ID: 17568
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 19:35:24
Date: 01/03/2023
Version: 37.0.0 Beryl

Table of Contents

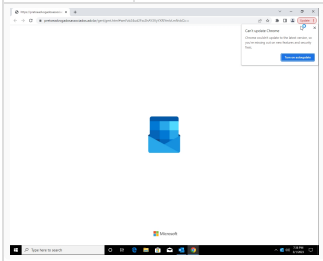
Windows Analysis Report

https://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYlOfq~~/OMbOowf~/aHR0cDovL0N1cmF...

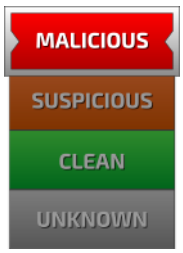
Overview

General Information

Sample URL:	https://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYlOfq~~/OMbOowf~/aHR0...WJpby5VU0VSaEJNWUkubXNibG9nZ2VyLmNvbS5hdS9qYXNvbi53YWxzaEBjdXJhdGViaW8uY29t
Analysis ID:	17568
Infos:	



Detection

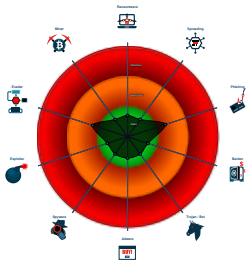


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Sample execution stops while proce...
- Yara signature match
- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 3128 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYlOfq~~/OMbOowf~/aHR0cDovL0N1cmF0ZWJpby5VU0VSaEJNWUkubXNibG9nZ2VyLmNvbS5hdS9qYXNvbi53YWxzaEBjdXJhdGViaW8uY29t MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - conhost.exe (PID: 1288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
  - chrome.exe (PID: 6140 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=2104 --field-trial-handle=1824,i,3608302658647549143,7935353812338714585,131072 --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

Source	Rule	Description	Author	Strings
93690.0.pages.csv	SUSP_obfuscated_JS_obfuscatorio	Detects JS obfuscation done by the js obfuscator (often malicious)	@imp0rtp3	• 0x45d0:$c8: while(!![]) • 0x45ef:$d1: parseInt(_0x15c7b0(0x156))/0x1+-parseInt(_0x15c7b0(0x15e))/0x2*(parseInt(_0x15c7b0(0x172))/0x3)+parseInt(_0x15c7b0(0x15d))/0x4+parseInt(_0x15c7b0(0x164))/0x5+-parseInt(_0x15c7b0(0x16d))/0x6*(• 0x460f:$d1: parseInt(_0x15c7b0(0x15e))/0x2*(parseInt(_0x15c7b0(0x172))/0x3)+parseInt(_0x15c7b0(0x15d))/0x4+parseInt(_0x15c7b0(0x164))/0x5+-parseInt(_0x15c7b0(0x16d))/0x6*(parseInt(_0x15c7b0(0x16e))/0x7)+- • 0x462f:$d1: parseInt(_0x15c7b0(0x172))/0x3)+parseInt(_0x15c7b0(0x15d))/0x4+parseInt(_0x15c7b0(0x164))/0x5+-parseInt(_0x15c7b0(0x16d))/0x6*(parseInt(_0x15c7b0(0x16e))/0x7)+-parseInt(_0x15c7b0(0x154))/0x8*(- • 0x464f:$d1: parseInt(_0x15c7b0(0x15d))/0x4+parseInt(_0x15c7b0(0x164))/0x5+-parseInt(_0x15c7b0(0x16d))/0x6*(parseInt(_0x15c7b0(0x16e))/0x7)+-parseInt(_0x15c7b0(0x154))/0x8*(-parseInt(_0x15c7b0(0x173))/0x9)+

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

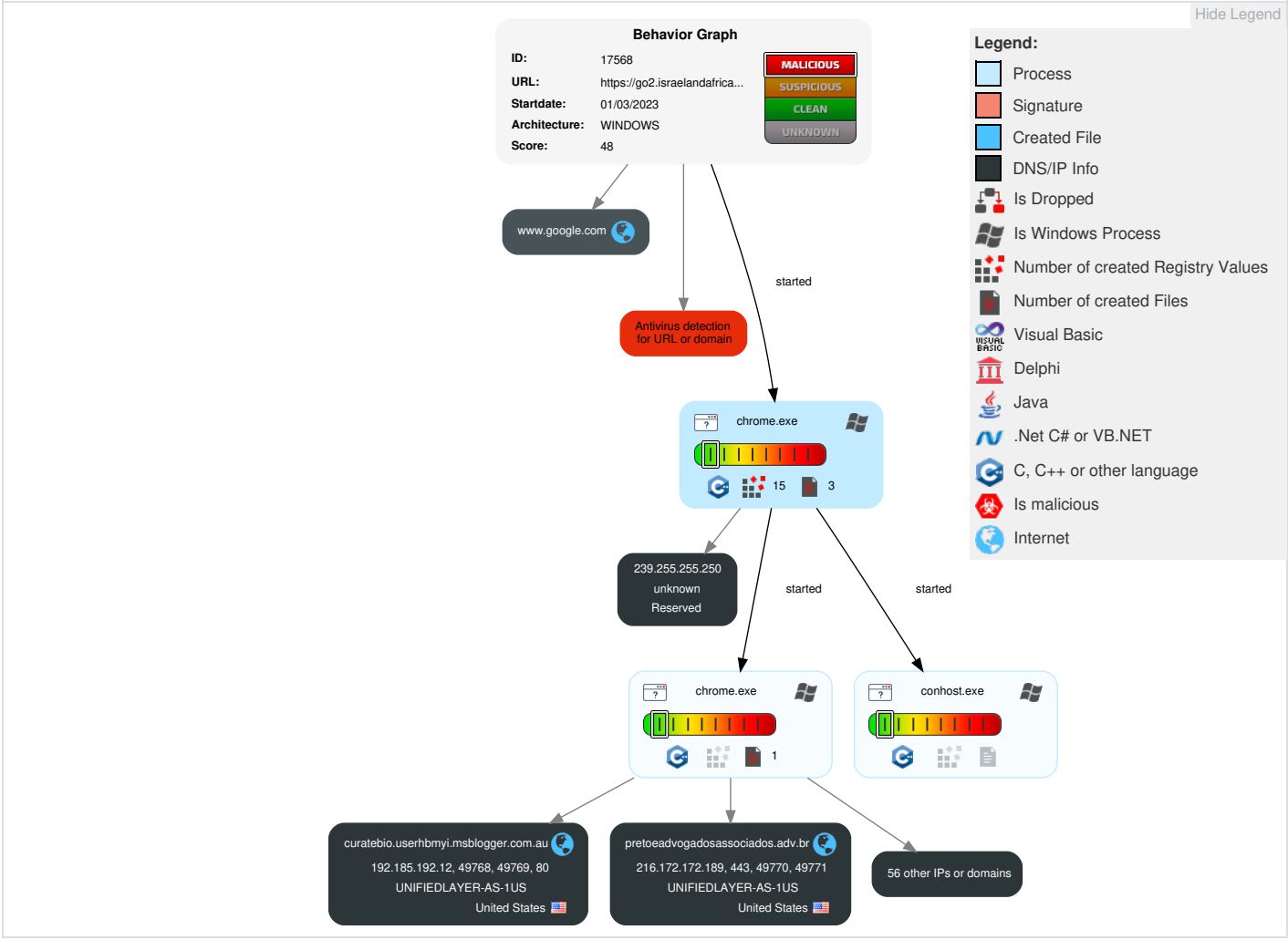
AV Detection

Antivirus detection for URL or domain

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	5 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	6 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	4 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

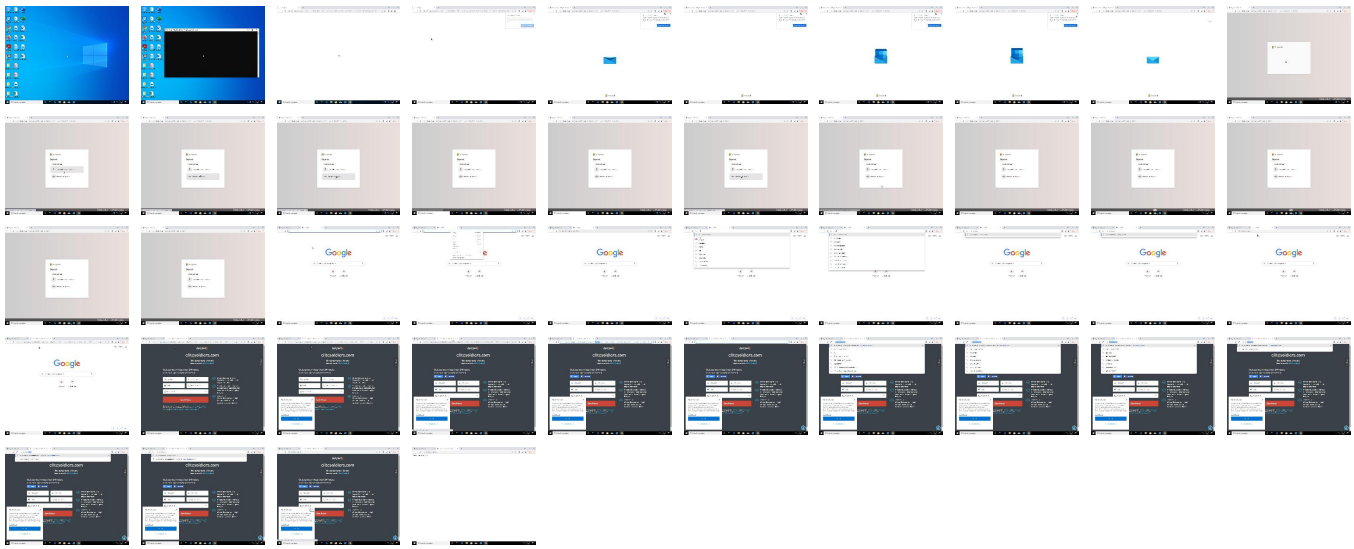
Behavior Graph

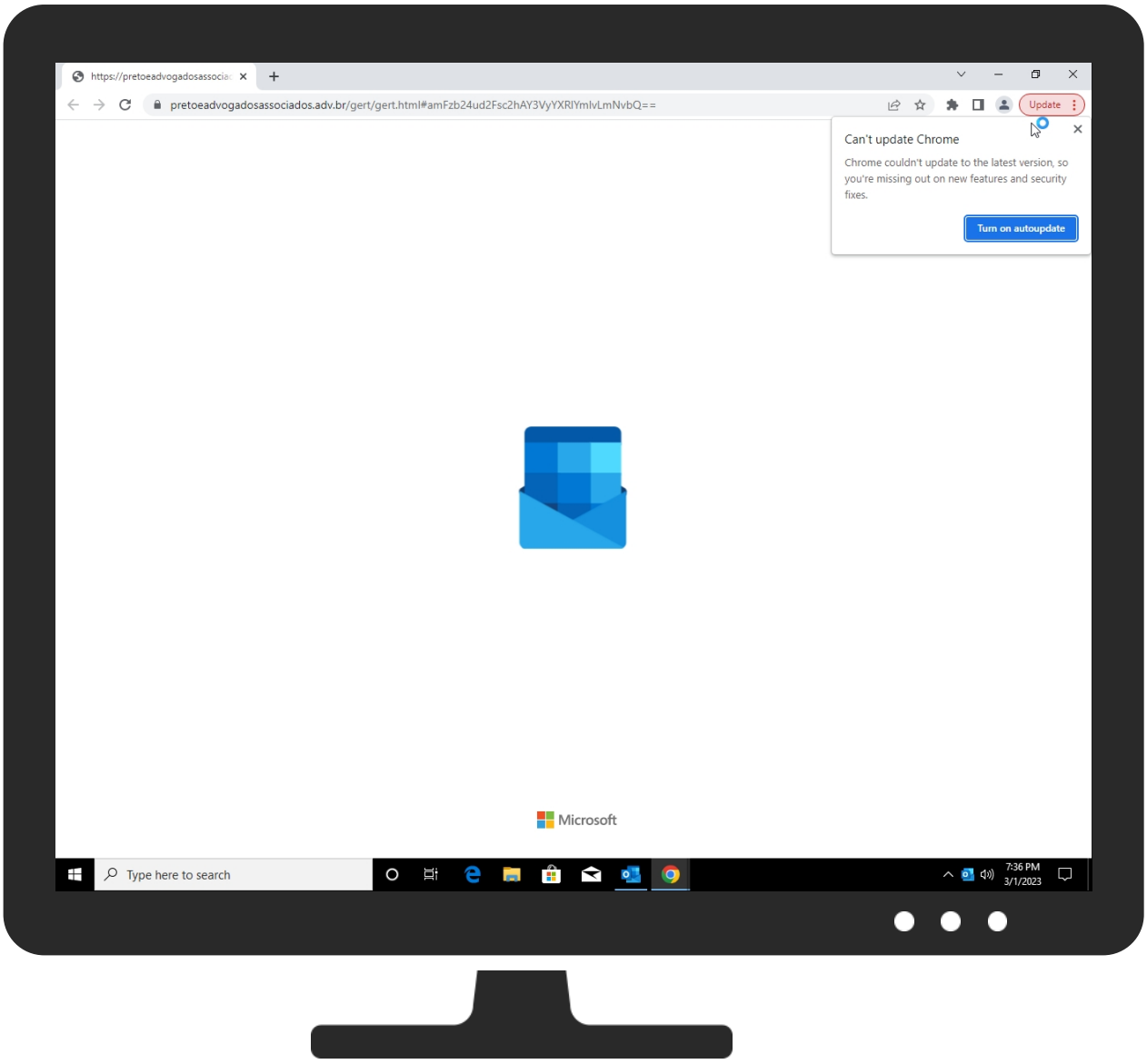


Screenshots

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://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYIOfq~~/OMbOowf~/aHR0cDovL0N1cmF0ZWJpby5VU0VSaEJNWUkubXNibG9nZ2VyLmNvbS5hdS9qYXNvbi53YWxzaEBjdXJhdGViaW8uY29t	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://pretoeadvogadosassociados.adv.br/gert/gert.html#amFzb24ud2Fsc2hAY3VyYXRlYmlvLmNvbQ==	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://c2.elitesoldiers.org/favicon.ico	0%	Avira URL Cloud	safe	
http://https://analytics.audioeye.com/air/v0/send	0%	Virustotal		Browse
http://c2.elitesoldiers.com/	0%	Avira URL Cloud	safe	
http://curatebio.userhbmyi.msblogger.com.au/jason.walsh@curatebio.com	0%	Avira URL Cloud	safe	
http://https://analytics.audioeye.com/air/v0/send	0%	Avira URL Cloud	safe	
http://https://d.impactradius-event.com/A136666-2811-40ba-bff2-3df3af8bc2ae1.js	0%	Avira URL Cloud	safe	
http://https://pretoeadvogadosassociados.adv.br/gert/gert.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.buydomains.com	207.148.248.132	true	false		high
dart.l.doubleclick.net	172.217.18.102	true	false		high
visitor-services.bold360.com	18.157.190.196	true	false		high
rpc-dc19.bold360.com	52.41.47.191	true	false		high
pretoeadvogadosassociados.adv.br	216.172.172.189	true	false		unknown
adservice.google.com	142.250.181.226	true	false		high
p01g.t.eloqua.com	142.0.173.27	true	false		high
nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com	52.204.155.250	true	false		high
stats.g.doubleclick.net	66.102.1.154	true	false		high
insight.adsrvr.org	3.33.220.150	true	false		high
scontent.xx.fbcdn.net	157.240.253.1	true	false		high
privacyportal.onetrust.com	104.18.43.158	true	false		high
script.hotjar.com	18.66.147.47	true	false		high
cdnjs.cloudflare.com	104.17.24.14	true	false		high
curatebio.userhbmyi.msblogger.com.au	192.185.192.12	true	false		unknown
c2.elitesoldiers.org	194.87.151.158	true	false		unknown
d.monetate-prod.zone	54.161.222.185	true	false		unknown
analytics.audioeye.com	44.239.25.130	true	false		unknown
www.google.com	172.217.16.196	true	false		high
luvtimwrtytrinity.com	64.225.112.96	true	false		unknown
d.impactradius-event.com	35.186.249.72	true	false		unknown
api.buydomains.com	207.148.248.128	true	false		high
static-cdn.hotjar.com	18.66.97.37	true	false		high
accounts.google.com	216.58.212.141	true	false		high
plus.l.google.com	142.250.185.110	true	false		high
d1pux066p3zvi3.cloudfront.net	13.32.99.51	true	false		high
googleads.g.doubleclick.net	142.250.181.226	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.237.45	true	false		unknown
clients.l.google.com	142.250.185.174	true	false		high
c2.elitesoldiers.com	207.148.248.143	true	false		unknown
www.google.ch	142.250.185.195	true	false		high
cdn.cookielaw.org	104.19.188.97	true	false		high
geolocation.onetrust.com	172.64.144.98	true	false		high
vmss.boldchat.com	unknown	unknown	false		high
6928088.fls.doubleclick.net	unknown	unknown	false		high
vms.boldchat.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
static.buydomains.com	unknown	unknown	false		high
wsmcdn.audioeye.com	unknown	unknown	false		unknown
go2.israelandafrica.com	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
static.hotjar.com	unknown	unknown	false		high
se.monetate.net	unknown	unknown	false		high
d.monetate.net	unknown	unknown	false		high
wsv3cdn.audioeye.com	unknown	unknown	false		unknown
sb.monetate.net	unknown	unknown	false		high
visitor-services.boldchat.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
apps.mypurecloud.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high
s1731649222.t.eloqua.com	unknown	unknown	false		high

Contacted URLs

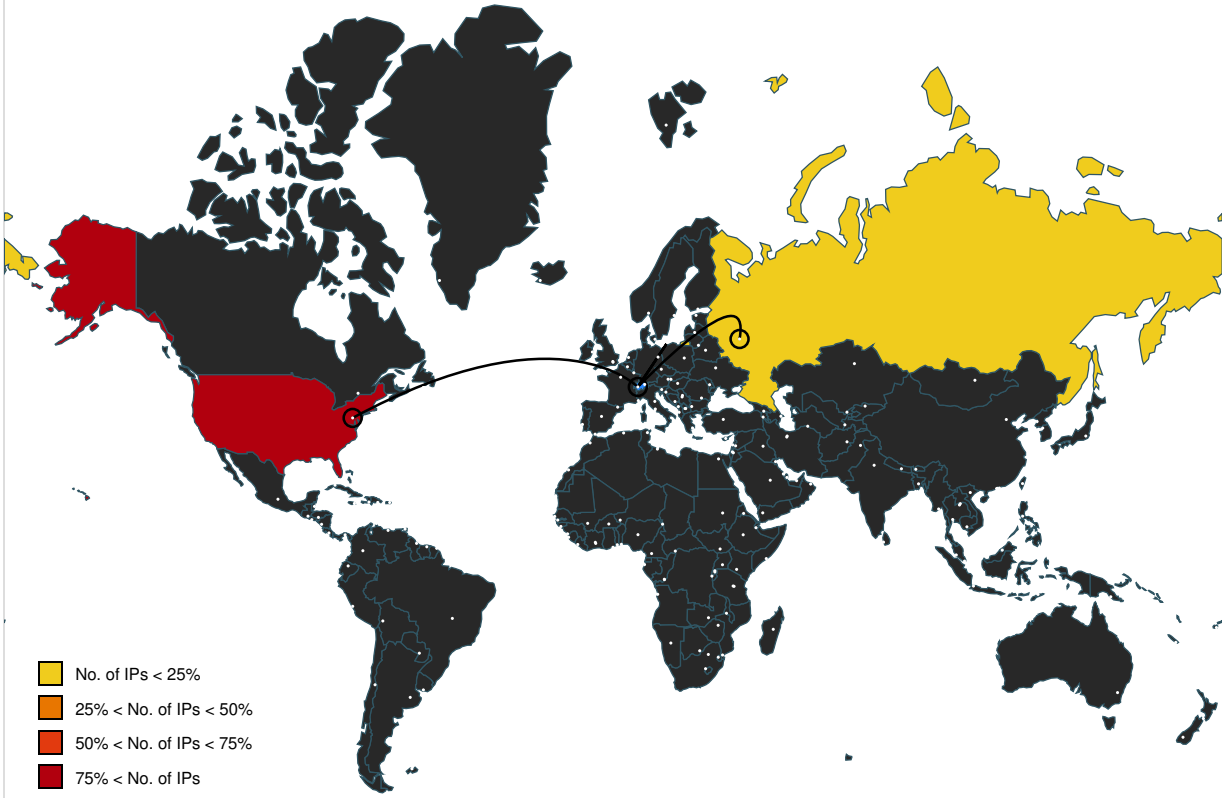
Name	Malicious	Antivirus Detection	Reputation
http://https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-700.woff	false		high
http://https://static.buydomains.com//eloqua.js?version=2023-02-09-1	false		high
http://https://vmss.boldchat.com/aid/288248359635244124 8/bc.vms4/vms.js	false		high
http://c2.elitesoldiers.com/	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-47761645-6&cid=95733560.1677695849&jid=262765478&gjid=280525562&_gid=213938997.1677695849&_u=YGDAAEABAAAAAGgCI~&z=459877897	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.com&oit=3&cp=20&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elites&oit=1&cp=9&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers&oit=1&cp=16&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/scripttemplates/202301.2.0/assets/otFloatingRoundedCorner.json	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesold&oit=1&cp=12&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/logos/static/powered_by_logo.svg	false		high
http://https://6928088.fls.doubleclick.net/activityi;dc_pre=CPyky4iwu_0CFSoFewodco0BhQ;src=6928088;type=remar0;cat=bd-al0;ord=5403398804933;u=elitesoldiers.com;gtm=45He32r0;auiddc=1118355647.1677695847;u2=elitesoldiers.com;u1=unknown%20value;~oref=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect?	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.e&oit=1&cp=4&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-regular.woff	false		high
http://https://apps.mypurecloud.com/widgets/9.0/cxbus.min.js	false		high
http://https://c2.elitesoldiers.org/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://apps.mypurecloud.com/webfonts/roboto.css	false		high
http://https://static.buydomains.com//browser/img/favicon.ico?version=2023-02-09-1	false		high
http://https://connect.facebook.net/en_US/sdk.js?hash=bc91546a6be007a51eb44b9f223eb53e	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2&oit=1&cp=2&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://connect.facebook.net/en_US/sdk.js	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-47761645-6&cid=95733560.1677695849&jid=460476489&_u=YGBAgEABAAAAAEgAI~&z=108882502	false		high
http://https://d.monetate.net/trk/4/s/a-685a7abb/d/www.qa.buydomains.com/479339224-0?mr=t1545228048&mi=%272.106500537.1677695849599%27&mt=!n&cs=!f&e=!(viewPage,gt)&pt=unknown&r=%27%27&sw=1280&sh=1024&sc=24&j=!f&u=%27https://www.buydomains.com/lander/elitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect%27&fl=!f&hvc=!t&eoq=!t	false		high
http://https://cdn.cookielaw.org/logos/static/ot_guard_logo.svg	false		high
http://https://www.google.com/async/newtab_ogb?hl=en-US&async=fixed:0	false		high
http://https://www.buydomains.com/browser/js/worker/workerJS.min.js	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://static.buydomains.com//browser/img/tdfs/logo-custom.svg?version=2023-02-09-1	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elit&oit=1&cp=7&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.buydomains.com//trackingParams.js?version=2023-02-09-1	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
http://https://static.buydomains.com//browser/js/vendor/elqCfg.min.js?version=2023-02-09-1	false		high
http://https://s1731649222.t.eloqua.com/visitor/v200/svrGP?pps=3&siteid=1731649222&ref2=elqNone&tzo=-60&ms=235&optin=disabled	false		high
http://https://www.buydomains.com/get-user-fields	false		high
http://https://vms.boldchat.com/aid/2882483596352441248/bc.pv?script=true&securevm=true&&blur=false&vm=true&poll=65000&swidth=1280&sheight=1024&sdpi=96&url=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect&wdid=2943214817915460751&idid=815288250086333991&1677695850978&tabIdentifier=6110055183325786431&clientScheme=https&visitorTrackingAllowed=true&visitorToken=7036766419288412160&_bcvm_vrid_=true&_bcvm_vid_combined=1677695850980Sundefined&_bcvm_vrid_combined=1677695850980Sundefined&&hasbutton=false	false		high
http://https://adservice.google.com/ddm/fls/z/dc_pre=CPyky4iwu_0CFSoFewodco0BhQ;src=6928088;type=remar0;cat=bd-al0;ord=5403398804933;u=elitesoldiers.com;gtm=45He32r0;auiddc=*;u2=elitesoldiers.com;u1=unknown%20value;~oref=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect	false		high
http://curatebio.userhbmyi.msblogger.com.au/jason.walsh@curatebio.com	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesolde&oit=1&cp=13&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.buydomains.com/get-user-country-info/	false		high
http://https://cdn.cookielaw.org/scripttemplates/202301.2.0/assets/v2/otPcCenter.json	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAlkUAAAAAHjOK9ZepI7lU55yYRmOEigfrp6C	false		high
http://https://static.buydomains.com/browser/img/icons/selectArrowGrey.svg	false		high
http://https://script.hotjar.com/modules.3bdf981e73ecd1bf9fca.js	false		high
http://https://static.buydomains.com/browser/img/icons/checkmark-blue.svg	false		high
http://https://www.google.com/pagead/1p-user-list/1067119116/?random=1677695847339&cv=11&fst=1677693600000&bg=ffffff&guid=ON&async=1>m=45He32r0&u_w=1280&u_h=1024&label=9jrJCIX4tW0QjOTr_AM&frm=0&url=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect&tiba=Buy%20Domains%20-%20elitesoldiers.com%20is%20for%20sale!&fmt=3&is_vtc=1&cid=CAQSKQDUE5ymrYICgWv1O0klvpjD4kJNJMwZyD1GXm_vEaFB9wJ2QNMEPVhc&random=1690235126&rmt_tld=0&ipr=y	false		high
http://https://www.buydomains.com/version.html	false		high
http://https://cdn.cookielaw.org/consent/91181fd5-0816-4a3d-8427-63a8d53f717e/91181fd5-0816-4a3d-8427-63a8d53f717e.json	false		high
http://https://www.buydomains.com/browser/js/vendor/genesys-chat-widgets.min.css	false		high
http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.el&oit=1&cp=5&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.buydomains.com//browser/css/lander/g/lander-v7.css?version=2023-02-09-1	false		high
http://https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldier&oit=1&cp=15&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/scripttemplates/202301.2.0/assets/otCommonStyles.css	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.c&oit=1&cp=18&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.js	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldie&oit=1&cp=14&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.buydomains.com/browser/img/icons/public-24px.svg	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.&oit=1&cp=3&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://analytics.audioeye.com/air/v0/send	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesolder&oit=1&cp=14&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.hotjar.com/c/hotjar-541823.js?sv=7	false		high
http://https://d.impactradius-event.com/A136666-2811-40ba-bff2-3df3af8bc2ae1.js	false	• Avira URL Cloud: safe	unknown
http://https://wsv3cdn.audioeye.com/v2/frame/cookieStorage.html?build=prod/m&pscb=&cb=67f89c3	false		unknown
http://https://cdn.cookielaw.org/consent/91181fd5-0816-4a3d-8427-63a8d53f717e/6cb1a7b0-5ed5-4585-b708-bbbfbee82576/en.json	false		high
http://https://pretoeadvogadosassociados.adv.br/gert/gert.html	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/o/oauth2/iframe	false		high
http://https://www.buydomains.com/locate?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect	false		high
http://https://apps.mypurecloud.com/widgets/9.0/plugins/widgets-core.min.js	false		high
http://https://6928088.fls.doubleclick.net/activityi;src=6928088;type=remar0;cat=bd-al0;ord=5403398804933;u=elitesoldiers.com;gtm=45He32r0;auiddc=1118355647.1677695847;u2=elitesoldiers.com;u1=unknown%20value;~oref=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect?	false		high
http://https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-regular.woff2	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c&oit=1&cp=1&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://pretoeadvogadosassociados.adv.br/gert/gert.html#amFzb24ud2Fsc2hAY3VyYXRlYmlvLmNvbQ==	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C&co=aHR0cHM6Ly93d3cuYnV5ZG9tYWlucy5jb206NDQz&hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&size=invisible&badge=inline&cb=y189nut6t10x	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldi&oit=1&cp=13&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.buydomains.com/browser/img/icons/person-24px.svg	false		high
http://https://s1731649222.t.eloqua.com/visitor/v200/svrGP?pps=70&siteid=1731649222&ref=&ms=235	false		high
http://https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-700.woff2	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.eliteso&oit=1&cp=10&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C	false		high
http://https://www.google.com/recaptcha/api.js	false		high
http://https://www.google.com/recaptcha/api2/reload?k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C&co=aHR0cHM6Ly93d3cuYnV5ZG9tYWlucy5jb206NDQz&hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&size=invisible&badge=inline&cb=y189nut6t10x	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.co&oit=3&cp=19&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://static.buydomains.com//google_oauth.js?version=2023-02-09-1	false		high
http://https://www.buydomains.com/browser/js/vendor/genesys-chat-widgets.min.js	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.o&oit=1&cp=18&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesol&oit=1&cp=11&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/logos/03213524-9e9e-4852-a3ab-334c10e24fe4/a4e57db3-75be-4450-843d-640b760b40c3/c63e0daa-fd7e-4ff3-8fa1-3bc8b00d8047/BlankImg.png	false		high
http://https://accounts.google.com/o/oauth2/iframerpc?action=checkOrigin&origin=https%3A%2F%2Fwww.buydomains.com&client_id=26200011094-f6n31v26gh6o5hsjh2960tei8tdeiq28.apps.googleusercontent.com	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://static.buydomains.com/browser/img/icons/email-24px.svg	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.eli&oit=1&cp=6&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.org&oit=3&cp=20&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elite&oit=1&cp=8&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://www.google.com/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=c2.elitesoldiers.&oit=1&cp=17&gs_rn=42&psi=HfOUX1-31JW5RcEd&sugkey=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw	false		high
http://https://cdn.cookielaw.org/scripttemplates/202301.2.0/otBannerSdk.js	false		high
http://https://www.google.com/async/newtab_promos	false		high
http://https://6928088.fls.doubleclick.net/activityi;dc_pre=CPyky4iwu_0CFSoFewodco0BhQ;src=6928088;type=remar0;cat=bd-al0;ord=5403398804933;u=elitesoldiers.com;gtm=45He32r0;auiddc=1118355647.1677695847;u2=elitesoldiers.com;u1=unknown%20value;~oref=https%3A%2F%2Fwww.buydomains.com%2Flander%2Felitesoldiers.com%3Fdomain%3Delitesoldiers.com%26utm_source%3Delitesoldiers.com%26utm_medium%3Dclick%26utm_campaign%3Dtdfs-AprTest%26traffic_id%3DAprTest%26traffic_type%3Dtdfs%26redirect%3Dono-redirect?	false		high
http://https://c2.elitesoldiers.org/	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.66.97.37	static-cdn.hotjar.com	United States		3	MIT-GATEWAYSUS	false
54.161.222.185	d.monetate-prod.zone	United States		14618	AMAZON-AESUS	false
207.148.248.143	c2.elitesoldiers.com	United States		29873	BIZLAND-SDUS	false
66.102.1.154	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
216.172.172.189	pretoeadvogadosassociados.adv.br	United States		46606	UNIFIEDLAYER-AS-1US	false
3.33.220.150	insight.adsrvr.org	United States		8987	AMAZONEXPANSIONGB	false
64.225.112.96	luvtimwrtytrinity.com	United States		14061	DIGITALOCEAN-ASNUS	false
192.185.192.12	curatebio.userhbmyi.msblogger.com.au	United States		46606	UNIFIEDLAYER-AS-1US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved	?	unknown	unknown	false
194.87.151.158	c2.elitesoldiers.org	Russian Federation		208544	PAUTINA05RU	false
13.107.237.45	part-0017.t-0009.fdv2-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.18.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
18.157.190.196	visitor-services.bold360.com	United States		16509	AMAZON-02US	false
172.217.18.100	unknown	United States		15169	GOOGLEUS	false
18.66.147.47	script.hotjar.com	United States		3	MIT-GATEWAYSUS	false
52.41.47.191	rpc-dc19.bold360.com	United States		16509	AMAZON-02US	false
54.200.68.184	unknown	United States		16509	AMAZON-02US	false
142.0.173.27	p01g.t.eloqua.com	United States		7160	NETDYNAMICSUS	false
142.250.181.237	unknown	United States		15169	GOOGLEUS	false
207.148.248.128	api.buydomains.com	United States		29873	BIZLAND-SDUS	false
52.204.155.250	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
13.32.99.51	d1pux066p3zvi3.cloudfront.net	United States		16509	AMAZON-02US	false
207.148.248.132	www.buydomains.com	United States		29873	BIZLAND-SDUS	false
142.250.181.226	adservice.google.com	United States		15169	GOOGLEUS	false
104.18.43.158	privacyportal.onetrust.com	United States		13335	CLOUDFLARENETUS	false
172.64.144.98	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.174	clients.l.google.com	United States		15169	GOOGLEUS	false
35.186.249.72	d.impactradius-event.com	United States		15169	GOOGLEUS	false
142.250.181.228	unknown	United States		15169	GOOGLEUS	false
157.240.253.1	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
104.19.188.97	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
216.58.212.141	accounts.google.com	United States		15169	GOOGLEUS	false
44.239.25.130	analytics.audioeye.com	United States		16509	AMAZON-02US	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	17568
Start date and time:	2023-03-01 19:35:24 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://https://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYIOfq~~/OMbOowf~/aHR0cDovL0N1cmF0ZWJpby5VU0VSaEJNWUkubXNibG9nZ2VyLmNvbS5hdS9qYXNvbi53YWxzaEBjdXJhdGViaW8uY29t
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:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.win@43/2@48/35
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): SIHClient.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.190.160.22, 20.190.160.17, 40.126.32.72, 40.126.32.74, 40.126.32.136, 20.190.160.14, 40.126.32.76, 40.126.32.68, 142.250.186.163, 34.104.35.123, 69.16.175.42, 69.16.175.10, 142.250.186.99, 172.217.23.99, 142.250.185.110, 142.250.185.234, 142.250.185.195, 142.250.184.195, 142.250.185.232, 142.250.185.202, 142.250.74.202, 172.217.23.106, 142.250.185.106, 172.217.16.138, 142.250.184.202, 142.250.186.138, 142.250.186.74, 142.250.186.170, 142.250.185.138, 142.250.181.234, 142.250.186.106, 142.250.185.170, 142.250.186.42, 142.250.185.74, 142.250.184.206, 104.108.6.231, 104.18.36.34, 172.64.151.222
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, slscr.update.microsoft.com, clientservices.googleapis.com, www.tm.a.prd.aadg.trafficmanager.net, prda.aadg.msidentity.com, wsmcdn.audioeye.com.cdn.cloudflare.net, login.live.com, www.googletagmanager.com, update.googleapis.com, www.gstatic.com, cdn.onenote.net, www.google-analytics.com, http2.monetate.edgekey.net, wsv3cdn.audioeye.com.cdn.cloudflare.net, fonts.googleapis.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, encrypted-tbn0.gstatic.com, fonts.gstatic.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, aadcdn.msauth.net, login.msa.msidentity.com, firstparty-azurefd-prod.trafficmanager.net, e4361.b.akamaiedge.net, edgedl.me.gvt1.com, aadcdnoriginwus2.afd.azureedge.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\ConDrv

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.096521881401656
Encrypted:	false
SSDEEP:	6:sUuvLX+toHtW3o33QXmUvLX+toHtW3o33QXmUvLHs9oHtW3o33QXmUvLHs9oHtWY:sFXWY3A2SXWY3A2FyWY3A2FyWY3AG
MD5:	E7D25F8043229E1AE38783D560C02637
SHA1:	9C065D75E774A6F7D70326A799A8EFDD4C2940CB
SHA-256:	1D7BD86FB4FB392C6AB73133809154955230F9DFD74A84886AA5FFE304151E70
SHA-512:	6BBF13E399FAD28A4860508187CA045B2B61BC5D518D6C0C369AD701EE9E75948966538E4914198C60DB0A8B8910CD296B38672D7EDA464710EFE0BF0E7E2AA1
Malicious:	false
Reputation:	low
Preview:	[6140:6100:0301/193721.225:ERROR:ssl_client_socket_impl.cc(983)] handshake failed; returned -1, SSL error code 1, net_error -101..[6140:6100:0301/193721.225:ERROR:ssl_client_socket_impl.cc(983)] handshake failed; returned -1, SSL error code 1, net_error -101..[6140:6100:0301/193721.324:ERROR:ssl_client_socket_impl.cc(983)] handshake failed; returned -1, SSL error code 1, net_error -101..[6140:6100:0301/193721.324:ERROR:ssl_client_socket_impl.cc(983)] handshake failed; returned -1, SSL error code 1, net_error -101..

Static File Info

No static file info

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:36:06.132946014 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.133038044 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.133169889 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.133279085 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.133310080 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.133388996 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.134277105 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.134309053 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.134553909 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.134577990 CET	443	49764	142.250.185.174	192.168.2.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:36:06.235033989 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.236274958 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.236336946 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.237023115 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.237160921 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.238327980 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.238430023 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.240709066 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.245084047 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.245142937 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.247189999 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.247281075 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.312434912 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.312505007 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.312627077 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.328666925 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.328711033 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.405952930 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.411232948 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.411257029 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.413064003 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.413216114 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.636811972 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.636883974 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.637119055 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.640947104 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.641000032 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.641477108 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.641514063 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.641923904 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.644671917 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.644721031 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.644969940 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.645015001 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.645328045 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.645838022 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.645874023 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.673846006 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:06.673959017 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.675478935 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.675549030 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.675569057 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.675827026 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.675898075 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.707706928 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.707787991 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.707807064 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.708123922 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.708215952 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.737500906 CET	49764	443	192.168.2.2	142.250.185.174
Mar 1, 2023 19:36:06.737565041 CET	443	49764	142.250.185.174	192.168.2.2
Mar 1, 2023 19:36:06.738917112 CET	49763	443	192.168.2.2	216.58.212.141
Mar 1, 2023 19:36:06.738967896 CET	443	49763	216.58.212.141	192.168.2.2
Mar 1, 2023 19:36:06.919676065 CET	49766	443	192.168.2.2	194.87.151.158
Mar 1, 2023 19:36:06.919734955 CET	443	49766	194.87.151.158	192.168.2.2
Mar 1, 2023 19:36:07.616722107 CET	49768	80	192.168.2.2	192.185.192.12
Mar 1, 2023 19:36:07.710473061 CET	49769	80	192.168.2.2	192.185.192.12
Mar 1, 2023 19:36:07.741414070 CET	80	49768	192.185.192.12	192.168.2.2
Mar 1, 2023 19:36:07.741596937 CET	49768	80	192.168.2.2	192.185.192.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:36:07.744029045 CET	49768	80	192.168.2.2	192.185.192.12
Mar 1, 2023 19:36:07.835469007 CET	80	49769	192.185.192.12	192.168.2.2
Mar 1, 2023 19:36:07.835618973 CET	49769	80	192.168.2.2	192.185.192.12
Mar 1, 2023 19:36:07.868508101 CET	80	49768	192.185.192.12	192.168.2.2
Mar 1, 2023 19:36:08.002048016 CET	80	49768	192.185.192.12	192.168.2.2
Mar 1, 2023 19:36:08.141237020 CET	49768	80	192.168.2.2	192.185.192.12
Mar 1, 2023 19:36:08.821732044 CET	49770	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.821804047 CET	443	49770	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:08.821917057 CET	49770	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.822547913 CET	49770	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.822586060 CET	443	49770	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:08.838349104 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.838429928 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:08.838552952 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.838849068 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:08.838879108 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.106884003 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.109076023 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.109106064 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.110229969 CET	443	49770	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.112018108 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.112145901 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.112740040 CET	49770	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.112770081 CET	443	49770	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.113965988 CET	443	49770	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.114098072 CET	49770	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.115972996 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.115991116 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.116142988 CET	443	49771	216.172.172.189	192.168.2.2
Mar 1, 2023 19:36:09.117836952 CET	49771	443	192.168.2.2	216.172.172.189
Mar 1, 2023 19:36:09.117860079 CET	443	49771	216.172.172.189	192.168.2.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:36:06.082439899 CET	53801	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:06.095560074 CET	62638	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:06.096482038 CET	50049	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:06.100294113 CET	53	53801	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:06.113775969 CET	53	50049	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:06.247781038 CET	53	62638	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:06.951627970 CET	49571	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:07.593990088 CET	53	49571	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:08.421493053 CET	54266	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:08.787774086 CET	53	54266	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:09.157824993 CET	49389	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:09.175993919 CET	53	49389	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:09.183778048 CET	57390	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:09.201761007 CET	53	57390	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:09.604764938 CET	53544	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:09.883450031 CET	63358	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:09.938874960 CET	53	63358	1.1.1.1	192.168.2.2
Mar 1, 2023 19:36:19.916965961 CET	54161	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:36:19.934791088 CET	53	54161	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:07.577893019 CET	54636	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:07.595545053 CET	53	54636	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:09.208617926 CET	56048	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:09.226696014 CET	53	56048	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:09.234946012 CET	62175	53	192.168.2.2	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:37:09.252573967 CET	53	62175	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:21.131221056 CET	55541	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:21.331682920 CET	53	55541	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:21.670815945 CET	55190	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:21.937639952 CET	53	55190	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:22.211211920 CET	58534	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:22.229751110 CET	53	58534	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:23.316659927 CET	55638	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:23.334558010 CET	53	55638	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:23.342228889 CET	54976	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:23.560102940 CET	53	54976	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:23.810709000 CET	58857	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:23.887655020 CET	53	58857	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:25.603523970 CET	54801	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:25.629709005 CET	53	54801	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:25.925262928 CET	55228	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:25.942883968 CET	53	55228	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:26.120826960 CET	63209	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:26.138643980 CET	53	63209	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:26.526747942 CET	54842	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:26.580171108 CET	53	54842	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:26.815079927 CET	64226	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:26.832638979 CET	53	64226	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.533356905 CET	64723	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.550825119 CET	53	64723	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.631872892 CET	51053	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.631872892 CET	54298	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.640275002 CET	58145	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.642138958 CET	53075	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.649617910 CET	53	51053	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.658061981 CET	53	58145	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.678494930 CET	63575	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.679244995 CET	53	54298	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.731709003 CET	63613	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:27.749377012 CET	53	63613	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:27.884152889 CET	53	53075	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:28.535530090 CET	49627	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:28.536685944 CET	56581	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:28.553061962 CET	53	49627	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:28.554292917 CET	53	56581	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:28.814424038 CET	55184	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:28.832180977 CET	53	55184	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:28.850555897 CET	59415	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:28.867937088 CET	53	59415	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:29.803153992 CET	51029	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:29.805111885 CET	61221	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:29.823287964 CET	53	61221	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:29.849996090 CET	53683	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:29.851181030 CET	61057	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:29.853570938 CET	60797	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:29.868901968 CET	53	53683	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:29.874939919 CET	53	60797	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:30.087975025 CET	49566	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:30.972330093 CET	63916	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:30.973687887 CET	61371	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:30.987922907 CET	62000	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:31.003066063 CET	53	61371	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:31.017127991 CET	53	62000	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:31.023927927 CET	53	63916	1.1.1.1	192.168.2.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 1, 2023 19:37:52.302956104 CET	50664	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:52.304375887 CET	62535	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:37:52.321763039 CET	53	50664	1.1.1.1	192.168.2.2
Mar 1, 2023 19:37:52.554722071 CET	53	62535	1.1.1.1	192.168.2.2
Mar 1, 2023 19:38:09.263935089 CET	64510	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:38:09.281991959 CET	53	64510	1.1.1.1	192.168.2.2
Mar 1, 2023 19:38:09.284117937 CET	52118	53	192.168.2.2	1.1.1.1
Mar 1, 2023 19:38:09.301785946 CET	53	52118	1.1.1.1	192.168.2.2

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 1, 2023 19:36:06.082439899 CET	192.168.2.2	1.1.1.1	0xaacb	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:06.095560074 CET	192.168.2.2	1.1.1.1	0x6349	Standard query (0)	go2.israelandafrica.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:06.096482038 CET	192.168.2.2	1.1.1.1	0x7eb3	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:06.951627970 CET	192.168.2.2	1.1.1.1	0x8ff6	Standard query (0)	curatebio.userhbmyi.msblogger.com.au	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:08.421493053 CET	192.168.2.2	1.1.1.1	0x70b2	Standard query (0)	pretoeadvogadosassociados.adv.br	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.157824993 CET	192.168.2.2	1.1.1.1	0xd57e	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.183778048 CET	192.168.2.2	1.1.1.1	0x5cdd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.604764938 CET	192.168.2.2	1.1.1.1	0xd350	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.883450031 CET	192.168.2.2	1.1.1.1	0xb579	Standard query (0)	luvtimwrtytrinity.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:19.916965961 CET	192.168.2.2	1.1.1.1	0xd113	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:07.577893019 CET	192.168.2.2	1.1.1.1	0xc832	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:09.208617926 CET	192.168.2.2	1.1.1.1	0xfd4c	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:09.234946012 CET	192.168.2.2	1.1.1.1	0xe814	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:21.131221056 CET	192.168.2.2	1.1.1.1	0xa320	Standard query (0)	c2.elitesoldiers.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:21.670815945 CET	192.168.2.2	1.1.1.1	0x362e	Standard query (0)	c2.elitesoldiers.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:22.211211920 CET	192.168.2.2	1.1.1.1	0x1ca5	Standard query (0)	www.buydomains.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.316659927 CET	192.168.2.2	1.1.1.1	0x970f	Standard query (0)	apps.mypurecloud.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.342228889 CET	192.168.2.2	1.1.1.1	0xf77a	Standard query (0)	apps.mypurecloud.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.810709000 CET	192.168.2.2	1.1.1.1	0xe8bb	Standard query (0)	static.buydomains.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:25.603523970 CET	192.168.2.2	1.1.1.1	0xab9	Standard query (0)	api.buydomains.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:25.925262928 CET	192.168.2.2	1.1.1.1	0xb92c	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.120826960 CET	192.168.2.2	1.1.1.1	0xa4e2	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.526747942 CET	192.168.2.2	1.1.1.1	0x80bd	Standard query (0)	s1731649222.t.eloqua.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.815079927 CET	192.168.2.2	1.1.1.1	0x55	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.533356905 CET	192.168.2.2	1.1.1.1	0x68b4	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.631872892 CET	192.168.2.2	1.1.1.1	0x1ff1	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.631872892 CET	192.168.2.2	1.1.1.1	0x4141	Standard query (0)	6928088.fls.doubleclick.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 1, 2023 19:37:27.640275002 CET	192.168.2.2	1.1.1.1	0xd65b	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.642138958 CET	192.168.2.2	1.1.1.1	0x7e24	Standard query (0)	d.impactradius-event.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.678494930 CET	192.168.2.2	1.1.1.1	0x5bff	Standard query (0)	se.monetate.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.731709003 CET	192.168.2.2	1.1.1.1	0xc896	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.535530090 CET	192.168.2.2	1.1.1.1	0xcb2b	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.536685944 CET	192.168.2.2	1.1.1.1	0x3db3	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.814424038 CET	192.168.2.2	1.1.1.1	0x5a53	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.850555897 CET	192.168.2.2	1.1.1.1	0x6b65	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.803153992 CET	192.168.2.2	1.1.1.1	0xc807	Standard query (0)	sb.monetate.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.805111885 CET	192.168.2.2	1.1.1.1	0xa8b2	Standard query (0)	d.monetate.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.849996090 CET	192.168.2.2	1.1.1.1	0x6050	Standard query (0)	vmss.boldchat.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.851181030 CET	192.168.2.2	1.1.1.1	0x722f	Standard query (0)	wsmcdn.audioeye.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.853570938 CET	192.168.2.2	1.1.1.1	0xd7c9	Standard query (0)	d.monetate.net	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:30.087975025 CET	192.168.2.2	1.1.1.1	0xa5a8	Standard query (0)	wsv3cdn.audioeye.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:30.972330093 CET	192.168.2.2	1.1.1.1	0x2594	Standard query (0)	vms.boldchat.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:30.973687887 CET	192.168.2.2	1.1.1.1	0x10c1	Standard query (0)	visitor-services.boldchat.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:30.987922907 CET	192.168.2.2	1.1.1.1	0x164	Standard query (0)	analytics.audioeye.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:52.302956104 CET	192.168.2.2	1.1.1.1	0xa83c	Standard query (0)	privacyportal.onetrust.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:52.304375887 CET	192.168.2.2	1.1.1.1	0x525	Standard query (0)	c2.elitesoldiers.org	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:38:09.263935089 CET	192.168.2.2	1.1.1.1	0x4e04	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:38:09.284117937 CET	192.168.2.2	1.1.1.1	0x8140	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 1, 2023 19:36:06.100294113 CET	1.1.1.1	192.168.2.2	0xaacb	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:36:06.100294113 CET	1.1.1.1	192.168.2.2	0xaacb	No error (0)	clients.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:06.113775969 CET	1.1.1.1	192.168.2.2	0x7eb3	No error (0)	accounts.google.com		216.58.212.141	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:06.247781038 CET	1.1.1.1	192.168.2.2	0x6349	No error (0)	go2.israelandafrica.com	c2.elitesoldiers.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:36:06.247781038 CET	1.1.1.1	192.168.2.2	0x6349	No error (0)	c2.elitesoldiers.org		194.87.151.158	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:07.593990088 CET	1.1.1.1	192.168.2.2	0x8ff6	No error (0)	curatebio.userhbmyi.msblogger.com.au		192.185.192.12	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:08.787774086 CET	1.1.1.1	192.168.2.2	0x70b2	No error (0)	pretoeadvogadosassociados.adv.br		216.172.172.189	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 1, 2023 19:36:09.175993919 CET	1.1.1.1	192.168.2.2	0xd57e	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.201761007 CET	1.1.1.1	192.168.2.2	0x5cdd	No error (0)	www.google.com		172.217.18.100	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:09.622514009 CET	1.1.1.1	192.168.2.2	0xd350	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:36:09.938874960 CET	1.1.1.1	192.168.2.2	0xb579	No error (0)	luvtimwrtytrinity.com		64.225.112.96	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:19.934791088 CET	1.1.1.1	192.168.2.2	0xd113	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:19.934791088 CET	1.1.1.1	192.168.2.2	0xd113	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:19.991708994 CET	1.1.1.1	192.168.2.2	0xdba0	No error (0)	shed.dual-low.part-0017.t-0009.fdv2-t-msedge.net	part-0017.t-0009.fdv2-t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:36:19.991708994 CET	1.1.1.1	192.168.2.2	0xdba0	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.237.45	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:36:19.991708994 CET	1.1.1.1	192.168.2.2	0xdba0	No error (0)	part-0017.t-0009.fdv2-t-msedge.net		13.107.238.45	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:07.595545053 CET	1.1.1.1	192.168.2.2	0xc832	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:07.595545053 CET	1.1.1.1	192.168.2.2	0xc832	No error (0)	plus.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:09.226696014 CET	1.1.1.1	192.168.2.2	0xfd4c	No error (0)	www.google.com		142.250.186.132	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:09.252573967 CET	1.1.1.1	192.168.2.2	0xe814	No error (0)	www.google.com		142.250.181.228	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:21.331682920 CET	1.1.1.1	192.168.2.2	0xa320	No error (0)	c2.elitesoldiers.com		207.148.248.143	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:21.937639952 CET	1.1.1.1	192.168.2.2	0x362e	No error (0)	c2.elitesoldiers.com		207.148.248.143	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:22.229751110 CET	1.1.1.1	192.168.2.2	0x1ca5	No error (0)	www.buydomains.com		207.148.248.132	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.334558010 CET	1.1.1.1	192.168.2.2	0x970f	No error (0)	apps.mypurecloud.com	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:23.334558010 CET	1.1.1.1	192.168.2.2	0x970f	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		52.204.155.250	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.334558010 CET	1.1.1.1	192.168.2.2	0x970f	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		174.129.175.90	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.334558010 CET	1.1.1.1	192.168.2.2	0x970f	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		54.196.220.56	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 1, 2023 19:37:23.560102940 CET	1.1.1.1	192.168.2.2	0xf77a	No error (0)	apps.mypurecloud.com	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:23.560102940 CET	1.1.1.1	192.168.2.2	0xf77a	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		52.204.155.250	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.560102940 CET	1.1.1.1	192.168.2.2	0xf77a	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		174.129.175.90	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.560102940 CET	1.1.1.1	192.168.2.2	0xf77a	No error (0)	nginx-alb-routed-321992225.us-east-1.elb.amazonaws.com		54.196.220.56	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.887655020 CET	1.1.1.1	192.168.2.2	0xe8bb	No error (0)	static.buydomains.com	d1pux066p3zvi3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:23.887655020 CET	1.1.1.1	192.168.2.2	0xe8bb	No error (0)	d1pux066p3zvi3.cloudfront.net		13.32.99.51	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.887655020 CET	1.1.1.1	192.168.2.2	0xe8bb	No error (0)	d1pux066p3zvi3.cloudfront.net		13.32.99.28	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.887655020 CET	1.1.1.1	192.168.2.2	0xe8bb	No error (0)	d1pux066p3zvi3.cloudfront.net		13.32.99.21	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:23.887655020 CET	1.1.1.1	192.168.2.2	0xe8bb	No error (0)	d1pux066p3zvi3.cloudfront.net		13.32.99.99	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:25.629709005 CET	1.1.1.1	192.168.2.2	0xab9	No error (0)	api.buydomains.com		207.148.248.128	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:25.942883968 CET	1.1.1.1	192.168.2.2	0xb92c	No error (0)	cdn.cookielaw.org		104.19.188.97	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:25.942883968 CET	1.1.1.1	192.168.2.2	0xb92c	No error (0)	cdn.cookielaw.org		104.19.187.97	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.138643980 CET	1.1.1.1	192.168.2.2	0xa4e2	No error (0)	accounts.google.com		142.250.181.237	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.580171108 CET	1.1.1.1	192.168.2.2	0x80bd	No error (0)	s1731649222.t.eloqua.com	p01g.t.eloqua.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:26.580171108 CET	1.1.1.1	192.168.2.2	0x80bd	No error (0)	p01g.t.eloqua.com		142.0.173.27	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.832638979 CET	1.1.1.1	192.168.2.2	0x55	No error (0)	geolocation.onetrust.com		172.64.144.98	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:26.832638979 CET	1.1.1.1	192.168.2.2	0x55	No error (0)	geolocation.onetrust.com		104.18.43.158	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.550825119 CET	1.1.1.1	192.168.2.2	0x68b4	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:27.550825119 CET	1.1.1.1	192.168.2.2	0x68b4	No error (0)	static-cdn.hotjar.com		18.66.97.37	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.550825119 CET	1.1.1.1	192.168.2.2	0x68b4	No error (0)	static-cdn.hotjar.com		18.66.97.10	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.550825119 CET	1.1.1.1	192.168.2.2	0x68b4	No error (0)	static-cdn.hotjar.com		18.66.97.53	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 1, 2023 19:37:27.550825119 CET	1.1.1.1	192.168.2.2	0x68b4	No error (0)	static-cdn.hotjar.com		18.66.97.49	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.649617910 CET	1.1.1.1	192.168.2.2	0x1ff1	No error (0)	googleads.g.doubleclick.net		142.250.181.226	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.658061981 CET	1.1.1.1	192.168.2.2	0xd65b	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:27.658061981 CET	1.1.1.1	192.168.2.2	0xd65b	No error (0)	scontent.xx.fbcdn.net		157.240.253.1	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.679244995 CET	1.1.1.1	192.168.2.2	0x4141	No error (0)	6928088.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:27.679244995 CET	1.1.1.1	192.168.2.2	0x4141	No error (0)	dart.l.doubleclick.net		172.217.18.102	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.696521044 CET	1.1.1.1	192.168.2.2	0x5bff	No error (0)	se.monetate.net	http2.monetate.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:27.749377012 CET	1.1.1.1	192.168.2.2	0xc896	No error (0)	script.hotjar.com		18.66.147.47	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.749377012 CET	1.1.1.1	192.168.2.2	0xc896	No error (0)	script.hotjar.com		18.66.147.108	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.749377012 CET	1.1.1.1	192.168.2.2	0xc896	No error (0)	script.hotjar.com		18.66.147.62	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.749377012 CET	1.1.1.1	192.168.2.2	0xc896	No error (0)	script.hotjar.com		18.66.147.7	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:27.884152889 CET	1.1.1.1	192.168.2.2	0x7e24	No error (0)	d.impactradius-event.com		35.186.249.72	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.553061962 CET	1.1.1.1	192.168.2.2	0xcb2b	No error (0)	insight.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.553061962 CET	1.1.1.1	192.168.2.2	0xcb2b	No error (0)	insight.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.553061962 CET	1.1.1.1	192.168.2.2	0xcb2b	No error (0)	insight.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.553061962 CET	1.1.1.1	192.168.2.2	0xcb2b	No error (0)	insight.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.554292917 CET	1.1.1.1	192.168.2.2	0x3db3	No error (0)	adservice.google.com		142.250.181.226	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.832180977 CET	1.1.1.1	192.168.2.2	0x5a53	No error (0)	stats.g.doubleclick.net		66.102.1.154	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.832180977 CET	1.1.1.1	192.168.2.2	0x5a53	No error (0)	stats.g.doubleclick.net		66.102.1.157	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.832180977 CET	1.1.1.1	192.168.2.2	0x5a53	No error (0)	stats.g.doubleclick.net		66.102.1.156	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.832180977 CET	1.1.1.1	192.168.2.2	0x5a53	No error (0)	stats.g.doubleclick.net		66.102.1.155	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:28.867937088 CET	1.1.1.1	192.168.2.2	0x6b65	No error (0)	www.google.ch		142.250.185.195	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.822460890 CET	1.1.1.1	192.168.2.2	0xc807	No error (0)	sb.monetate.net	http2.monetate.edgekey.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.823287964 CET	1.1.1.1	192.168.2.2	0xa8b2	No error (0)	d.monetate.net	d.monetate-prod.zone		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.823287964 CET	1.1.1.1	192.168.2.2	0xa8b2	No error (0)	d.monetate-prod.zone		54.161.222.185	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 1, 2023 19:37:29.823287964 CET	1.1.1.1	192.168.2.2	0xa8b2	No error (0)	d.monetate-prod.zone		54.165.48.193	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.823287964 CET	1.1.1.1	192.168.2.2	0xa8b2	No error (0)	d.monetate-prod.zone		3.86.126.62	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	vmss.boldchat.com	rpc.boldchat.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc.boldchat.com	rpc-dc19.bold360.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		52.41.47.191	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		44.226.244.84	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		52.13.124.118	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		54.200.230.213	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		54.200.68.184	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		44.242.45.116	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		54.188.53.58	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.868901968 CET	1.1.1.1	192.168.2.2	0x6050	No error (0)	rpc-dc19.bold360.com		54.69.177.37	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.870781898 CET	1.1.1.1	192.168.2.2	0x722f	No error (0)	wsmcdn.audioeye.com	wsmcdn.audioeye.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.874939919 CET	1.1.1.1	192.168.2.2	0xd7c9	No error (0)	d.monetate.net	d.monetate-prod.zone		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:29.874939919 CET	1.1.1.1	192.168.2.2	0xd7c9	No error (0)	d.monetate-prod.zone		54.161.222.185	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.874939919 CET	1.1.1.1	192.168.2.2	0xd7c9	No error (0)	d.monetate-prod.zone		54.165.48.193	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:29.874939919 CET	1.1.1.1	192.168.2.2	0xd7c9	No error (0)	d.monetate-prod.zone		3.86.126.62	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:30.107950926 CET	1.1.1.1	192.168.2.2	0xa5a8	No error (0)	wsv3cdn.audioeye.com	wsv3cdn.audioeye.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:31.003066063 CET	1.1.1.1	192.168.2.2	0x10c1	No error (0)	visitor-services.boldchat.com	visitor-services.bold360.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:31.003066063 CET	1.1.1.1	192.168.2.2	0x10c1	No error (0)	visitor-services.bold360.com		18.157.190.196	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.003066063 CET	1.1.1.1	192.168.2.2	0x10c1	No error (0)	visitor-services.bold360.com		35.156.91.37	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.017127991 CET	1.1.1.1	192.168.2.2	0x164	No error (0)	analytics.audioeye.com		44.239.25.130	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.017127991 CET	1.1.1.1	192.168.2.2	0x164	No error (0)	analytics.audioeye.com		52.41.227.209	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.017127991 CET	1.1.1.1	192.168.2.2	0x164	No error (0)	analytics.audioeye.com		44.240.164.89	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	vms.boldchat.com	rpc.boldchat.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc.boldchat.com	rpc-dc19.bold360.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		54.200.68.184	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		44.237.13.169	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		52.13.124.118	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		44.242.45.116	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		44.230.126.250	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		44.230.250.92	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		44.238.219.222	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:31.023927927 CET	1.1.1.1	192.168.2.2	0x2594	No error (0)	rpc-dc19.bold360.com		54.200.230.213	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:52.321763039 CET	1.1.1.1	192.168.2.2	0xa83c	No error (0)	privacyportal.onetrust.com		104.18.43.158	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:52.321763039 CET	1.1.1.1	192.168.2.2	0xa83c	No error (0)	privacyportal.onetrust.com		172.64.144.98	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:37:52.554722071 CET	1.1.1.1	192.168.2.2	0x525	No error (0)	c2.elitesoldiers.org		194.87.151.158	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:38:09.281991959 CET	1.1.1.1	192.168.2.2	0x4e04	No error (0)	www.google.com		142.250.181.228	A (IP address)	IN (0x0001)	false
Mar 1, 2023 19:38:09.301785946 CET	1.1.1.1	192.168.2.2	0x8140	No error (0)	www.google.com		142.250.184.196	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- go2.israelandafrica.com
- curatebio.userhbmyi.msblogger.com.au
  - pretoeadvogadosassociados.adv.br
- https:
  - luvtimwrtytrinity.com
  - cdnjs.cloudflare.com
  - aadcdn.msauth.net
  - www.buydomains.com
  - static.buydomains.com
  - www.google.com
  - apps.mypurecloud.com
  - cdn.cookielaw.org
  - api.buydomains.com
  - geolocation.onetrust.com
  - s1731649222.t.eloqua.com
  - static.hotjar.com
  - connect.facebook.net
  - 6928088.fls.doubleclick.net
  - script.hotjar.com
  - googleads.g.doubleclick.net
  - d.impactradius-event.com
  - adservice.google.com
  - insight.adsrvr.org
  - stats.g.doubleclick.net
  - vmss.boldchat.com
  - d.monetate.net
  - visitor-services.boldchat.com
  - vms.boldchat.com
  - analytics.audioeye.com
  - privacyportal.onetrust.com
  - c2.elitesoldiers.org
- c2.elitesoldiers.com

Chrome Debug Log

[3128:5648:0301/193610.682:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193614.633:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193619.583:INFO:CONSOLE(1)] "A parser-blocking, cross site (i.e. different eTLD+1) script, https://code.jquery.com/jquery-3.1.1.min.js, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.", source: https://pretoeadvogadosassociados.adv.br/gert/gert.html (1)

[3128:5648:0301/193619.583:INFO:CONSOLE(1)] "A parser-blocking, cross site (i.e. different eTLD+1) script, https://code.jquery.com/jquery-3.1.1.min.js, is invoked via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.", source: https://pretoeadvogadosassociados.adv.br/gert/gert.html (1)

[3128:5648:0301/193621.584:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193707.633:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193707.633:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193723.533:INFO:CONSOLE(2)] "Cloudfront Cache: version=2023-02-09-1", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (2)

[3128:5648:0301/193725.132:INFO:CONSOLE(133)] "HOST: www-03.prod", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (133)

[3128:5648:0301/193726.433:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193727.183:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193727.333:INFO:CONSOLE(1)] "this is not a sf_cart_link", source: (1)

[3128:5648:0301/193727.383:INFO:CONSOLE(390)] "Your client application uses libraries for user authentication or authorization that will soon be deprecated. See the [Migration Guide](https://developers.google.com/identity/gsi/web/guides/gis-migration) for more information.", source: https://apis.google.com/_/scs/abc-static/_/js/k=gapi.lb.en.Oupypiulh58.O/m=client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_CVmSAWqMsGCHgMRyaSvlE8hY6sw/cb=gapi.loaded_0?le=scs (390)

[3128:5648:0301/193727.433:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193727.683:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193727.832:INFO:CONSOLE(0)] "Access to font at 'https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-700.woff2' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193728.334:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193728.334:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193728.683:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/favicon.ico?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193728.683:INFO:CONSOLE(0)] "Access to font at 'https://apps.mypurecloud.com/webfonts/fonts/roboto-v29-latin-regular.woff2' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193728.683:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193728.733:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193728.783:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/tdfs/logo-custom.svg?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193728.783:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/selectArrowGrey.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193728.783:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/checkmark-blue.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193729.083:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193729.483:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/logo_48.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C&co=aHR0cHM6Ly93d3cuYnV5ZG9tYWlucy5jb206NDQz&hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&size=invisible&badge=inline&cb=y189nut6t10x (0)

[3128:5648:0301/193729.933:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193729.933:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193729.933:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193729.983:INFO:CONSOLE(1)] "Deployed Version: [2003] -> /var/lib/jenkins/product-tarballs/BuyDomainsWWW/2003.tgz .

[3128:5648:0301/193730.033:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193730.083:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/favicon.ico?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193730.133:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/tdfs/logo-custom.svg?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193730.133:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/selectArrowGrey.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193730.133:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/checkmark-blue.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193730.333:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193730.333:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193730.633:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/refresh_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193730.633:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/audio_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193730.633:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/info_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193730.633:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/image_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193731.033:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/undo_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193731.833:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193731.983:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

[3128:5648:0301/193732.083:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193733.083:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/logo_48.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C&co=aHR0cHM6Ly93d3cuYnV5ZG9tYWlucy5jb206NDQz&hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&size=invisible&badge=inline&cb=y189nut6t10x (0)

[3128:5648:0301/193733.133:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193734.383:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193734.583:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/favicon.ico?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193734.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/tdfs/logo-custom.svg?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193734.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/selectArrowGrey.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193734.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/checkmark-blue.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193734.783:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193735.133:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/refresh_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193735.133:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/audio_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193735.133:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/info_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193735.232:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/image_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193735.283:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/undo_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193735.283:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193736.583:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193738.133:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/logo_48.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C&co=aHR0cHM6Ly93d3cuYnV5ZG9tYWlucy5jb206NDQz&hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&size=invisible&badge=inline&cb=y189nut6t10x (0)

[3128:5648:0301/193738.183:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193739.583:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/favicon.ico?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193739.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com//browser/img/tdfs/logo-custom.svg?version=2023-02-09-1' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193739.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/selectArrowGrey.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193739.633:INFO:CONSOLE(0)] "Access to image at 'https://static.buydomains.com/browser/img/icons/checkmark-blue.svg' from origin 'https://www.buydomains.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.buydomains.com/lander/elitesoldiers.com?domain=elitesoldiers.com&utm_source=elitesoldiers.com&utm_medium=click&utm_campaign=tdfs-AprTest&traffic_id=AprTest&traffic_type=tdfs&redirect=ono-redirect (0)

[3128:5648:0301/193739.733:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193739.832:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193740.083:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/refresh_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193740.083:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/audio_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193740.083:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/info_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193740.183:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/image_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193740.283:INFO:CONSOLE(0)] "Access to image at 'https://www.gstatic.com/recaptcha/api2/undo_2x.png' from origin 'https://www.google.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.", source: https://www.google.com/recaptcha/api2/bframe?hl=en&v=Nh10qRQB5k2ucc5SCBLAQ4nA&k=6LcqAIkUAAAAAHjOK9ZepI7IU55yYRmOEigfrp6C (0)

[3128:5648:0301/193740.283:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193741.633:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193752.733:INFO:CONSOLE(169)] "Loaded", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (169)

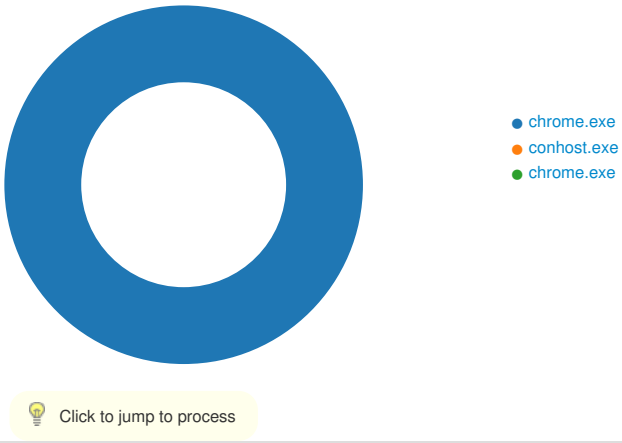
[3128:5648:0301/193753.132:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193757.633:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

[3128:5648:0301/193802.633:INFO:CONSOLE(49)] "Got source", source: chrome-extension://gdaefkejpgkiemlaofpalmlakkmbjdnl/scripts/extension/backgroundV3.js (49)

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3128, Parent PID: 1124

General

Target ID:	0
Start time:	19:36:01
Start date:	01/03/2023
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://go2.israelandafrica.com/f/a/y5H0bDO4woHaMQouJjYlOfq~~/OMbOowf~/aHR0cDovL0N1cmF0ZWJpby5VU0VSaEJNWUkubXNibG9nZ2VyLmNvbS5hdS9qYXNvbi53YWxzaEBjdXJhdGViaW8uY29t
Imagebase:	0x7ff6e5430000
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	7FF6E54888A3	RegSetValueExW

Analysis Process: conhost.exe PID: **1288**, Parent PID: **3128**

General

Target ID:	1
Start time:	19:36:02
Start date:	01/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff69a190000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6140**, Parent PID: **3128**

General

Target ID:	2
Start time:	19:36:03
Start date:	01/03/2023
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=2104 --field-trial-handle=1824,i,3608302658647549143,7935353812338714585,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6e5430000
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

Disassembly

No disassembly