E0C63CAF9CDE6E8F8145D1853EA9918E2263BA1245713174FEE943C
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/js/582a1ed459f5.js
Preview:	;(function(window,document){"use strict";var features={bind:!!function(){}.bind,classList:"classList"in document.documentElement,rAF:!!(window.requestAnimationFrame||window.webkitRequestAnimationFrame||window.mozRequestAnimationFrame)};window.requestAnimationFrame=window.requestAnimationFrame||window.webkitRequestAnimationFrame||window.mozRequestAnimationFrame;function Debouncer(callback){this.callback=callback;this.ticking=false}Debouncer.prototype={constructor:Debouncer,update:function(){this.callback&&this.callback();this.ticking=false},requestTick:function(){if(!this.ticking){requestAnimationFrame(this.rafCallback||(this.rafCallback=this.update.bind(this)));this.ticking=true}},handleEvent:function(){this.requestTick()}};function isDOMElement(obj){return obj&&typeof window!=="undefined"&&(obj===window||obj.nodeType)}function extend(object){if(arguments.length<=0){throw new Error("Missing arguments in extend function")}var result=object||{},key,i;for(i=1;i<arguments.length;i++){var r

Chrome Cache Entry: 253

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6190), with no line terminators
Category:	downloaded
Size (bytes):	6190
Entropy (8bit):	5.500015767498455
Encrypted:	false
SSDEEP:	96:NXInPtxfXAQ+QagfBUoh2dflSxdRFNqrEspOdJkmFA4k:aPnIy9h21lSmESaJkmWz
MD5:	B55FBBCA0F0AC20A41D9ABA8533ED1C5
SHA1:	3E317D4905C20267F3DD2CB894DB16A2145F195E
SHA-256:	EFDB5BCC25EFA09532FBBF93E67A4BD0F74016AD3CFE118A2FBC94296ADF875B
SHA-512:	E07114ACBC41FC25DFFECDC93C2629808B8FB7CD31C898D75BE23B04F6DA633064AAA4DE0CB9D340B990E8127EE37C4BBB2C1504ED180B482E0E1819146596F
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/styles/challenges.css
Preview:	*{box-sizing:border-box;margin:0;padding:0}html{line-height:1.15;-webkit-text-size-adjust:100%;color:#313131}html,button{font-family:system-ui,-apple-system,BlinkMacSystemFont,Segoe UI,Roboto,Helvetica Neue,Arial,Noto Sans,sans-serif,Apple Color Emoji,Segoe UI Emoji,Segoe UI Symbol,Noto Color Emoji}body{display:flex;flex-direction:column;min-height:100vh}a{transition:color .15s ease;background-color:transparent;text-decoration:none;color:#0051c3}a:hover{text-decoration:underline;color:#ee730a}.hidden{display:none}.main-content{margin:8rem auto;width:100%;max-width:60rem}.heading-favicon{margin-right:.5rem;width:2rem;height:2rem}@media (max-width: 720px){.main-content{margin-top:4rem}.heading-favicon{width:1.5rem;height:1.5rem}}.main-content,.footer{padding-right:1.5rem;padding-left:1.5rem}.main-wrapper{display:flex;flex:1;flex-direction:column;align-items:center}.font-red{color:#b20f03}.spacer{margin:2rem 0}.h1{line-height:3.75rem;font-size:2.5rem;font-weight:500}.h2{line-height:2.25re

Chrome Cache Entry: 254	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 39356, version 1.0
Category:	downloaded
Size (bytes):	39356
Entropy (8bit):	**7.995570740652827**
Encrypted:	**true**
SSDEEP:	768:JyzIl4utbJYZbuVOnri3K9vIWqaoGwCOoq5R6Kqqp8iIS5vaI8:JyxyutVCuOi0lGKoq5F6iISlaJ
MD5:	073BE11022BD7641641D31C320035D3B
SHA1:	36C80242F4A9CCA823C1F209D0B6A258548E6EB9
SHA-256:	FAFE7C2A01CD06D320949FB650302FDA71EA6A04739C39F4252B3EB1093287F0
SHA-512:	CC19B524E5B5FA26CE99465D4CE9C725DD6DBCCB3FB53800588507B187660D904BB899A4102C00B225D21D5958B81DA57CD5E049ADCD70B5AAD08AC2D72EF 3D
Malicious:	false
Reputation:	low
URL:	**http**://https://assets1.prezicdn.net/common/fonts/raleway-medium.woff2
Preview:	wOF2.....Z.....?FFTM..T...L..*.`..V.....L..4...,..6.$..T. ..u..-[G....CU..".m.@.GR~6....\}...j..je..(.O.t. ^.v.....1Y.m.N...r..#H.Vk.j.V.L..k..I.D.5eV.Xp&aQ. .\D].r.k.0@W.I...m.z6...l+...!a.'HB..M-..`$.....=.0...<..2.....27@s?.....M...;$'D...,.....9....)M*0B..&.....I..F.q.q.n.....o..w)..R.*=$!...~_....Jeff..B...l.....L.....d.3..G..3.....z.... .Pw....._.Z%._....E...m....T...`.....ntG.....R....6Z..i..Q.K..,.Gf...][.&r.....d<_.....Uu..!@M.....B.6$...o...m#T4..i..... ....2h....$C.E..e-&.9.....].=..E.`n.....J.HH..Qc.Qc....50.F. ..HK..b...(.[o?.T..l..... @`.....MS.E.4.8g.g....@..H.M{v.R.....sg..`.#..p....j..wO..{Ks..*).....mi..:...o.z.....v.%..T)2.H...ul.d...1...,n.d1g.....@.....sM.?78p..(..i..-.Z=TK.M..X8 1k4.a6..~..7.J)..B..!{..Em.).....7.o.....}...0....>.T.V.L..;.LU.Um[UU..;TUUUEUmU....""""bY"bY.eYDDD.u.s..h..i..(.._Z3...9p[.+.p...[.d"1...2..2....#.7." ...Fu....o..|...X/.&. .N.0.i...?

Chrome Cache Entry: 255	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	OpenType font data
Category:	downloaded
Size (bytes):	64368
Entropy (8bit):	6.65545606895014
Encrypted:	false
SSDEEP:	1536:gYGOiN3xu6mS9xhSf0Uwmd6O+MIvWgYoEpqYuHLMLz8:gYniNgLYdUwmd6O+H+zobjIv8
MD5:	5FAC632B1B61F953C384DBCCCDFDE933
SHA1:	ECC62264953A9EB3AFACE5EB28BD0ED83AF944AD
SHA-256:	A1321362DC043B61962D04485022CE923D0A1C926C4DBF59EE6EA9CE6E520C4D
SHA-512:	3263DE12CA369F5765F00E3E5C929E0A36DB9FB9ED270D24E53C78C2182823E4780AC64D5E96BF1E536DA9416447D672EBDF89EB0BAECE4F543BDC3E988F4A 36
Malicious:	false
Reputation:	low
URL:	**http**://https://prezi.com/api/v1/fonts/Raleway-Regular/
Preview:	OTTO.....@CFF ..h.....k.GPOS...\..\.../.GSUB.....H...NOS/2..ik...0...`cmaps.....X...vhead.y.s.....6hhea.2.....$hmtx.hP.....kern.J.q... ..Avmaxp..P....(....name"L~. .....post...2..... .....B...2_.<.....oM.....oM..(. .[.....(.(.[.....P.....&.....2.....P..[.....pyrs.@..... ....n..... .....=.....).....3.D.....3.D.....w.....".....Y.....h.s.....z.....q.....q .....R.....f.....f.....4.a.....D.....,..... .....4.%Copyright (c) 2010 - 2012, Matt McInerney (matt@pixelspread.com), Pablo Impallari(impallari@gm ail.com), Rodrigo Fuenzalida (hello@rfuenzalida.com) with Reserved Font Name "Raleway"RalewayRegularMattMcInerney,PabloImpallari,RodrigoFuen

Chrome Cache Entry: 256	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	3.875
Encrypted:	false
SSDEEP:	3:HoUinYn:IUyY
MD5:	903747EA4323C522742842A52CE710C9
SHA1:	9F806EA4288867A31A4AD53AC171AA4029DF182B
SHA-256:	4BD8B60F91849C936AE45615145A7B7BE2CF803322A30BABBAE7267A142CA5BB
SHA-512:	EEF73DC29A38ED70FFCFC321931BCB5B5A29FAAC356E8F6D84F57C532EEF44AE75021C341CF7DAE26B8211924A1C0E0EC4735F6BFC4AF3970A48EB63BFB78 95F
Malicious:	false
Reputation:	low
URL:	**http**://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTA0LjAuNTExMi4xMDISEAlcgveVy_w7kRIFDYOoWz0=?alt=proto
Preview:	CgkKBw2DqFs9GgA=

Chrome Cache Entry: 257	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/x/rnp5nz8xys5ucvg1hzu1pthyj
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

Chrome Cache Entry: 258	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1120
Entropy (8bit):	5.55518211480394
Encrypted:	false
SSDEEP:	12:TMHdPhRi/nzV7EIMu5E4BL/KYf3yN8jN/HrKvvHkl8LLrgEKbUj48NRT9suNl7l8:2dzAOx8LfCNQ/+vh6Tj48N3lPllnQ
MD5:	22B734D58BE41F35CACB1D206AA1088D
SHA1:	E09943F68AF1B60C3B868E6FFADB42B653D06293
SHA-256:	58A112A455DAA8A0912990D4E30FEFB594C1F4B79FB386EEB7B64B9D18B0E8C0
SHA-512:	A61E49382DF06AF514C56B0F6C10DA19F2B1958607D067F51A37F7360A426F24C73833AC8442A52B521CD578E02DF76746EE2E6DF18B726962AE60CB1FCFE9F5
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/footers/linkedin-icon.svg
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) --><!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd"><svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="18px" height="18px" viewBox="0 0 18 18" style="enable-background:new 0 0 18 18;" xml:space="preserve"><style type="text/css">...st0{fill:#152235;}.</style><title>linkedin</title><desc>Created with Sketch.</desc><g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-874.000000, -718.000000)">...<g id="linkedin" transform="translate(874.000000, 718.000000)">....<g id="LinkedIn">.....<path id="Shape" class="st0" d="M4,2c0,1.1-0.7,2-2,2C0.8,4,0,3.1,0,2.1C0,1,0.8,0,2,0S4,0.9,4,2L4,2z M0,18h4V5H0V18L0,18z..... M13.6,5.2c-2.1,0-3.3,1.2-3.8,2H9.7L9.5,5.5H5.9C5.9,6.6,6,7.9,6,9.4V18h4v-7.1c0-0.4,0-0.7,0.1-1c0.3-0.7,0

Chrome Cache Entry: 259	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1024
Entropy (8bit):	5.555714280948775
Encrypted:	false
SSDEEP:	24:2dzAOx8LfCNQ/6h6pxrS8BqT+TvP14Tl5H:czAOKfEq6YGB+TvP14r
MD5:	73605F769148DB36D71439F235DD2B8E
SHA1:	34535388896117DAB0A48B1FD19118F8DAB21142
SHA-256:	70ED38179144E26BC93DCB6FA40F1396CCDD02F6BC04AD4700210582574A75DC
SHA-512:	F882FB739F80192CE90F03A658E2F403FDBFB926D27A9F8EFFC16FA0CF8B088F55CAC78993F569738B18E3E586906E587075DB00A0F082F2339DF3BA43B6C7C6
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/footers/facebook-icon.svg

Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 19.2.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<!DOCTYPE svg PUBLIC "-//W3C //DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. width="18px" height="18px" viewBox="0 0 18 18" style="enable-background:new 0 0 18 18;" xml:space="preserve">.<style type="text/css">...st0{fill:#152235;}.</style>.<title>facebook</title>.<desc>Created with Sketch.</desc>.<g id="Page-2">..<g id="Payment-page-Copy-16" transform="translate(-778.000000, -718.000000)">...<g id="facebook" transform="translate(778.000000, 718.000000)">....<g id="Facebook">.....<path id="Shape" class="st0" d="M16,0H2C0.9,0,0,0.9,0,2v14c0,1.1,0.9,2,2,2h7v-7H7V8.5h2v-2c0-2.2,1.2-3.7,3.8-3.7l1.8,0v2.6.....h-1.2c-1,0-1.4,0.7-1.4,1.4v1.7h2.6L14,11h-2v7h4c1.1,0,2-0.9,2-2V2C18,0.9,17.1,0,16,0L16,0z"/>....</g>..

Chrome Cache Entry: 260	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (60008)
Category:	downloaded
Size (bytes):	65286
Entropy (8bit):	5.539497149656779
Encrypted:	false
SSDEEP:	768:soxMMeIUiGUWO4btNlqlbRaw/X4oIA8pYM9MXKr0OzkAmMapKS+IGmqp:RSlIUiGUL4bt7qlbRgzA8pYQMaGMLIGz
MD5:	ED5D6CAF417FAB681343BC3414BABC55
SHA1:	410BA8D8866D7C7DF41F21526345CFB7426386F2
SHA-256:	7E86F52CB0D423805EC541A4BCCAE5156A01FBE36355E6D798A4505932126 51F
SHA-512:	16658100C4AD2587EA9F9964FC628094C798F52F242A5364874DF4EF2D4DAFB05BAF96CCA9F8B127F2290DB3175E5C89035E81D32A3CFB5B129532AC3F1A6964
Malicious:	false
Reputation:	low
URL:	http://https://connect.facebook.net/signals/plugins/identity.js?v=2.9.99
Preview:	/**.* Copyright (c) 2017-present, Facebook, Inc. All rights reserved..*.* You are hereby granted a non-exclusive, worldwide, royalty-free license to use,.* copy, modify, and distribute this software in source code or binary form for use.* in connection with the web services and APIs provided by Facebook..*.* As with any software that integrates with the Facebook platform, your use of.* this software is subject to the Facebook Platform Policy.* [http://developers.facebook.com/policy/]. This copyright notice shall be .* included in all copies or substantial portions of the software..*.* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR.* IM PLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS.* FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR.* COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER.* IN AN ACTION OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN.* CONNECTION WI

Chrome Cache Entry: 261	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 186 x 106, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33231
Entropy (8bit):	7.986474350329641
Encrypted:	false
SSDEEP:	768:j+VTrD2c/rvtINAVofu9Paa+gR5n6JwXJK+2us+m:aVTWc/r2ffuj+gDnkww+2v3
MD5:	68411045E8288B5FF677386D8444E551
SHA1:	0A8E0599304D3B93ACBB9AD85AC63084EB2BB95D
SHA-256:	A23F7D2BFF3DABEFE64F16BD4A77BF0524EB87D14FE944A300142F234AD244E4
SHA-512:	4D6A0D49C2A6A8513D5869433BBDE49C96A57604D7903C803DD23EABB618389E1EFF2DF277FF0B03F90A3162FA3472559BFDAAFD6DB60115B22564B5F3C1273A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....j.....0K.....pHYs...%...%.IR$... .IDATx...w.Y.....yg.{L..C.....$@H.!...@^.....'bgf.u7.g..jTTe..;v.'"..h.....L...|dd$....k..<.....M.e..4....+...F.s6x..F=..g\|W\|. .Y....^...iT^...z}.....:.....o&&&.....g...../^.C...p...H>.....W..._.o.....3.y.^..Y.~...5==._.t).kW~...V[.....z9vi...J....1.+.....a..q.:^.s.....m.._.3.{<s...<?.jA.{zz..C/....\|\|,. x6..};.x.B~.....3okk.....S.N.g.....]]...b.CP.H.1...U...I..P.....{._.rY....3...\|`` .....[...yg....)....\|..d~n.B....;y.....k..G.....{'.....6F.....>hQLNN.3&...s~.FLl.....K./.Z% ..&...x.BH..~.Q..(.....ZB....hdM..h....g....x....?z....Y....6N.l.n.X^./^.h.t%.m.r.....\|..X^....r.W..z~_<.....I.....#..HX....;w..W.Z.....+...../.....'O.W.....z.*.....i..... ...&w....l>7;.....B(..>.....W.g.H....0.\... ...<w...s.1]h.,.\9Y.....$=~.8....&.....7oJ....._.W..w...q_.....M.

Chrome Cache Entry: 262	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 13 x 76, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	61
Entropy (8bit):	4.022997040570905
Encrypted:	false
SSDEEP:	3:yionv//thPlozttZt/hAkxl/k4E08up:6v/lhPyt/Kk7Tp
MD5:	D6A0FA403A4B06A2E824553DDF751F0F
SHA1:	A46F5AFB54CC321A41C7A5FB0959E2C51FC5C137
SHA-256:	73E03D4C2911F7666D780BEFD1D27F0E3FA6097D17489872C8D6EFDEC1CD5DA8

SHA-512:	1855FFA1B592E056C4ECD1D11E1911ABC993DB99AE595976A5B9428CE71E1BF7A0D3074158A79776E50749E31B429F9CEDB32AB9F8DD9BC27635B15DEF0820 8
Malicious:	false
Reputation:	low
URL:	http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/img/7ab14eb85d4f0476/1679350460996/n3rcr4Aukl5lmkK
Preview:	.PNG.....IHDR.....L.....9.....IDAT.....$.....IEND.B`.

Chrome Cache Entry: 263	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	42
Entropy (8bit):	2.9881439641616536
Encrypted:	false
SSDEEP:	3:CUXPQE/xlEy:1QEoy
MD5:	D89746888DA2D9510B64A9F031EAECD5
SHA1:	D5FCEB6532643D0D84FFE09C40C481ECDF59E15A
SHA-256:	EF1955AE757C8B966C83248350331BD3A30F658CED11F387F8EBF05AB3368629
SHA-512:	D5DA26B5D496EDB0221DF1A4057A8B0285D15592A8F8DC7016A294DF37ED335F3FDE6A2252962E0DF38B62847F8B771463A0124EF3F84299F262ED9D9D3CEE4 C
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D.;

Chrome Cache Entry: 264	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (5219), with no line terminators
Category:	downloaded
Size (bytes):	5219
Entropy (8bit):	4.7351281625811215
Encrypted:	false
SSDEEP:	48:ig6czE27T7u1JxDOPejEtx0hX/h3RrAntKJZP7IP713XV7lV71ysLtMP55rQ:i5czE2f4JxDOPCtB/BRMtoNzbtLu+
MD5:	EEF7A4C5184F09FA78700CCCE9F69F9A
SHA1:	ED64059D104BF4575FA86C9723A5FAD8C0F513C5
SHA-256:	97F813FF56B4E66611F509B50D765DFF5B9ED3EEA1B6D4776B268868E8131021
SHA-512:	62D6AAABF09C4DB7F8F062A02D6E85252A07817B059BEF25E17116D14059AF28576C18D3ADA75BFB576A9C03AA1B849C1D2E63F32FBB50B5D06A80C446DC9D EE
Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/CACHE/css/97f813ff56b4.css
Preview:	.footer-container.footer-marketing-min .container,.inc-info{text-align:center}.footer-container,.footer-container-mobile{background-color:#F3F5F9}.footer-container-mobile .footer-padding,.footer-container.footer-padding{padding:60px 0 30px}.footer-container-mobile.footer-padding-mobile,.footer-container.footer-padding-mobile{padd ing:30px 0}.footer-container ul,.footer-container-mobile ul{list-style:none;margin-bottom:36px}.footer-container-no-margin-bottom-ul ul{margin-bottom:0}.footer-container-no-margin-bottom-ul ul.btm-18{margin-bottom:18px}@media (min-width:768px){.footer-container-no-margin-bottom-ul ul.infogram-btm{margin-bottom:36px}}@media (min-width:992px){.footer-container-no-margin-bottom-ul ul.infogram-btm{margin-bottom:0}}.text-gray-3{color:#8E939C}.no-underline:focus,.no-underline:hover{text-deco ration:none}.icons{margin-right:6px;opacity:.7;transition:all .2s ease}.icons:hover{opacity:1}.footer-list-container{padding-right:24px}.footer-list-container li{line-hei ght:0;marg

Chrome Cache Entry: 265	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65441)
Category:	downloaded
Size (bytes):	3351882
Entropy (8bit):	5.4739540174171655
Encrypted:	false
SSDEEP:	49152:bsXbGIdIEetNQCQ4m5+KQfa5FlVrBI+bPVRYy3KUTGGBLG90:bsX7smeaHGB0
MD5:	795999113324CFE31E351895D7FE49FE
SHA1:	85EB2403CB50278500B8D0F7AD5AF7B708C67323
SHA-256:	D64FEFA6E899825AF9572CB76C598F33B5CBD2FB5204C37B9FD1AE4FEBC5AE81
SHA-512:	CE737E1D1253295C589EF019B8D565E01FB5E229B09FDAE02FAE689E65CA3A8112D680E9D541C39EDB8B9121B72A1720F8CF2C70E01A23725C654705274E239
Malicious:	false

Reputation:	low
URL:	http://https://cdn.jifo.co/js/dist/viewer-f49489f3c1e5f6317f0b-prezigram.js
Preview:	/*! For license information please see viewer-f49489f3c1e5f6317f0b-prezigram.js.LICENSE.txt */.var PreziGram=function(e){function t(t){for(var n,o,i=t[0],a=t[1],c=0,s=[];c<i.length;c++)o=i[c],Object.prototype.hasOwnProperty.call(r,o)&&r[o]&&s.push(r[o][0]),r[o]=0;for(n in a)Object.prototype.hasOwnProperty.call(a,n)&&(e[n]=a[n]);for(u&&u(t);s.length;)s.shift()()}var n={},r={viewer:0};function o(t){if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return e[t].call(r.exports,r,r.exports,o),r.l=!0,r.exports}o.e=function(e){var t=[],n=r[e];if(0!==n)if(n)t.push(n[2]);else{var i=new Promise((function(t,o){n=r[e]=[t,o]}));t.push(n[2]=i);var a,c=document.createElement("script");c.charset="utf-8",c.timeout=120,o.nc&&c.setAttribute("nonce",o.nc),c.src=function(e){return o.p+""+({"vendors~infogram-charts/alluvial~infogram-charts/charts-area~infogram-charts/charts-area_stacked~inf~07784584":"vendors~infogram-charts/alluvial~infogram-charts/charts-area~infogram-charts/charts-area_stacked~

Chrome Cache Entry: 266	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (6863), with no line terminators
Category:	downloaded
Size (bytes):	6863
Entropy (8bit):	5.490013026714877
Encrypted:	false
SSDEEP:	96:+w2lmNhJntW3vsKNZVqNtcgycdhimkCSUz537rke6AR3eaVyeK09kZHB4iDM7ZBu:PBtK0Q8cgycN5jFPFlz9yH0Lu
MD5:	CF0A59EC7B720FAC103980D562066586
SHA1:	9664C8FDD7B8D30D3FC8D582C050EAADCC47E5AC
SHA-256:	C58EFF1681E56AD329066E586E32915C6A3C805CA159B14818744669B7348F69
SHA-512:	759161C454435AB100A4604F9396DE79BE2033489B784624E7E1239FCA20EAB4CFDCFAB3CA0CA223AF2E05B9AB01E643A0AD833ABC147FB31242241EB110522A
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/scripts/pica.js
Preview:	~function(l,d,e,f,g,h,i){l=b,function(c,j,H,k,l){for(H=b,k=c();!![];)try{if(l=-parseInt(H(412))/1*(-parseInt(H(419))/2)+parseInt(H(427))/3+parseInt(H(451))/4*(-parseInt(H(407))/5)+parseInt(H(464))/6*(-parseInt(H(420))/7)+parseInt(H(442))/8+-parseInt(H(405))/9+-parseInt(H(462))/10*(-parseInt(H(421))/11),j===l)break;else k.push(k.shift())}catch(m){k.push(k.shift())}}(a,690301),d=this||self,e=d[l(423)],(l(424)!==typeof d?d:self)[l(435)]=function(c,L,z){return L=l,z=L(431)[L(453)](''),'d'!=n(o(L(425)))[1]&&(j=function(A,B,C){return C=(A&65535)+(65535&B),(A>>16.55)+(B>>16)+(C>>16.07)<<16.84|C&65535},n(o(c));function w(A,B,C,D,E,F,G){return x(B&C|D&~B,A,B,E,F,G)}function y(A,B,C,D,E,F){C=A[0],D=A[1],E=A[2],F=A[3],C=w(C,D,E,F,B[0],7,-680876936),F=w(F,C,D,E,B[1],12,-389564586),E=w(E,F,C,D,B[2],17,606105819),D=w(D,E,F,C,B[3],22,-1044525330),C=w(C,D,E,F,B[4],7,-176418897),F=w(F,C,D,E,B[5],12,1200080426),E=w(E,F,C,D,B[6],17,-1473231341),D=w(D,E,F,C,B[7],22,-45705983),C=w(C,D,E,F,B[8],7,177003541

Chrome Cache Entry: 267	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	36
Entropy (8bit):	4.215354779870081
Encrypted:	false
SSDEEP:	3:YEHuHQYYvcW:YEonYEW
MD5:	2DDF287D0D7556C838B335AE5C88A09D
SHA1:	D52113B5FA2E61F152F5E1CAD6EBD7353C9BDFA0
SHA-256:	7B1EAAAF180A13C29B6DDDC3B0AE23333B4397E0F3C065B4C86DA2F2530A5F89
SHA-512:	24502D05D68B4C6A2FCF9366E19E3D0372DE0027829860C3F7E8D8178F11C1768D3B6C4679CC354EB68227873B334859CA6C3D2807F13F8529262A141E0FAED3
Malicious:	false
Reputation:	low
URL:	http://https://cdn.linkedin.oribi.io/partner/70210/domain/prezi.com/token
Preview:	{"allowed":false,"scriptToken":null}

Chrome Cache Entry: 268	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	367
Entropy (8bit):	4.91512135645049
Encrypted:	false
SSDEEP:	6:tnrwdhC/gKumc4slvtM65tfTLCMhrygjFboBsJO6yUFORulUTL0TxPKVM:trwdU/gKuXM65JT+Mh1FboBViQUT1Kq
MD5:	5E58B5B139E41CC0645ADA25F7D29F09
SHA1:	9161EAC1663B931DC69EAD690AF33CE968AD4E0C
SHA-256:	CA98E42319955E993F6CE9AF1B31C69054E260147F9B3AD6DBBB4DD4D36E5DDA
SHA-512:	162AD1019859187E3CD71A23132F843734B1E06BCADAFEF73F15C965D1CB26E1798A56CC0A5F12A1BF8CDEF7452A21B6808FAB71A1980053E8AF3AD1AE7BD7E0

Malicious:	false
Reputation:	low
URL:	http://https://assets.prezicdn.net/assets-versioned/prezipage-versioned/4367-508a952/common/img/icons/Close.svg
Preview:	<svg width="24" height="24" viewBox="0 0 24 24" fill="none" xmlns="http://www.w3.org/2000/svg">.<path fill-rule="evenodd" clip-rule="evenodd" d="M12.0002 10.585 8L7.75748 6.34314L6.34326 7.75735L10.5859 12L6.3433 16.2427L7.75752 17.6569L12.0002 13.4142L16.2428 17.6568L17.657 16.2426L13.4144 12L17.657 7.75739L16.2428 6.34317L12.0002 10.5858Z" fill="#000000"/>.</svg>.

Chrome Cache Entry: 269

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (14029)
Category:	downloaded
Size (bytes):	14030
Entropy (8bit):	5.232453222408614
Encrypted:	false
SSDEEP:	384:RXDHOs/tnqxFHR7URdGaayYoJpN6VfayrX2jxu5wtEvRvIhUJdxtJ:lHOuCEfdJJpAVfayrX2jxu5TvRvIhUJT
MD5:	AB6F5DAD37138714B2B042E5135DA1FA
SHA1:	51C1790132750CCE2EFC080EC9F9BA0ECD8D4B40
SHA-256:	D395CC53363E6E22C75F73DE0D4DE7355ED844B65B8F0D149664EC06FACD2D8E
SHA-512:	B5C63BCA704D802E1B05A914FA23507A2E17020FAB39BB5E9C061A9D6DCB611C7C587A6BC1E9FC67DDF9E54A76A93F4E666CA499747D40787B7F8C1EDA117C B2
Malicious:	false
Reputation:	low
URL:	http://https://challenges.cloudflare.com/turnstile/v0/g/db880165/api.js?onload=_cf_chl_turnstile_l&render=explicit
Preview:	(()=>{function E(e,l){return e.indexOf(l)!==-1}function k(e){return E(["auto","dark","light"],e)}function O(e){return E(["auto","never"],e)}function W(e){return e>0&&e<9e5}var Ee=/^[0-9A-Za-z_-]{3,100}$/;function ae(e){return Ee.test(e)}var ye=/^[a-z0-9_-]{0,32}$/i;function oe(e){return ye.test(e)}var he=/^[a-z0-9_\-=]{0,255}$/i;function se(e){retu rn he.test(e)}function P(e){return E(["normal","compact","invisible"],e)}function D(e){return E(["auto","manual","never"],e)}var le=/^[a-z]{2}(-[A-Z]{2})?$/;function U(e){return e==="auto"||le.test(e)}function H(e){return E(["always","execute","interaction-only"],e)}function z(e){return E(["render","execute"],e)}var ve=".cf-turnstile",xe=".cf-chall enge",we=".g-recaptcha",Te="cf_challenge_response",Ae="cf-turnstile-response",be="g-recaptcha-response",Re=8e3,_=!1,ue=!1;function s(e){let l=`[Cloudflare Turnstile] ${e}.`;throw console.error(l),new Error(l)}function p(e){console.warn(`[Cloudflare Turnstile] ${e}.`)}function $e(e){s(`Failed with co

Chrome Cache Entry: 270

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	154957
Entropy (8bit):	5.666979602298695
Encrypted:	false
SSDEEP:	1536:vWZqA1D9dAxOZi+jClRGJJActrW3jJAYWAkZq2k0F6shZewhav5m7qrPPrIouB7N:vWZqSLJJhEAYzkZRfTewUvwUuB72OFoK
MD5:	8F2AB3D70777AA99AFA56F60E81D58C1
SHA1:	2BD664BC106D2643E7DA61CF53AEB13CAFD4B3A5
SHA-256:	1623FF0138FD438805AE3BA18D3BBAB986919C91EB2938188284A1605911C619
SHA-512:	757FF2DCE37BD5FF7D020BA9D62F277FE0B0C28F2F4871CAAA88CD98E29A94C167B0FE387AB141F86117D2726CD9A05BCD346AF2A091007BF8CEFA89396E0A 91
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7ab14ea51c463602
Preview:	window._cf_chl_opt.uaSR=true;window._cf_chl_opt.uaO=false;~function(hi,f7,f8,f9,fa,fj,fk,fl,fm,fn,fo,fp,fq,fr,fs,ft,fu,fv,fw,fx,fy,fz,fA,fB,fC,fD,fE,fF,fG,fH,fI,fJ,fK,fN,gu,gv,gw,g x,gy,gz,gA,gB,gE,gF,ha,hd,he,hf,hg,gC,gD){for(hi=c,function(d,e,hh,f,g){for(hh=c,f=d();!![];)try{if(g=-parseInt(hh(1063))/1*(-parseInt(hh(1123))/2)+parseInt(hh(692))/3*(p arseInt(hh(1830))/4)+parseInt(hh(1575))/5*(-parseInt(hh(1060))/6)+-parseInt(hh(580))/7+parseInt(hh(1339))/8+parseInt(hh(1207))/9*(-parseInt(hh(1109))/10)+-parse Int(hh(1248))/11,g===e)break;else f.push(f.shift())}catch(h){f.push(f.shift())}}(b,107224),f7=this||self,f8=f7[hi(1132)],f9=[],fa=[],f7[hi(1872)]=function(d,e,f,g,h,hp,i,j,k,l){(hp =hi,i={'vSswT':function(m){return m()},'dyyno':function(m,n){return m+n},'OZXus':hp(1088),'HgdJB':hp(1050),'rVwgo':hp(1222),'nKAJm':hp(1391)},j=d[hp(852)](),k=h p(704),j[hp(1015)](k)>-1)?f7[hp(1316)](function(hq){hq=hp,i[hq(425)](fe)},1e3):(l=[i[hp(645)](hp(880),d),hp(482)+e,i[hp(929)]+f,hp(1623)+g,i[hp(511)]+

Chrome Cache Entry: 271

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 6 icons, -128x-128, 16 colors, 72x72, 16 colors
Category:	dropped
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyio7eeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5

SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD(1
Malicious:	false
Reputation:	low
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(.....P.....""" ...3 3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...3333333333333333333333333333333""""" """ ...3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...33333333333 3333333333333333333""" ...3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...33333333333 """ ...3333333333333333333333333333333""" ...3333333333333333333333333333333""" ...33333333333 3333333333333333333""" ...3333333333333333333333333333333""

Chrome Cache Entry: 272

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (63552)
Category:	downloaded
Size (bytes):	453446
Entropy (8bit):	5.414090395854072
Encrypted:	false
SSDEEP:	3072:k7pe6Q89GqWY1inz8fVvyqU7CeYOzBH05EFboQLMnmuCxXWCcUPcufdBKjb3t6tp:k7eYeiXsd0GFboQkbUfdBQC
MD5:	52ADEA9202C18D810B6730ACF1A43F8C
SHA1:	4DF6ED40482D996CB7DB95342956FE33FE06620D
SHA-256:	717A053CA441490867A4D1D8FB4728DB9A8D78A054F2962444E8E3BC5636FBA3
SHA-512:	C885EB6D345D5E1B360B04D958F0CAF61C255E029EE6E7951ECB0916CA824086FD2D4215C0CE544B2AF0736719A90B74C9EFCA5A34F57F02262E0A9FEE3FB7 C4
Malicious:	false
Reputation:	low
URL:	http://https://package-bundles.prezi.com/design-view-page/design-view-page.0.1.669/design-view-page.js
Preview:	var DesignViewPageModule=function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports} return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTa g&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"stri ng"!=typeof e)for(var o in e)n.d(r,o,function(t){return e[t]}.bind(null,o));return r},n.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function(){return e};return n.d(t,"a",t),t},n.o=function(e,t){return Object.prototype.hasOwnProperty.call(e,t)},n.p="",n(n.s=271)}([function(e,t){e.exports=React},function(e,t,n){"use str

Chrome Cache Entry: 273

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	155255
Entropy (8bit):	5.682949587787375
Encrypted:	false
SSDEEP:	3072:VOJHZkCljskSpKeAP2wR0OPvx4FMwusmDs:VOJ5FljsUPAO3eFMRU
MD5:	C9BEAC714542C3C0460BDFED661A2D9A
SHA1:	1700B1DC8A6ED46AC9895CA4CD68E7FDE138E55A
SHA-256:	75E7207BBB1CEB84EA4A4EB79976E0F67EDB3239D7B5EF226A8FA152ACA5EB8C
SHA-512:	95AE0A5994980F5E85217A3AB803B5ED03D0EF212D1BFE1ABD64FBE3AA45C29858C5C11EE0063D29A9ED0D2F807EEEF1713B7EF6B1BCEB0E0AE14F0603C8D D5D
Malicious:	false
Reputation:	low
URL:	http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/orchestrate/chl_api/v1?ray=7ab14eb85d4f0476
Preview:	window._cf_chl_opt.uaO=false;~function(hk,f8,f9,fa,fb,fd,fg,fh,fi,fj,fk,fn,fo,fY,fZ,g0,g1,g2,g3,g4,g5,g6,g7,g8,g9,ga,gb,gc,gd,ge,gf,gg,gh,gi,gj,gk,gl,gm,gn,go,gp,gs,h9,ha ,hb,hc,hd,he,hf,hg,hh,hi,fl,fm){if(hk=c,function(d,e,hj,f,g){for(hj=c,f=d();!![];)try{if(g=parseInt(hj(367))/1*(parseInt(hj(1406))/2)+-parseInt(hj(982))/3*(parseInt(hj(1188))/4)+pa rseInt(hj(210))/5+-parseInt(hj(944))/6+-parseInt(hj(881))/7*(parseInt(hj(200))/8)+-parseInt(hj(375))/9*(parseInt(hj(838))/10)+-parseInt(hj(1039))/11*(-parseInt(hj(523))/1 2),g===e)break;else f.push(f.shift())}catch(h){f.push(f.shift())}}(b,234549),f8=this||self,f9=f8[hk(295)],fa=[],fb=[],fb[hk(745)](function(){return gE()}),f8[hk(437)]=function(hm,g ,h,j,k,l,m){for(hm=hk,g={},g.Lwvpq=function(n,o){return n<o},h=g,j=f8[hm(1162)],k={},k.kd=0,k.pm=0,k.po=0,k.ts=0,k.mm=0,k.cl=0,k.t=0,l={},l[hm(694)]=j[hm(1019)] ,l[hm(1622)]=j[hm(1622)],l[hm(1346)]=j[hm(1346)],l[hm(1440)]=0,l[hm(304)]=0,l.oV=1,l[hm(900)]=j[hm(900)],l.ie=k,f8[hm(1329)]=l,m=0;h[hm(1574

Chrome Cache Entry: 274

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with very long lines (8524)
Category:	downloaded
Size (bytes):	21679
Entropy (8bit):	5.283467487147688

Encrypted:	false
SSDEEP:	384:121nbgnGtkOruFU8kLk2SwnfmtzHuXmalWxRY5ptyv:QsGtee8sSwnfmlsmalWL
MD5:	FA6D15A7F11EBFA4A5BD7F6208D3A04D
SHA1:	C2822124ABD0C0829182067E76F7A5A3B1DA3C32
SHA-256:	9B915A373B52BCE9B53E2D411495FCC7B3737F918C32DB49120F28D1DCA8FEDE
SHA-512:	0F013488EFA8A564AF91A7CE5307C8E94EA216780C2C2267AE760E8CF7D2DF85155D316A8F37951A450CE722317DF94104C3EFE58E5F099E406453FAAC45C6F8
Malicious:	false
Reputation:	low
URL:	http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/turnstile/if/ov2/av0/yqku6/0x4AAAAAAAAjq6WYeRDKmebM/light/normal
Preview:	<!DOCTYPE HTML>.<html lang="en-US">.<head>. <meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />. <meta name="robots" content="noindex, nofollow" />. <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1" />. <title>Checking your Browser... </title>. <style>html, body{margin:0;padding:0;width:100%;height:100%;overflow:hidden}body{background-color:#fff;line-height:17px;color:#1d1f20;font-family:-apple-system,system-ui,BlinkMacSystemFont,Segoe UI,Roboto,Oxygen,Ubuntu,Helvetica Neue,Arial,sans-serif;font-size:14px;font-weight:400;-webkit-font-smoothing:antialiased;font-style:normal}h1{margin:16px 0;text-align:center;line-height:1.25;color:#1d1f20;font-size:16px;font-weight:700}p{margin:8px 0;text-align:center;font-size:20px;font-weight:400}#content{border:1px solid #e0e0e0;background-color:#fafafa;height:60px;user-select:none}table,td,tr{margin:0;padding:0}#branding{padding-right:13px;width:60px;text-align:center}#cf-stage{padding-le

Chrome Cache Entry: 275

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (32065)
Category:	downloaded
Size (bytes):	85578
Entropy (8bit):	5.366055229017455
Encrypted:	false
SSDEEP:	1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2
MD5:	2F6B11A7E914718E0290410E85366FE9
SHA1:	69BB69E25CA7D5EF0935317584E6153F3FD9A88C
SHA-256:	05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E
SHA-512:	0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/jq/t1juppxc5gznyzvh5y8hur1ns
Preview:	/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call

Chrome Cache Entry: 276

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	105369
Entropy (8bit):	5.240719144154261
Encrypted:	false
SSDEEP:	1536:l+gu2w+EEnazA/PWrF7qvEAFiQcpmQoDZztVEHn8:E6CEVEH8
MD5:	8E6B0F88563F9C33F78BCE65CF287DF7
SHA1:	EF7765CD2A7D64ED27DD7344702597AFF6F8C397
SHA-256:	A7057BEBFFF43E7281CA31DA00D40BD88C8D02D1576B9C45891DD56A3853269A
SHA-512:	7DCE31D45ACA40340490B9F437A22ADF212B049DE0D4DDEB908A50C1F5C6C7B5561323B3A93B6ED3E5A7C44D7170460BFF8D8722749191C0F5A8DBD83E093EF
Malicious:	false
Reputation:	low
URL:	http://https://msdiufvm2163e59c4b67124.opticair.ru/APP-3T2EUU/nxhyus5zzgru1nt8cyvjhpp51
Preview:	html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background-color:transparent}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:bold}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-0.5em}sub{bottom:-0.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}

Chrome Cache Entry: 277

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (17346), with no line terminators
Category:	downloaded
Size (bytes):	17346
Entropy (8bit):	5.756065693439801
Encrypted:	false
SSDEEP:	384:cCgBEbDATWo7pCz8qpI7/+fsQRBMUgyvDDqgMLGUGOCLURIC1W6Gb:cCgBz6o1CzXa7+fsQH/3nAub
MD5:	DF82DA09581E0F287E5655FE47CEB559
SHA1:	4A86A0AA83B6AD6DA68C00DF71A8A98B73F25910
SHA-256:	5DAFE8B74BFD8567CEB1372730A1FBF9B6C585BFB52A64032F6A37A1DF7A522C
SHA-512:	7807AFA59F4ADF8A4C64E13B4D6FA7FC8EB5000E2DC4913FDDF617BCE0A0293F340E6C1C79A136A68FB8DDDC2EA4622D56B98DF650A287436F7FB5E6AAB09787
Malicious:	false
Reputation:	low
URL:	http://https://cdn.taboola.com/scripts/eid.es5.js
Preview:	function _createForOfIteratorHelper(b,t){var e="undefined"!=typeof Symbol&&b[Symbol.iterator]||b["@@iterator"];if(!e){if(Array.isArray(b)||(e=_unsupportedIterableToArray(b))||t&&b&&"number"==typeof b.length){e&&(b=e);var c=0,m=function b(){};return{s:m,n:function t(){return c>=b.length?{done:!0}:{done:!1,value:b[c++]}},e:function b(t){throw t},f:m}}throw new TypeError("Invalid attempt to iterate non-iterable instance.\nIn order to be iterable, non-array objects must have a [Symbol.iterator]() method.")}var W=!0,d=!1,n;return{s:function t(){e=e.call(b)},n:function b(){var t=e.next();return W=t.done,t},e:function b(t){d=!0,n=t},f:function b(){try{W||null==e.return||e.return()}finally{if(d)throw n}}}function _unsupportedIterableToArray(b,t){if(b){if("string"==typeof b)return _arrayLikeToArray(b,t);var e=Object.prototype.toString.call(b).slice(8,-1);return"Object"===e&&b.constructor&&(e=b.constructor.name),"Map"===e||"Set"===e?Array.from(b):"Arguments"===e||/^(?:Ui|I)nt(?:8|16|32)(?:Clamp

Chrome Cache Entry: 278

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 3 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	15086
Entropy (8bit):	3.9672871989666185
Encrypted:	false
SSDEEP:	96:3WqX555551hvQoKtKQQE7cvE/hfpMc07iBSD3vmduZbdZyW+6FLWqdoAl1To0Pyv:RoSEovT7iBSz6UhZygFLpoZ0qNwqjz7J
MD5:	0520A574E13AF7D1B6F2C608364577FF
SHA1:	360038AEF0A5E9FF4479A5EB47289BCFF56F4FE4
SHA-256:	2E2801B1412647B7E09AE1DA78685C4E4B4AD98945BE191650D84151A23D546F
SHA-512:	A1474DD394EC18FE9DAA420A3FA79036154EB72354ACCE2B9109510F141866CAF7067D5856514D1CC20D47D39EA339C638640C0FEC86D62CA32FFA10516A98AE
Malicious:	false
Reputation:	low
Preview:	..... .h...6... ....00.... ..%..F...(..... ....1X..2...2...1...2...2...1X.....6!..2...2...1X..1...U...1...1X..2...2...6!.....6!..2...2...,...2...2...1...2...2...,...2...2...6!.....2...2...4@..2...2...2...@...2...2...2...4@..2...2.....1X..2...,...2...2.....1.....1.....2...,...2...1X.....2...1X..2...2...1.....1.....1.....1...2...2...1X..2.....2...1...2...23..1.....1.....1.....1...23..2...1...2.....1...U...1...@...1.....1.....1.....1...;...1...U...1.....2...1...2...23..1.....1.....1.....1...23..2...1...2.....2...1X..2...2...2.....1.....1.....2...2...2...1X..2.....1X..2...,...2...4@.....1.....1.....4@..2...,...2...1X.....2...2...4@..2...2...2...@...2...2...2...4@..2...2.....6!..2...2...,...2...2...1...2...2...,...2...2...6!.....

Chrome Cache Entry: 279

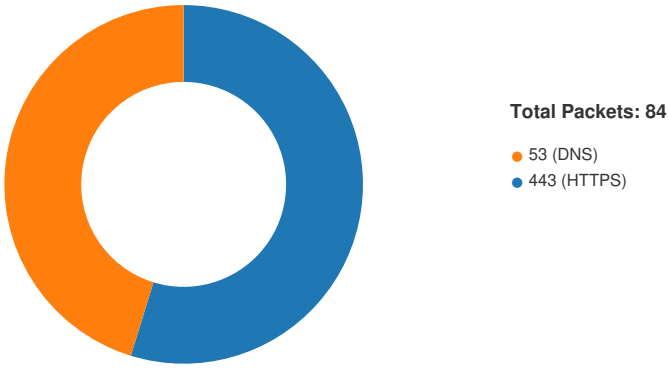
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (42123)
Category:	downloaded
Size (bytes):	331700
Entropy (8bit):	5.6366643058857715
Encrypted:	false
SSDEEP:	6144:8Fl2oXeGaP8Ez5WMEbTHza3gqDyLGUjJOO:8Fl2oOjP8QtOp
MD5:	117E2F069804BBD614BB959FCEB82424
SHA1:	30942138FE8533A1C8CE42EA6227900A5CCEDB87
SHA-256:	AE9B5E9DE5ECC32F0247A7A31D8A07B9ACC6C2531425D2D61FD62B20C10AE96F
SHA-512:	1CAF073129E59B3F9866D62111D199E500A1A041FE975372D4B8CCC2BCC623814E3022F63465092D066E01E2E809615FDFCC757C5159AC6C70561EBC0DE4844
Malicious:	false
Reputation:	low
URL:	http://https://www.googletagmanager.com/gtm.js?id=GTM-MQ6FG2
Preview:	.// Copyright 2012 Google Inc. All rights reserved..(function(w,g){w[g]=w[g]||{};w[g].e=function(s){return eval(s);};})(window,'google_tag_manager');(function(){..var data = {."resource": {. "version":"972",. . "macros":[{"function":"__e"},{"function":"__v","vtp_name":"gtm.triggers","vtp_dataLayerVersion":2,"vtp_setDefaultValue":true,"vtp_defaultValue":""},{"function":"__u","vtp_component":"PATH","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__j","vtp_name":"document.title"},{"function":"__u","vtp_component":"URL","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__v","vtp_dataLayerVersion":2,"vtp_setDefaultValue":false,"vtp_name":"quantity"},{"function":"__jsm","vtp_javascript":["template","(function(){return 600*",["escape",["macro",5],8,16],"})();"]},{"function":"__u","vtp_enableMultiQueryKeys":false,"vtp_enableIgnoreEmptyQueryParam":false},{"function":"__v","vtp_dataLayerVersion":2,"vtp_setDefaultValue

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:13:58.729944944 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:58.729993105 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:58.730062962 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:58.730779886 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:58.730822086 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:58.730915070 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:58.732161045 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.732202053 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.732265949 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.735141039 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:58.735171080 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:58.735723972 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:58.735761881 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:58.735984087 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.736006021 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.801664114 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.803169012 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.803232908 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.804308891 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.804440022 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.806793928 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:58.806922913 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:58.822144985 CET	443	49729	142.250.185.237	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:13:58.850337982 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:58.850370884 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:58.853108883 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:58.853210926 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.091809034 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.209604979 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.215552092 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.215607882 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.219753027 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.219830990 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.219849110 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.298105001 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.298146009 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.298501968 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.299554110 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.299585104 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.300148010 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.300200939 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.300371885 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.300748110 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:59.300812960 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.300928116 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.301140070 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.301171064 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.301953077 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:59.301986933 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.332107067 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.332190990 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:59.332233906 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.332257986 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.332334995 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:59.333502054 CET	49731	443	192.168.2.5	142.250.186.142
Mar 20, 2023 23:13:59.333537102 CET	443	49731	142.250.186.142	192.168.2.5
Mar 20, 2023 23:13:59.341619968 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.350389004 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.350702047 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.350775003 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.379779100 CET	49729	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:13:59.379829884 CET	443	49729	142.250.185.237	192.168.2.5
Mar 20, 2023 23:13:59.409641027 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.479840994 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.479938984 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.480017900 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.484247923 CET	49730	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.484286070 CET	443	49730	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.487518072 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.487572908 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.487682104 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.488094091 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.488115072 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.693206072 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.693703890 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.693723917 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.694197893 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.695822954 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.695846081 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.695945024 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:13:59.696405888 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:13:59.696423054 CET	443	49732	75.2.83.248	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:14:00.169691086 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.170285940 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.170327902 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.170568943 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.170568943 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.170604944 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.170681000 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.189022064 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.189104080 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.189177990 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.189210892 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.189227104 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.189246893 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.189295053 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.274404049 CET	49732	443	192.168.2.5	75.2.83.248
Mar 20, 2023 23:14:00.274458885 CET	443	49732	75.2.83.248	192.168.2.5
Mar 20, 2023 23:14:00.359517097 CET	49735	443	192.168.2.5	142.250.185.237
Mar 20, 2023 23:14:00.359575033 CET	443	49735	142.250.185.237	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:13:58.694641113 CET	51301	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:13:58.696841002 CET	55303	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:13:58.702814102 CET	50278	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:13:58.712229013 CET	53	51301	1.1.1.1	192.168.2.5
Mar 20, 2023 23:13:58.714293957 CET	53	55303	1.1.1.1	192.168.2.5
Mar 20, 2023 23:13:58.720139027 CET	53	50278	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:00.279421091 CET	57096	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:00.321419954 CET	53	57096	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:00.327910900 CET	63823	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:00.333157063 CET	58686	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:00.343931913 CET	57659	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:00.349195957 CET	53	63823	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:00.350797892 CET	53	58686	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:00.377329111 CET	53	57659	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.115431070 CET	55762	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.117314100 CET	54226	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.132551908 CET	53	55762	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.182491064 CET	61330	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.199810982 CET	53	61330	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.342125893 CET	51235	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.359108925 CET	53	51235	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.431765079 CET	64325	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.449028015 CET	53	64325	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.702487946 CET	59924	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.719336987 CET	53	59924	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.807262897 CET	64359	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:01.824207067 CET	53	64359	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:01.986496925 CET	59725	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.004285097 CET	53	59725	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.120417118 CET	59284	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.124309063 CET	49553	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.140208960 CET	53	59284	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.155183077 CET	53	49553	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.320122004 CET	58626	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.337241888 CET	53	58626	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.347619057 CET	60471	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.351387978 CET	58536	53	192.168.2.5	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 23:14:02.364888906 CET	53	60471	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.528897047 CET	52710	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.532011986 CET	61835	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.546056986 CET	53	52710	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.549653053 CET	53	61835	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.806629896 CET	57237	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.823458910 CET	53	57237	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:02.940901041 CET	51803	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:02.957678080 CET	53	51803	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:03.510663033 CET	55596	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:03.658840895 CET	54079	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:03.676111937 CET	53	54079	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:03.869405985 CET	58384	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:03.887854099 CET	53	58384	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:04.088033915 CET	49765	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:04.105509043 CET	53	49765	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:04.846575022 CET	55522	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:04.863913059 CET	53	55522	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:05.118741989 CET	54267	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:05.136539936 CET	53	54267	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:06.402050972 CET	60266	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:06.420185089 CET	53	60266	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:16.820343971 CET	52692	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:16.960437059 CET	53	52692	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:17.152658939 CET	59792	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:17.170135975 CET	53	59792	1.1.1.1	192.168.2.5
Mar 20, 2023 23:14:17.902318001 CET	65134	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:14:17.919872999 CET	53	65134	1.1.1.1	192.168.2.5
Mar 20, 2023 23:15:06.497411013 CET	60010	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:15:06.514492035 CET	53	60010	1.1.1.1	192.168.2.5
Mar 20, 2023 23:15:17.366421938 CET	61468	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:15:17.383615971 CET	53	61468	1.1.1.1	192.168.2.5
Mar 20, 2023 23:16:01.793258905 CET	53404	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:16:01.832674980 CET	53	53404	1.1.1.1	192.168.2.5
Mar 20, 2023 23:16:01.835256100 CET	62632	53	192.168.2.5	1.1.1.1
Mar 20, 2023 23:16:01.852653980 CET	53	62632	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 23:13:58.694641113 CET	192.168.2.5	1.1.1.1	0x1f72	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:13:58.696841002 CET	192.168.2.5	1.1.1.1	0x5f9d	Standard query (0)	prezi.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:13:58.702814102 CET	192.168.2.5	1.1.1.1	0x8f54	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.279421091 CET	192.168.2.5	1.1.1.1	0xf6b8	Standard query (0)	prezi-analytics.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.327910900 CET	192.168.2.5	1.1.1.1	0xc5dc	Standard query (0)	assets.prezicdn.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.333157063 CET	192.168.2.5	1.1.1.1	0x900e	Standard query (0)	assets1.prezicdn.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.343931913 CET	192.168.2.5	1.1.1.1	0xec97	Standard query (0)	package-bundles.prezi.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.115431070 CET	192.168.2.5	1.1.1.1	0xd2dd	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.117314100 CET	192.168.2.5	1.1.1.1	0xd83d	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.182491064 CET	192.168.2.5	1.1.1.1	0x47db	Standard query (0)	cdn.taboola.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.342125893 CET	192.168.2.5	1.1.1.1	0x8e66	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 23:14:01.431765079 CET	192.168.2.5	1.1.1.1	0x6014	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.702487946 CET	192.168.2.5	1.1.1.1	0xbbab	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.807262897 CET	192.168.2.5	1.1.1.1	0xb761	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.986496925 CET	192.168.2.5	1.1.1.1	0x1c9	Standard query (0)	bandar-logger.prezi.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.120417118 CET	192.168.2.5	1.1.1.1	0x9ba3	Standard query (0)	cdn.jifo.co	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.124309063 CET	192.168.2.5	1.1.1.1	0xf98e	Standard query (0)	d2pj2twnjx3fya.cloudfront.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.320122004 CET	192.168.2.5	1.1.1.1	0x345b	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.347619057 CET	192.168.2.5	1.1.1.1	0x1ddc	Standard query (0)	cdn.linkedin.oribi.io	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.351387978 CET	192.168.2.5	1.1.1.1	0x4e74	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.528897047 CET	192.168.2.5	1.1.1.1	0xb5b5	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.532011986 CET	192.168.2.5	1.1.1.1	0x1ca0	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.806629896 CET	192.168.2.5	1.1.1.1	0x5e7c	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.940901041 CET	192.168.2.5	1.1.1.1	0x9d63	Standard query (0)	trc.taboola.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.510663033 CET	192.168.2.5	1.1.1.1	0xae3	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.658840895 CET	192.168.2.5	1.1.1.1	0x5206	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.869405985 CET	192.168.2.5	1.1.1.1	0xd0b	Standard query (0)	pips.taboola.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:04.088033915 CET	192.168.2.5	1.1.1.1	0xa4b4	Standard query (0)	cds.taboola.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:04.846575022 CET	192.168.2.5	1.1.1.1	0x498	Standard query (0)	trc-events.taboola.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:05.118741989 CET	192.168.2.5	1.1.1.1	0x93c9	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:06.402050972 CET	192.168.2.5	1.1.1.1	0x4feb	Standard query (0)	prezigram-assets.prezicdn.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:16.820343971 CET	192.168.2.5	1.1.1.1	0xac92	Standard query (0)	msdiufvm2163e59c4b67124.opticair.ru	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:17.152658939 CET	192.168.2.5	1.1.1.1	0x2dce	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:17.902318001 CET	192.168.2.5	1.1.1.1	0xb52a	Standard query (0)	challenges.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:15:06.497411013 CET	192.168.2.5	1.1.1.1	0x995a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:15:17.366421938 CET	192.168.2.5	1.1.1.1	0x5cf1	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:16:01.793258905 CET	192.168.2.5	1.1.1.1	0x7871	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:16:01.835256100 CET	192.168.2.5	1.1.1.1	0x3b57	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
Mar 20, 2023 23:13:58.712229013 CET	1.1.1.1	192.168.2.5	0x1f72	No error (0)	accounts.google.com		142.250.185.237	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:13:58.714293957 CET	1.1.1.1	192.168.2.5	0x5f9d	No error (0)	prezi.com		75.2.83.248	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:13:58.714293957 CET	1.1.1.1	192.168.2.5	0x5f9d	No error (0)	prezi.com		99.83.220.209	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 23:13:58.720139027 CET	1.1.1.1	192.168.2.5	0x8f54	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:13:58.720139027 CET	1.1.1.1	192.168.2.5	0x8f54	No error (0)	clients.l.google.com		142.250.186.142	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.321419954 CET	1.1.1.1	192.168.2.5	0xf6b8	No error (0)	prezi-analytics.com		75.2.83.248	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.321419954 CET	1.1.1.1	192.168.2.5	0xf6b8	No error (0)	prezi-analytics.com		99.83.220.209	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.349195957 CET	1.1.1.1	192.168.2.5	0xc5dc	No error (0)	assets.prezicdn.net	d3aeorqw7ononu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:00.349195957 CET	1.1.1.1	192.168.2.5	0xc5dc	No error (0)	d3aeorqw7ononu.cloudfront.net		18.165.227.73	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.349195957 CET	1.1.1.1	192.168.2.5	0xc5dc	No error (0)	d3aeorqw7ononu.cloudfront.net		18.165.227.121	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.349195957 CET	1.1.1.1	192.168.2.5	0xc5dc	No error (0)	d3aeorqw7ononu.cloudfront.net		18.165.227.72	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.349195957 CET	1.1.1.1	192.168.2.5	0xc5dc	No error (0)	d3aeorqw7ononu.cloudfront.net		18.165.227.112	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.350797892 CET	1.1.1.1	192.168.2.5	0x900e	No error (0)	assets1.prezicdn.net	d1zvw2klwdlloe.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:00.350797892 CET	1.1.1.1	192.168.2.5	0x900e	No error (0)	d1zvw2klwdlloe.cloudfront.net		18.66.122.80	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.350797892 CET	1.1.1.1	192.168.2.5	0x900e	No error (0)	d1zvw2klwdlloe.cloudfront.net		18.66.122.62	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.350797892 CET	1.1.1.1	192.168.2.5	0x900e	No error (0)	d1zvw2klwdlloe.cloudfront.net		18.66.122.50	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.350797892 CET	1.1.1.1	192.168.2.5	0x900e	No error (0)	d1zvw2klwdlloe.cloudfront.net		18.66.122.48	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.377329111 CET	1.1.1.1	192.168.2.5	0xec97	No error (0)	package-bundles.prezi.com	d3rwxsx3brl7p6.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:00.377329111 CET	1.1.1.1	192.168.2.5	0xec97	No error (0)	d3rwxsx3brl7p6.cloudfront.net		99.86.4.124	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.377329111 CET	1.1.1.1	192.168.2.5	0xec97	No error (0)	d3rwxsx3brl7p6.cloudfront.net		99.86.4.6	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.377329111 CET	1.1.1.1	192.168.2.5	0xec97	No error (0)	d3rwxsx3brl7p6.cloudfront.net		99.86.4.51	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:00.377329111 CET	1.1.1.1	192.168.2.5	0xec97	No error (0)	d3rwxsx3brl7p6.cloudfront.net		99.86.4.11	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.132551908 CET	1.1.1.1	192.168.2.5	0xd2dd	No error (0)	googleads.g.doubleclick.net		142.250.185.98	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.134974003 CET	1.1.1.1	192.168.2.5	0xd83d	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:01.199810982 CET	1.1.1.1	192.168.2.5	0x47db	No error (0)	cdn.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:01.199810982 CET	1.1.1.1	192.168.2.5	0x47db	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.199810982 CET	1.1.1.1	192.168.2.5	0x47db	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.199810982 CET	1.1.1.1	192.168.2.5	0x47db	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 23:14:01.199810982 CET	1.1.1.1	192.168.2.5	0x47db	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.359108925 CET	1.1.1.1	192.168.2.5	0x8e66	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.359108925 CET	1.1.1.1	192.168.2.5	0x8e66	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.359108925 CET	1.1.1.1	192.168.2.5	0x8e66	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.359108925 CET	1.1.1.1	192.168.2.5	0x8e66	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.359108925 CET	1.1.1.1	192.168.2.5	0x8e66	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.449028015 CET	1.1.1.1	192.168.2.5	0x6014	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:01.449028015 CET	1.1.1.1	192.168.2.5	0x6014	No error (0)	scontent.xx.fbcdn.net		157.240.20.19	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.719336987 CET	1.1.1.1	192.168.2.5	0xbbab	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:01.824207067 CET	1.1.1.1	192.168.2.5	0xb761	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.004285097 CET	1.1.1.1	192.168.2.5	0x1c9	No error (0)	bandar-logger.prezi.com		52.200.133.160	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.004285097 CET	1.1.1.1	192.168.2.5	0x1c9	No error (0)	bandar-logger.prezi.com		3.234.156.222	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.004285097 CET	1.1.1.1	192.168.2.5	0x1c9	No error (0)	bandar-logger.prezi.com		54.85.152.153	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.140208960 CET	1.1.1.1	192.168.2.5	0x9ba3	No error (0)	cdn.jifo.co		104.26.7.6	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.140208960 CET	1.1.1.1	192.168.2.5	0x9ba3	No error (0)	cdn.jifo.co		172.67.74.6	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.140208960 CET	1.1.1.1	192.168.2.5	0x9ba3	No error (0)	cdn.jifo.co		104.26.6.6	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.155183077 CET	1.1.1.1	192.168.2.5	0xf98e	No error (0)	d2pj2twnjx3fya.cloudfront.net		18.66.121.214	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.155183077 CET	1.1.1.1	192.168.2.5	0xf98e	No error (0)	d2pj2twnjx3fya.cloudfront.net		18.66.121.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.155183077 CET	1.1.1.1	192.168.2.5	0xf98e	No error (0)	d2pj2twnjx3fya.cloudfront.net		18.66.121.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.155183077 CET	1.1.1.1	192.168.2.5	0xf98e	No error (0)	d2pj2twnjx3fya.cloudfront.net		18.66.121.164	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.337241888 CET	1.1.1.1	192.168.2.5	0x345b	No error (0)	www.google.ch		142.250.185.131	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.364888906 CET	1.1.1.1	192.168.2.5	0x1ddc	No error (0)	cdn.linkedin.oribi.io	d1ni990a184w7d.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:02.364888906 CET	1.1.1.1	192.168.2.5	0x1ddc	No error (0)	d1ni990a184w7d.cloudfront.net		13.226.175.126	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.364888906 CET	1.1.1.1	192.168.2.5	0x1ddc	No error (0)	d1ni990a184w7d.cloudfront.net		13.226.175.70	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.364888906 CET	1.1.1.1	192.168.2.5	0x1ddc	No error (0)	d1ni990a184w7d.cloudfront.net		13.226.175.34	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 23:14:02.364888906 CET	1.1.1.1	192.168.2.5	0x1ddc	No error (0)	d1ni990a184w7d.cloudfront.net		13.226.175.16	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.368578911 CET	1.1.1.1	192.168.2.5	0x4e74	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:02.368578911 CET	1.1.1.1	192.168.2.5	0x4e74	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:02.546056986 CET	1.1.1.1	192.168.2.5	0xb5b5	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.546056986 CET	1.1.1.1	192.168.2.5	0xb5b5	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.546056986 CET	1.1.1.1	192.168.2.5	0xb5b5	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.546056986 CET	1.1.1.1	192.168.2.5	0xb5b5	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.546056986 CET	1.1.1.1	192.168.2.5	0xb5b5	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.549653053 CET	1.1.1.1	192.168.2.5	0x1ca0	No error (0)	js.hs-banner.com		104.18.33.171	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.549653053 CET	1.1.1.1	192.168.2.5	0x1ca0	No error (0)	js.hs-banner.com		172.64.154.85	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.823458910 CET	1.1.1.1	192.168.2.5	0x5e7c	No error (0)	stats.g.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.823458910 CET	1.1.1.1	192.168.2.5	0x5e7c	No error (0)	stats.g.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.823458910 CET	1.1.1.1	192.168.2.5	0x5e7c	No error (0)	stats.g.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.823458910 CET	1.1.1.1	192.168.2.5	0x5e7c	No error (0)	stats.g.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.957678080 CET	1.1.1.1	192.168.2.5	0x9d63	No error (0)	trc.taboola.com	dualstack.tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:02.957678080 CET	1.1.1.1	192.168.2.5	0x9d63	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.957678080 CET	1.1.1.1	192.168.2.5	0x9d63	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.957678080 CET	1.1.1.1	192.168.2.5	0x9d63	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:02.957678080 CET	1.1.1.1	192.168.2.5	0x9d63	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.527936935 CET	1.1.1.1	192.168.2.5	0xae3	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:03.676111937 CET	1.1.1.1	192.168.2.5	0x5206	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:03.676111937 CET	1.1.1.1	192.168.2.5	0x5206	No error (0)	star-mini.c10r.facebook.com		157.240.20.35	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.887854099 CET	1.1.1.1	192.168.2.5	0xd0b	No error (0)	pips.taboola.com	dualstack.tls13.taboola.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
Mar 20, 2023 23:14:03.887854099 CET	1.1.1.1	192.168.2.5	0xd0b	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.887854099 CET	1.1.1.1	192.168.2.5	0xd0b	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.887854099 CET	1.1.1.1	192.168.2.5	0xd0b	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:03.887854099 CET	1.1.1.1	192.168.2.5	0xd0b	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:04.105509043 CET	1.1.1.1	192.168.2.5	0xa4b4	No error (0)	cds.taboola.com	us-cds.taboola.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:04.105509043 CET	1.1.1.1	192.168.2.5	0xa4b4	No error (0)	us-cds.taboola.com		141.226.224.32	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:04.863913059 CET	1.1.1.1	192.168.2.5	0x498	No error (0)	trc-events.taboola.com	am-trc-events.taboola.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:04.863913059 CET	1.1.1.1	192.168.2.5	0x498	No error (0)	am-trc-events.taboola.com	am-vip001.taboola.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 23:14:04.863913059 CET	1.1.1.1	192.168.2.5	0x498	No error (0)	am-vip001.taboola.com		141.226.228.48	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:05.136539936 CET	1.1.1.1	192.168.2.5	0x93c9	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:05.136539936 CET	1.1.1.1	192.168.2.5	0x93c9	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:06.420185089 CET	1.1.1.1	192.168.2.5	0x4feb	No error (0)	prezigram-assets.prezicdn.net		18.66.218.128	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:06.420185089 CET	1.1.1.1	192.168.2.5	0x4feb	No error (0)	prezigram-assets.prezicdn.net		18.66.218.115	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:06.420185089 CET	1.1.1.1	192.168.2.5	0x4feb	No error (0)	prezigram-assets.prezicdn.net		18.66.218.109	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:06.420185089 CET	1.1.1.1	192.168.2.5	0x4feb	No error (0)	prezigram-assets.prezicdn.net		18.66.218.57	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:16.960437059 CET	1.1.1.1	192.168.2.5	0xac92	No error (0)	msdiufvm2163e59c4b67124.opticair.ru		188.114.96.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:16.960437059 CET	1.1.1.1	192.168.2.5	0xac92	No error (0)	msdiufvm2163e59c4b67124.opticair.ru		188.114.97.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:17.170135975 CET	1.1.1.1	192.168.2.5	0x2dce	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:17.919872999 CET	1.1.1.1	192.168.2.5	0xb52a	No error (0)	challenges.cloudflare.com		104.18.7.185	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:14:17.919872999 CET	1.1.1.1	192.168.2.5	0xb52a	No error (0)	challenges.cloudflare.com		104.18.6.185	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:15:06.514492035 CET	1.1.1.1	192.168.2.5	0x995a	No error (0)	accounts.google.com		142.250.185.141	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:15:17.383615971 CET	1.1.1.1	192.168.2.5	0x5cf1	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:16:01.832674980 CET	1.1.1.1	192.168.2.5	0x7871	No error (0)	www.google.com		142.250.186.36	A (IP address)	IN (0x0001)	false
Mar 20, 2023 23:16:01.852653980 CET	1.1.1.1	192.168.2.5	0x3b57	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false

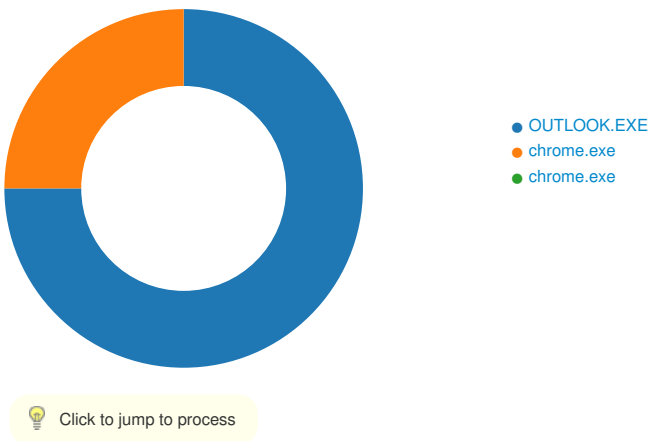
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS

HTTP Request Dependency Graph

- prezi.com
- accounts.google.com
- clients2.google.com
- https:
  - assets1.prezicdn.net
  - package-bundles.prezi.com
  - assets.prezicdn.net
  - prezi-analytics.com
  - cdn.taboola.com
  - googleads.g.doubleclick.net
  - js.hs-scripts.com
  - connect.facebook.net
  - cdn.jifo.co
  - www.google.com
  - d2pj2twnjx3fya.cloudfront.net
  - bandar-logger.prezi.com
  - www.google.ch
  - js.hs-banner.com
  - js.hs-analytics.net
  - cdn.linkedin.oribi.io
  - stats.g.doubleclick.net
  - trc.taboola.com
  - www.facebook.com
  - pips.taboola.com
  - cds.taboola.com
  - trc-events.taboola.com
  - track.hubspot.com
  - prezigram-assets.prezicdn.net
  - msdiufvm2163e59c4b67124.opticair.ru
  - challenges.cloudflare.com
- a.nel.cloudflare.com

Statistics

Behavior



System Behavior

Analysis Process: OUTLOOK.EXE PID: 260, Parent PID: -1

General

Target ID:	0
Start time:	23:13:52
Start date:	20/03/2023
Path:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail
Imagebase:	0x7ff669f00000
File size:	41778000 bytes
MD5 hash:	CA3FDE8329DE07C95897DB0D828545CD
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_Accessibility_ReminderType	unicode	{"name":"Accessibility_ReminderType","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF66A1ABB70	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings	Accounts	unicode	[]	[{"scope":"","userUpn":"","accountAge":0,"timestamp":0,"anchorMailbox":"","roamingStatus":"LOCAL"}]	success or wait	1	7FF66A1ABE60	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Settings\Data	global_AccountsNeedResyncing	unicode	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"false","isFirstSync":"false","source":""}	{"name":"AccountsNeedResyncing","itemClass":"","id":"","scope":"global","parentSetting":"","secondaryKey":"","status":"LOCAL","type":"Bool","timestamp":0,"metadata":"","value":"true","isFirstSync":"false","source":""}	success or wait	1	7FF66A1ABB70	RegSetValueExW

Analysis Process: chrome.exe PID: **3732**, Parent PID: **1288**

General

Target ID:	1
Start time:	23:13:53
Start date:	20/03/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://prezi.com/i/rx6p99-v72pt/
Imagebase:	0x7ff6bfcc0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF6BFD188A3	RegSetValueExW

Analysis Process: chrome.exe PID: **4664**, Parent PID: **3732**

General

Target ID:	2
Start time:	23:13:55
Start date:	20/03/2023
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=2024 --field-trial-handle=1808,i,11624139978826758221,4570325623230477738,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6bfcc0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
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

Disassembly

No disassembly