ID: 736961
Cookbook: browseurl.jbs
Time: 12:34:25
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report
http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 8
World Map of Contacted IPs 11
Public IPs 12
Private 13
General Information 13
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 14
Network Behavior 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: chrome.exePID: 5832, Parent PID: 4896 15
General 15
File Activities 15
Registry Activities 15
Analysis Process: chrome.exePID: 6048, Parent PID: 5832 15
General 15
File Activities 16
Analysis Process: chrome.exePID: 6136, Parent PID: 4896 16
General 16
Registry Activities 16
Disassembly 16

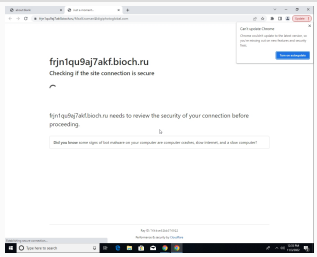
Windows Analysis Report

http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1...

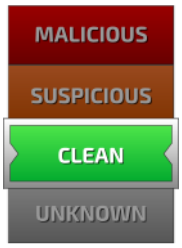
Overview

General Information

Sample URL:	484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9o...XNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2WW1Gc0xtTnZiUT09
Analysis ID:	736961
Infos:	



Detection

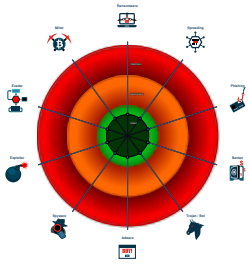


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5832 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6048 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=1980 --field-trial-handle=1816,i,2919350836162336761,13592327512595919683,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 6136 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2WW1Gc0xtTnZiUT09 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

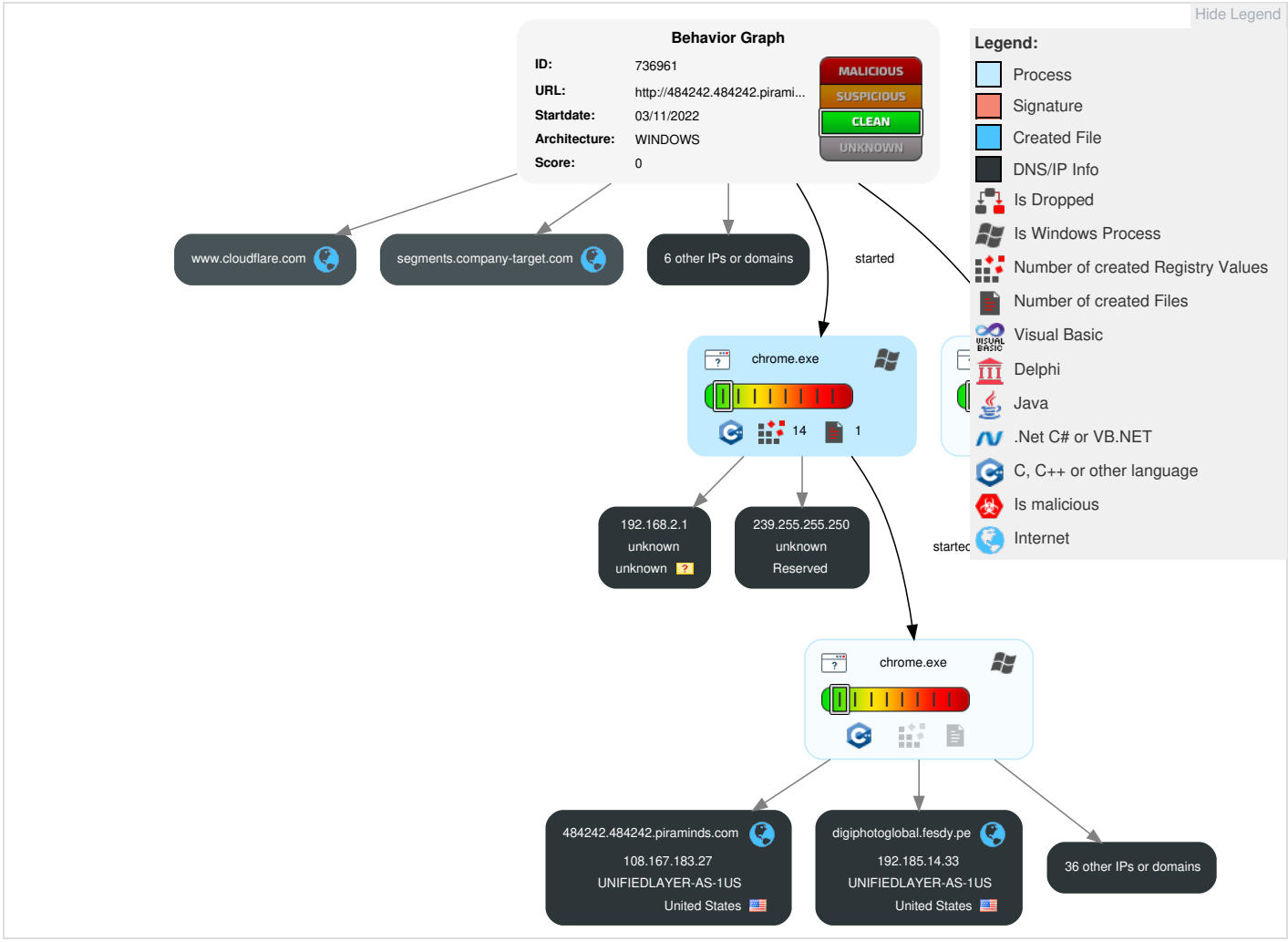
Joe Sandbox Signatures

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

Mitre Att&ck Matrix

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

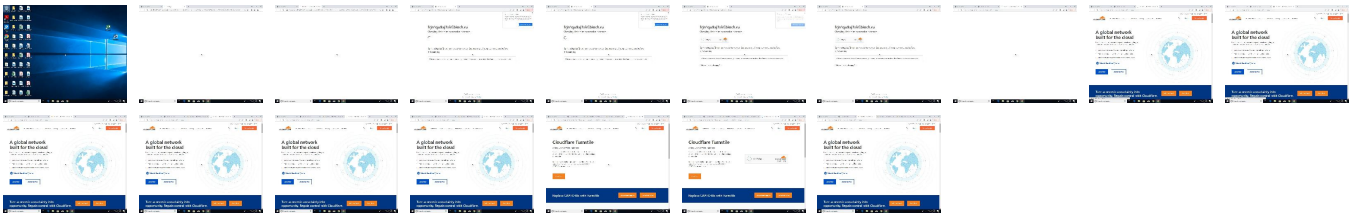
Behavior Graph

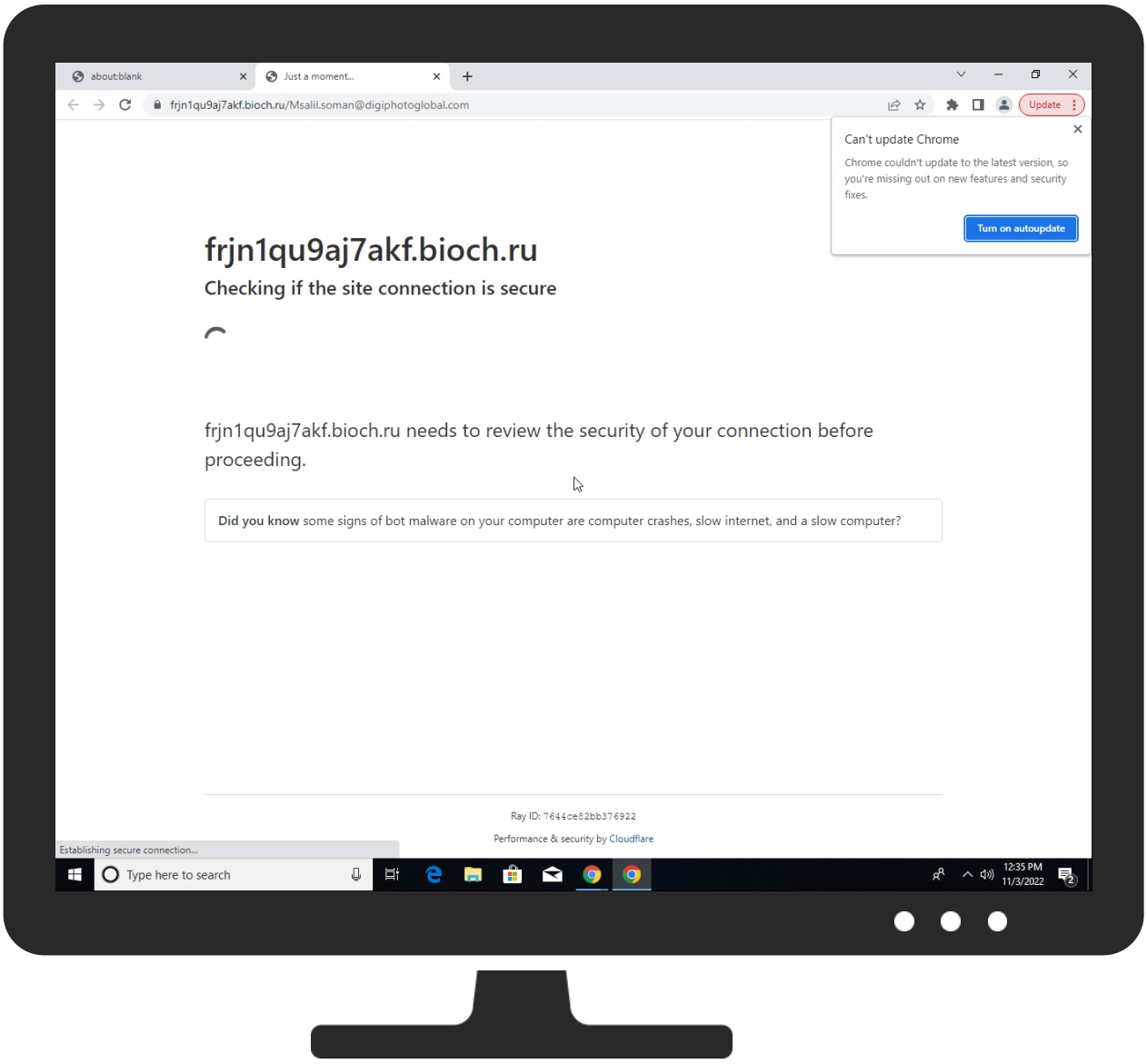


Screenshots

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://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2WW1Gc0xtTnZiUT09	1%	Virustotal		Browse
http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2WW1Gc0xtTnZiUT09	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://match.prod.bidr.io/cookie-sync/demandbase?_bee_ppp=1	0%	URL Reputation	safe	
http://https://match.prod.bidr.io/cookie-sync/demandbase	0%	URL Reputation	safe	
http://https://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8	0%	URL Reputation	safe	
http://https://713-xsc-918.mktoresp.com/webevents/visitWebPage?_mchNc=1667504180881&_mchCn=&_mchId=713-XSC-918&_mchTk=_mch-cloudflare.com-1667504180879-97994&_mchHo=www.cloudflare.com&_mchPo=&_mchRu=%2F&_mchPc=https%3A&_mchVr=162&_mchEcid=&_mchHa=&_mchRe=&_mchQp=utm_source%3Dchallenge__-__utm_campaign%3Dm	0%	Avira URL Cloud	safe	
http://https://adservice.google.co.uk/ddm/fls/p/dc_pre=CJz-7On1kfsCFZiVmwod4FwO0A;src=9309168;type=adh_o0;cat=adh_g0;ord=4509911983999;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A11;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=undefined;~oref=https://www.cloudflare.com/	0%	Avira URL Cloud	safe	
http://https://api.company-target.com/api/v2/ip.json?referrer=&page=https%3A%2F%2Fwww.cloudflare.com%2Fen-gb%2Fproducts%2Fturnstile%2F%3Futm_source%3Dturnstile%26utm_campaign%3Dwidget&page_title=Cloudflare%20Turnstile%2C%20a%20free%20CAPTCHA%20replacement%20%7C%20Cloudflare	0%	Avira URL Cloud	safe	
http://https://713-xsc-918.mktoresp.com/webevents/visitWebPage?_mchNc=1667504200295&_mchCn=&_mchId=713-XSC-918&_mchTk=_mch-cloudflare.com-1667504180879-97994&_mchHo=www.cloudflare.com&_mchPo=&_mchRu=%2Fen-gb%2Fproducts%2Fturnstile%2F&_mchPc=https%3A&_mchVr=162&_mchEcid=&_mchHa=&_mchRe=&_mchQp=utm_source%3Dturnstile__-__utm_campaign%3Dwidget	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/favicon.ico	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7644ce82bb376922	0%	Avira URL Cloud	safe	
http://digiphotoglobal.fesdy.pe/html/	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/img/7644ce82bb376922/1667475329326/DxNlck9TWz50FZA	0%	Avira URL Cloud	safe	
http://https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe946216663173699993	0%	Avira URL Cloud	safe	
http://https://segments.company-target.com/log?vendor=choca&user_id=AAEn-k7Gx1AAACD4_0321w	0%	Avira URL Cloud	safe	
http://https://segments.company-target.com/validateCookie?vendor=choca&user_id=AAEn-k7Gx1AAACD4_0321w&verifyHash=47413aef4791e2c8c095d8f2f0fc0c5a33d7a8f8	0%	Avira URL Cloud	safe	
http://https://api.company-target.com/api/v2/ip.json?referrer=&page=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm&page_title=Cloudflare%20-%20The%20Web%20Performance%20%26%20Security%20Company%20%7C%20Cloudflare	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/styles/challenges.css	0%	Avira URL Cloud	safe	
http://digiphotoglobal.fesdy.pe/html	0%	Avira URL Cloud	safe	
http://https://segments.company-target.com/validateCookie?vendor=choca&user_id=AAGWck7Gx08AACFLtnVIaQ&verifyHash=3ced7b9a71d5d7f145fc832a6100b1ec6ce78301	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/pat/7644ce82bb376922/1667475329324/3b4e8252d3d82181a2c4ddc71259a96c4a752369b3bd03252bd73f618b82ae7d/clwre8ykeajALTC	0%	Avira URL Cloud	safe	
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=7644ce82bb376922	0%	Avira URL Cloud	safe	
http://https://segments.company-target.com/log?vendor=choca&user_id=AAGWck7Gx08AACFLtnVIaQ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
static.cloudflareinsights.com	104.16.57.101	true	false		unknown
tr.www.cloudflare.com	104.16.124.96	true	false		high
segments.company-target.com	52.222.191.11	true	false		unknown
adservice.google.com	142.251.143.98	true	false		high
stats.g.doubleclick.net	142.250.153.156	true	false		high
tag.demandbase.com	52.85.92.7	true	false		high
adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com	63.32.183.38	true	false		high
performance.radar.cloudflare.com	104.18.31.78	true	false		high
www.google.com	142.251.143.132	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
484242.484242.piraminds.com	108.167.183.27	true	false		unknown
frjn1qu9aj7akf.bioch.ru	188.114.96.3	true	false		unknown
match.prod.bidr.io	54.229.166.11	true	false		unknown
pagead46.l.doubleclick.net	142.251.143.98	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
digiphotoglobal.fesdy.pe	192.185.14.33	true	false		unknown
accounts.google.com	142.251.143.141	true	false		high
dual-a-0001.a-msedge.net	204.79.197.200	true	false		unknown
ad.doubleclick.net	142.251.143.134	true	false		high
cloudflare.hcaptcha.com	104.18.19.132	true	false		unknown
www.googleoptimize.com	142.251.143.142	true	false		unknown
www.cloudflare.com	104.16.123.96	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
challenges.cloudflare.com	104.18.6.185	true	false		high
www.google.co.uk	142.251.143.99	true	false		unknown
api.company-target.com	54.230.206.114	true	false		unknown
clients.l.google.com	142.251.143.174	true	false		high
713-xsc-918.mktoresp.com	192.28.144.124	true	false		unknown
digiphotoglobal.com	104.18.2.24	true	false		unknown
alb.reddit.com	unknown	unknown	false		high
d.adroll.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
munchkin.marketo.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/?utm_source=challenge&utm_campaign=m	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/orchestrate/chl_api/v1?ray=7644ce9c6e578fdd	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/img/7644ce9c6e578fdd/1667475333476/rc2rUmmE6n-7BY8	false		high
http://https://www.cloudflare.com/static/778263f53a53630a857a9290654bdb6f/turnstile_gif.gif	false		high
http://https://www.cloudflare.com/static/e45e66a9871bd16f924c89eba16b1b57/cloudflare-pages-blue.svg	false		high
http://https://www.cloudflare.com/static/9ec514a3b8b51dfe57543cc0424e127e/security-api-web-apps-spot-illustration.svg	false		high
http://https://frjn1qu9aj7akf.bioch.ru/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://ad.doubleclick.net/activity;src=9309168;type=adh_o0;cat=adh_g0;ord=4509911983999;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A11;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=undefined?	false		high
http://https://www.cloudflare.com/?utm_source=challenge&utm_campaign=m	false		high
http://https://id.rlcdn.com/464526.gif	false		high
http://https://www.cloudflare.com/static/b067ac772150e57a54e7a1aa0f018c72/cloudflare-browser-blue.svg	false		high
http://https://www.cloudflare.com/page-data/en-gb/products/turnstile/page-data.json	false		high
http://https://adservice.google.co.uk/ddm/fls/p/dc_pre=CJz-7On1kfsCFZiVmwod4FwO0A;src=9309168;type=adh_o0;cat=adh_g0;ord=4509911983999;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A11;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=undefined;~oref=https://www.cloudflare.com/	false	• Avira URL Cloud: safe	unknown
http://https://api.company-target.com/api/v2/ip.json?referrer=&page=https%3A%2F%2Fwww.cloudflare.com%2Fen-gb%2Fproducts%2Fturnstile%2F%3Futm_source%3Dturnstile%26utm_campaign%3Dwidget&page_title=Cloudflare%20Turnstile%2C%20a%20free%20CAPTCHA%20replacement%20%7C%20Cloudflare	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/vendor/onetrust/scripttemplates/otSDKStub.js	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://tr.www.cloudflare.com/gtag/js?id=G-PHVG60J2FD&l=dataLayer&cx=c&sign=d5a9b882437b3ac13c16066909793746b80cfeb6b0588c4062210ea2efe00b76_20221103	false		high
http://https://www.cloudflare.com/page-data/index/page-data.json	false		high
http://https://www.cloudflare.com/commons-7a405212b282de3f8e6f.js	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/pat/7644ce9c6e578fdd/1667475333477/f70c782704a49e50c9e9cbb533b881fb40963c6d84a7e462b38153bf682f7f45/6DhiGC_ed1XnpJ1	false		high
http://https://ad.doubleclick.net/activity;dc_pre=CPLay_f1kfsCFe3JOwId7wMPtA;src=9309168;type=adh_o0;cat=adh_g0;ord=2038357168494;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A40;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2Fen-gb%2Fproducts%2Fturnstile%2F%3Futm_source%3Dturnstile%26utm_campaign%3Dwidget;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=1796770398.1667504172?	false		high
http://https://www.cloudflare.com/page-data/sq/d/809133105.json	false		high
http://https://www.cloudflare.com/static/8bba4c4f12798edd31b6f2b8e600246e/internet-globe-blue.svg	false		high
http://https://713-xsc-918.mktoresp.com/webevents/visitWebPage?_mchNc=1667504200295&_mchCn=&_mchId=713-XSC-918&_mchTk=_mch-cloudflare.com-1667504180879-97994&_mchHo=www.cloudflare.com&_mchPo=&_mchRu=%2Fen-gb%2Fproducts%2Fturnstile%2F&_mchPc=https%3A&_mchVr=162&_mchEcid=&_mchHa=&_mchRe=&_mchQp=utm_source%3Dturnstile__-__utm_campaign%3Dwidget	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/6d28db3ec2ddd52c893b4bd3b26d26bc/logo_loreal_trusted-by_gray.svg	false		high
http://https://www.cloudflare.com/rvs/?u=https%3A%2F%2Fwww.cloudflare.com%2Fen-gb%2Fproducts%2Fturnstile%2F%3Futm_source%3Dturnstile%26utm_campaign%3Dwidget	false		high
http://https://frjn1qu9aj7akf.bioch.ru/Msalil.soman@digiphotoglobal.com	false		unknown
http://https://713-xsc-918.mktoresp.com/webevents/visitWebPage?_mchNc=1667504180881&_mchCn=&_mchId=713-XSC-918&_mchTk=_mch-cloudflare.com-1667504180879-97994&_mchHo=www.cloudflare.com&_mchPo=&_mchRu=%2F&_mchPc=https%3A&_mchVr=162&_mchEcid=&_mchHa=&_mchRe=&_mchQp=utm_source%3Dchallenge__-__utm_campaign%3Dm	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/page-data/sq/d/3934964512.json	false		high
http://https://www.cloudflare.com/cdn-cgi/zaraz/s.js?z=JTdCJTIyZXhlY3V0ZWQlMjIlM0ElNUIlNUQlMkMlMjJ0JTIyJTNBJTIyQ2xvdWRmbGFyZSUyMC0lMjBUaGUlMjBXZWIlMjBQZXJmb3JtYW5jZSUyMCUyNiUyMFNlY3VyaXR5JTIwQ29tcGFueSUyMCU3QyUyMENsb3VkZmxhcmUlMjIlMkMlMjJ4JTIyJTNBMC40MDgyNzA3NDM1MTk5MTY2NiUyQyUyMnclMjIlM0ExMjgwJTJDJTIyaCUyMiUzQTEwMjQlMkMlMjJqJTIyJTNBOTEzJTJDJTIyZSUyMiUzQTEyODAlMkMlMjJsJTIyJTNBJTIyaHR0cHMlM0ElMkYlMkZ3d3cuY2xvdWRmbGFyZS5jb20lMkYlM0Z1dG1fc291cmNlJTNEY2hhbGxlbmdlJTI2dXRtX2NhbXBhaWduJTNEbSUyMiUyQyUyMnIlMjIlM0ElMjIlMkMlMjJrJTIyJTNBMjQlMkMlMjJuJTIyJTNBJTIyVVRGLTglMjIlMkMlMjJvJTIyJTNBNDIwJTJDJTIycSUyMiUzQSU1QiU1RCU3RA==	false		high
http://https://stats.g.doubleclick.net/g/collect?v=2&tid=G-PHVG60J2FD&cid=1796770398.1667504172>m=2reav0&aip=1	false		high
http://https://www.cloudflare.com/en-gb/products/turnstile/?utm_source=turnstile&utm_campaign=widget	false		high
http://https://ad.doubleclick.net/activity;dc_pre=CJz-7On1kfsCFZiVmwod4FwO0A;src=9309168;type=adh_o0;cat=adh_g0;ord=4509911983999;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A11;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=undefined?	false		high
http://https://www.cloudflare.com/static/88d8a61effe6ece596ff34fc796fa7b9/end_of_road.png	false		high
http://https://tag.demandbase.com/f309084f574a9b8e.min.js	false		high
http://https://www.cloudflare.com/static/6a54ab9058dd2854c6c48ef65a6d931d/Area-1_Vendor-Email-Fraud-Icon.svg	false		high
http://https://www.cloudflare.com/static/b605eca229bbf7bc64daaae689da14ad/logo_zendesk_gray_32px-wrapper.svg	false		high
http://https://www.cloudflare.com/static/82a73aab9040a829207ef10e8859e3ef/logo_labcorp_trusted-by_gray.svg	false		high
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/orchestrate/managed/v1?ray=7644ce82bb376922	false	• Avira URL Cloud: safe	unknown
http://https://alb.reddit.com/rp.gif?id=t2_1upmecjq&event=PageVisit&ts=1667475371532&uuid=ffb754cf-ce40-4369-98c4-47a56b354747&s=%2F6C8i9X7STOQDh39eWje0g4rowozfKJwWFtgRQaPXt4%3D	false		high
http://digiphotoglobal.fesdy.pe/html/	false	• Avira URL Cloud: safe	unknown
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/g/flow/ov1/0.23651009508986148:1667474967:fi0-4-A-sC4gybQGWCySYv6nPl6_WaDVssClb3Kh0Qs/7644ce9c6e578fdd/645a2645b8a2530	false		high
http://https://www.cloudflare.com/static/f66c9352641e2d181c7d3d4f4e80c899/Test_V1.svg	false		high
http://https://match.prod.bidr.io/cookie-sync/demandbase?_bee_ppp=1	false	• URL Reputation: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://www.cloudflare.com/static/4b39f12c05140c199c0a97d48c11fb63/analytics-data.svg	false		high
http://https://tr.www.cloudflare.com/analytics.js	false		high
http://https://a.nel.cloudflare.com/report/v3?s=rKkqCaen49IaKvCBM8l3nL9pljiacbmCifS7EH98Ums6MYMe2ZY9hNq%2FU%2BwhSQcH9k6dsyE1MWQE3SRtW6LU0fXHwZxir6V3CAe2Kt53q2MGp%2B0BuHYqHqrWJBoGo02SdP6gjSfsL1SdLg%3D%3D	false		high
http://https://match.prod.bidr.io/cookie-sync/demandbase	false	• URL Reputation: safe	unknown
http://https://www.cloudflare.com/static/cfe3596a8bbbc41b827c27e457c97607/face-sad.png	false		high
http://https://frjn1qu9aj7akf.bioch.ru/Msalil.soman@digiphotoglobal.com	false		unknown
http://https://www.cloudflare.com/framework-a161050e12a4e036ba91.js	false		high
http://https://tr.www.cloudflare.com/ns.html?id=GTM-PKQFGQB	false		high
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/img/7644ce82bb376922/1667475329326/DxNlck9TWz50FZA	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/107b38103df2882b72b7d0117478f787/teams-access-hero_1.svg	false		high
http://https://www.cloudflare.com/static/9669cae57f56c6e3049faec567a9e6a7/cloudflare-access-blue.svg	false		high
http://https://www.cloudflare.com/page-data/sq/d/1869562119.json	false		high
http://https://www.googleoptimize.com/optimize.js?id=GTM-N4JSZJ8	false	• URL Reputation: safe	unknown
http://https://www.cloudflare.com/static/e4e28c9fc1e9fc6ae9cd481258b4e0f6/performance-1-blue.svg	false		high
http://https://www.cloudflare.com/static/01f0e9e70dbb5132df9a1ebc4b978b79/security-fingerprint-privacy-blue.svg	false		high
http://https://www.cloudflare.com/static/963dade74282b833006aeacef3caf511/workers-hero-illustration.svg	false		high
http://https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe94621666317369993	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/67c8dcbe189a2cf2a0a2966ba23a3da5/logo_garmin_trusted-by_gray.svg	false		high
http://https://segments.company-target.com/log?vendor=choca&user_id=AAEn-k7Gx1AAACD4_0321w	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/e1ad67500628752027 82bbb3fc19101a33b1e306-e253e64b9d4f28e16878.js	false		high
http://https://www.cloudflare.com/page-data/sq/d/2333086113.json	false		high
http://https://www.cloudflare.com/static/ff006509bb342c576c2f15bd7bee9704/logo_shopify_trusted-by_gray.svg	false		high
http://https://tr.www.cloudflare.com/g/collect?v=2&tid=G-PHVG60J2FD>m=2reav0&_p=1330291102&_gaz=1&cid=1796770398.1667504172&ul=en-us&sr=1280x1024&_fplc=0&uaa=x86&uab=64&uafvl=Chromium%3B104.0.5112.81%7C%2520Not%2520A%253BBrand%3B99.0.0.0%7CGoogle%2520Chrome%3B104.0.5112.81&uamb=0&uam=&uap=Windows&uapv=6.0.0&uaw=0&_s=1&dl=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm&dr=&sid=1667504180&sct=1&seg=0&dt=Cloudflare%20-%20The%20Web%20Performance%20%26%20Security%20Company%20%7C%20Cloudflare&en=page_view&_fv=1&_ss=1&ep.content_group=Marketing%20Site&ep.timestamp=2022-11-03T12%3A36%3A11.78-07%3A00&ep.blog_post_date=&ep.content_interest_score=&ep.gtm_container_id=GTM-PKQFGQB&upn.timezone_offset=-7&richsstsse	false		high
http://https://www.cloudflare.com/static/bc68754f416c6ace80b7ced3c1a0706a/cloudflare-gateway-blue.svg	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://www.cloudflare.com/page-data/app-data.json	false		high
http://https://www.cloudflare.com/static/8e6e17c1d426c4173db2d937aeeead9d/performance-cloud-speed-blue.svg	false		high
http://https://www.cloudflare.com/rvs/?u=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm	false		high
http://https://alb.reddit.com/rp.gif?id=t2_1upmecjq&event=PageVisit&ts=1667475400788&uuid=ffb754cf-ce40-4369-98c4-47a56b354747&s=plKct8GSOItMF%2BqYHQCqL35CP8Qw32mCeNRfA1ICbTM%3D	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/turnstile/if/ov2/av0/bm9y5/0x4AAAAAAAAjq6WYeRDKmebM/light/normal	false		high
http://https://tr.www.cloudflare.com/ns.html?id=GTM-PKQFGQB	false		high
http://https://challenges.cloudflare.com/cdn-cgi/challenge-platform/turnstile/if/ov2/av0/bm9y5/0x4AAAAAAAAjq6WYeRDKmebM/light/normal	false		high
http://https://www.cloudflare.com/vendor/onetrust/consent/e34df59b-4a48-4bf9-b2b5-7a4bb09cd231/4505fd23-3c09-44db-82b2-07a7d776e9a7/en.json	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/styles/challenges.css	false	• Avira URL Cloud: safe	unknown
http://https://segments.company-target.com/validateCookie?vendor=choca&user_id=AAEn-k7Gx1AAACD4_0321w&verifyHash=47413aef4791e2c8c095d8f2f0fc0c5a33d7a8f8	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/cdn-cgi/rum?	false		high
http://https://api.company-target.com/api/v2/ip.json?referrer=&page=https%3A%2F%2Fwww.cloudflare.com%2F%3Futm_source%3Dchallenge%26utm_campaign%3Dm&page_title=Cloudflare%20-%20The%20Web%20Performance%20%26%20Security%20Company%20%7C%20Cloudflare	false	• Avira URL Cloud: safe	unknown
http://digiphotoglobal.fesdy.pe/html	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/f9049af4fb3ca830e5bf61496a5f1024/price.svg	false		high
http://https://www.cloudflare.com/static/8700e89879f875a08b6769b1583cf270/logo_thomson-reuters_gray_32px-wrapper.svg	false		high
http://https://performance.radar.cloudflare.com/beacon.js	false		high
http://https://ad.doubleclick.net/activity;src=9309168;type=adh_o0;cat=adh_g0;ord=2038357168494;gtm=2ygav0;auiddc=1638296394.1667504171;u1=2022%20Nov%2003%2012%3A36%3A40;u2=undefined;u3=https%3A%2F%2Fwww.cloudflare.com%2Fen-gb%2Fproducts%2Fturnstile%2F%3Futm_source%3Dturnstile%26utm_campaign%3Dwidget;u4=undefined;u5=undefined;u6=undefined;u7=undefined;u8=undefined;u9=undefined;u10=undefined;u11=undefined;u12=undefined;u13=undefined;u14=undefined;u15=1796770398.1667504172?	false		high
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/challenge-platform/h/g/pat/7644ce82bb376922/1667475329324/3b4e8252d3d82181a2c4ddc71259a96c4a752369b3bd03252bd73f618b82ae7d/clwre8ykeajALTC	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/c4368286eb1a4f525b305c8f78d517d5/reliability-timer-blue.svg	false		high
http://https://www.cloudflare.com/static/576796641c4fac80ee740be449732d6d/security-lock-blue.svg	false		high
http://https://segments.company-target.com/validateCookie?vendor=choca&user_id=AAGWck7Gx08AACFLtnVIaQ&verifyHash=3ced7b9a71d5d7f145fc832a6100b1ec6ce78301	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/vendor/onetrust/scripttemplates/6.19.0/otBannerSdk.js	false		high
http://https://frjn1qu9aj7akf.bioch.ru/cdn-cgi/images/trace/managed/js/transparent.gif?ray=7644ce82bb376922	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/4e9b58043dfcabfe0fc674a018c9276d0582457d-88366e8b1f8a45ef4fa5.js	false		high
http://https://www.cloudflare.com/SearchModal-4aee96a9b82d51fa9b43.js	false		high
http://https://www.cloudflare.com/fd09011b4bd62ef5a8881bd8b403fadf8959f782-edeb4547bbb622f13603.js	false		high
http://https://segments.company-target.com/log?vendor=choca&user_id=AAGWck7Gx08AACFLtnVIaQ	false	• Avira URL Cloud: safe	unknown
http://https://www.cloudflare.com/static/42f301a7759388a0cd4d88640f9ceae3/logo_lending-tree_color_32px-wrapper.svg	false		high
http://https://www.cloudflare.com/en-gb/products/turnstile/?utm_source=turnstile&utm_campaign=widget	false		high
http://https://www.google.com/ads/ga-audiences?v=1&aip=1&t=sr&_r=4&tid=UA-10218544-29&cid=1796770398.1667504172&jid=2019781536&_v=j98&z=1484409308	false		high
http://https://www.cloudflare.com/static/2bd82c17e6dc90a16e6877f133329444/logo_ncr_gray_32px-wrapper.svg	false		high
http://https://www.cloudflare.com/page-data/sq/d/1048862057.json	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.28.144.124	713-xsc-918.mktoresp.com	United States		15224	OMNITUREUS	false
52.222.191.11	segments.company-target.com	United States		16509	AMAZON-02US	false
204.79.197.200	dual-a-0001.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.18.2.24	digiphotoglobal.com	United States		13335	CLOUDFLARENETUS	false
54.230.206.114	api.company-target.com	United States		16509	AMAZON-02US	false
104.18.6.185	challenges.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
108.167.183.27	484242.484242.piraminds.com	United States		46606	UNIFIEDLAYER-AS-1US	false
104.16.57.101	static.cloudflareinsights.com	United States		13335	CLOUDFLARENETUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
142.251.143.134	ad.doubleclick.net	United States		15169	GOOGLEUS	false
52.85.92.7	tag.demandbase.com	United States		16509	AMAZON-02US	false
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.google.com	United States		15169	GOOGLEUS	false
104.16.124.96	tr.www.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.18.19.132	cloudflare.hcaptcha.com	United States		13335	CLOUDFLARENETUS	false
63.32.183.38	adserver-vpc-alb-1-1446435489.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
192.185.14.33	digiphotoglobal.fesdy.pe	United States		46606	UNIFIEDLAYER-AS-1US	false
151.101.1.140	reddit.map.fastly.net	United States		54113	FASTLYUS	false
142.250.153.156	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.251.143.98	adservice.google.com	United States		15169	GOOGLEUS	false
54.229.166.11	match.prod.bidr.io	United States		16509	AMAZON-02US	false
142.251.143.99	www.google.co.uk	United States		15169	GOOGLEUS	false
188.114.96.3	frjn1qu9aj7akf.bioch.ru	European Union		13335	CLOUDFLARENETUS	false
104.18.31.78	performance.radar.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
142.251.143.142	www.googleoptimize.com	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.123.96	www.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736961
Start date and time:	2022-11-03 12:34:25 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2IzUnZaMnh2WW1Gc0xtTnZiUT09
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@32/0@41/31
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.cloudflare.com/?utm_source=challenge&utm_campaign=m • Browse: https://www.cloudflare.com/?utm_source=challenge&utm_campaign=m • Browse: https://www.cloudflare.com/en-gb/products/turnstile/?utm_source=turnstile&utm_campaign=widget

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 142.251.143.131, 34.104.35.123, 23.205.237.4, 13.107.42.14, 142.251.143.168
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, l-0005.l-msedge.net, edgedl.me.gvt1.com, www.googletagmanager.com, bat.bing.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, e10776.b.akamaiedge.net, wildcard.marketo.net.edgekey.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

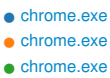
No static file info

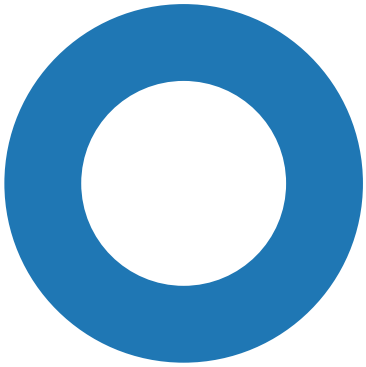
Network Behavior

No network behavior found

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5832, Parent PID: 4896

General

Target ID:	0
Start time:	12:35:21
Start date:	03/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: 6048, Parent PID: 5832

General

Target ID:	1
Start time:	12:35:22
Start date:	03/11/2022
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=1980 --field-trial-handle=1816,i,2919350836162336761,13592327512595919683,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **6136**, Parent PID: **4896**

General

Target ID:	2
Start time:	12:35:23
Start date:	03/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://484242.484242.piraminds.com/.#.aHR0cDovL0RpZ2lwaG90b2dsb2JhbC5mZXNkeS5wZS9odG1sI2MyRnNhV3d1YzI5dFlXNUFaR2xuYVhCb2lzUnZaMnh2WW1Gc0xtTnZiUT09
Imagebase:	0x7ff7d31b0000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Registry Activities

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

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

Disassembly

No disassembly