ID: 715089
Cookbook: browseurl.jbs
Time: 16:10:37
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

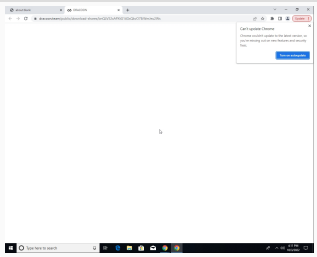
Windows Analysis Report

https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb2...

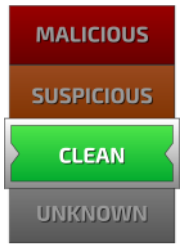
Overview

General Information

Sample URL:	https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0...ZC1zaGFyZXMlMkZiblFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscY
Analysis ID:	715089
Infos:	



Detection

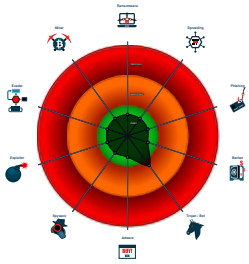


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

HTTP GET or POST without a user ...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6128 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5200 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=1944 --field-trial-handle=1808,i,10812047769471386771,6805671885659538109,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 2792 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb29uLnRlYW0lMkZwdWJsaWMlMkZkb3dubG9hZC1zaGFyZXMlMkZiblFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscYTJDrVmNKVcsJMUFqVTiobP6GgMqPFZKzMj&iat=1664797054&a=%7C%7C27821780%7C%7C&account=camservices%2Eactivehosted%2Ecom&email=V1inbcilbyhq5q3GQe2WGyBAWaAotQkn8fTjdS3g5M8%3D&s=d0f7bfb8e988e50796ae4b5ee42e911e&i=1A3A1A3 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

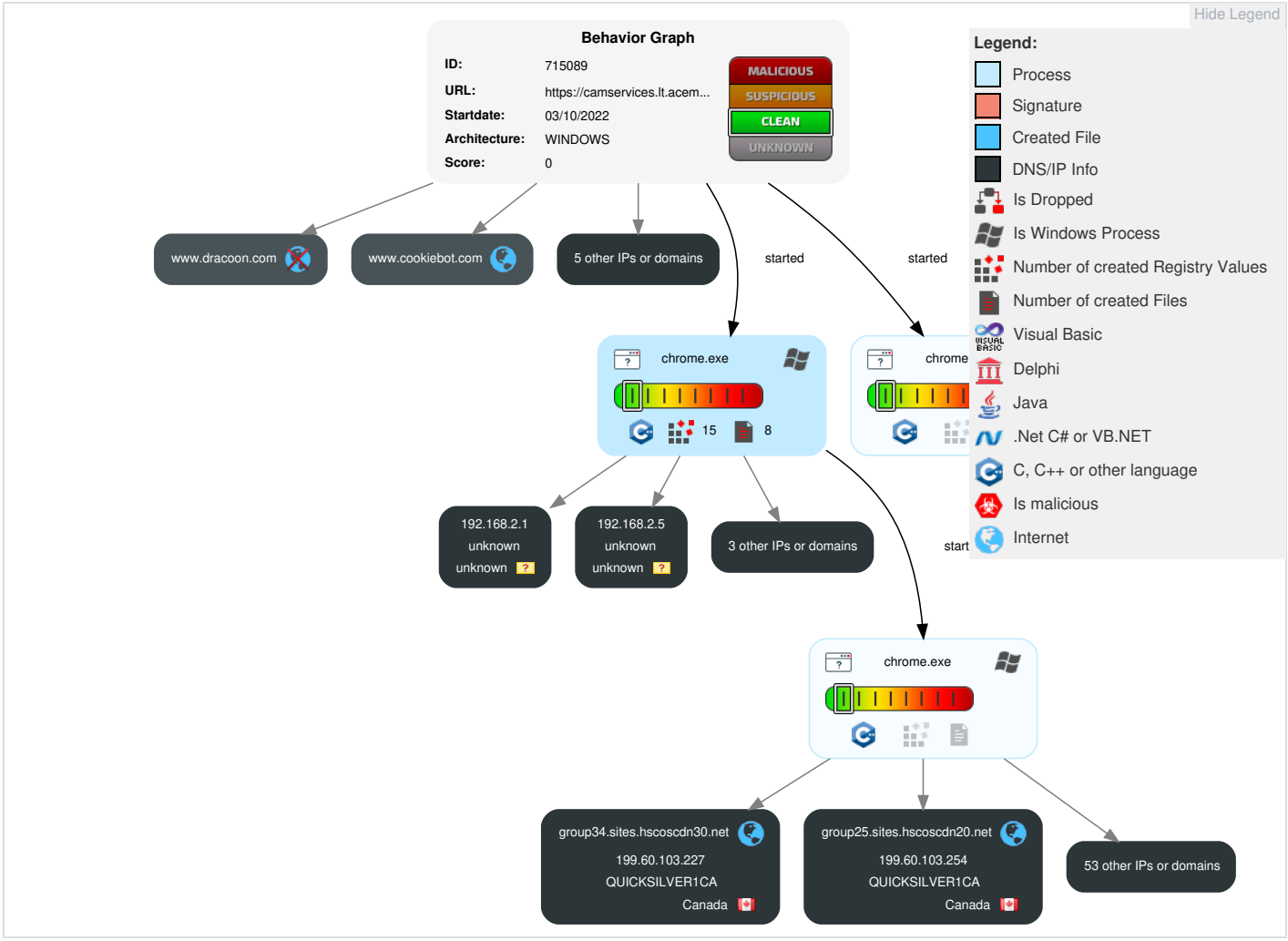
Joe Sandbox Signatures

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

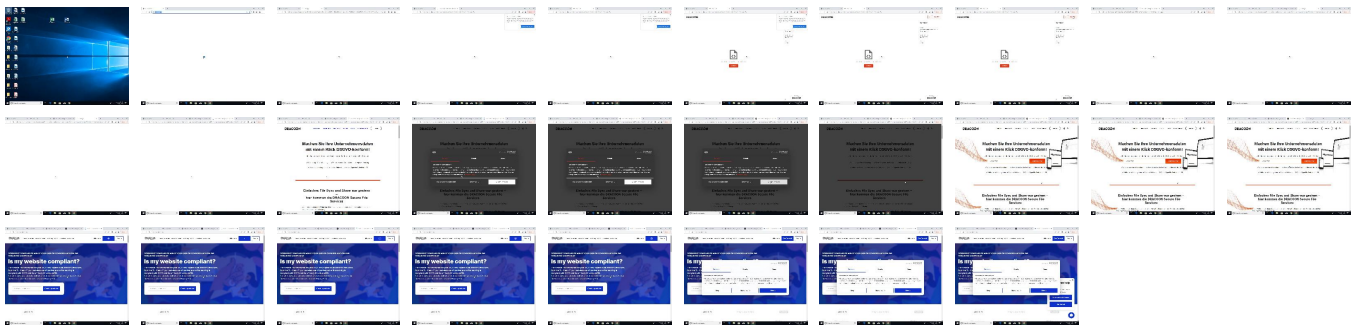
Behavior Graph

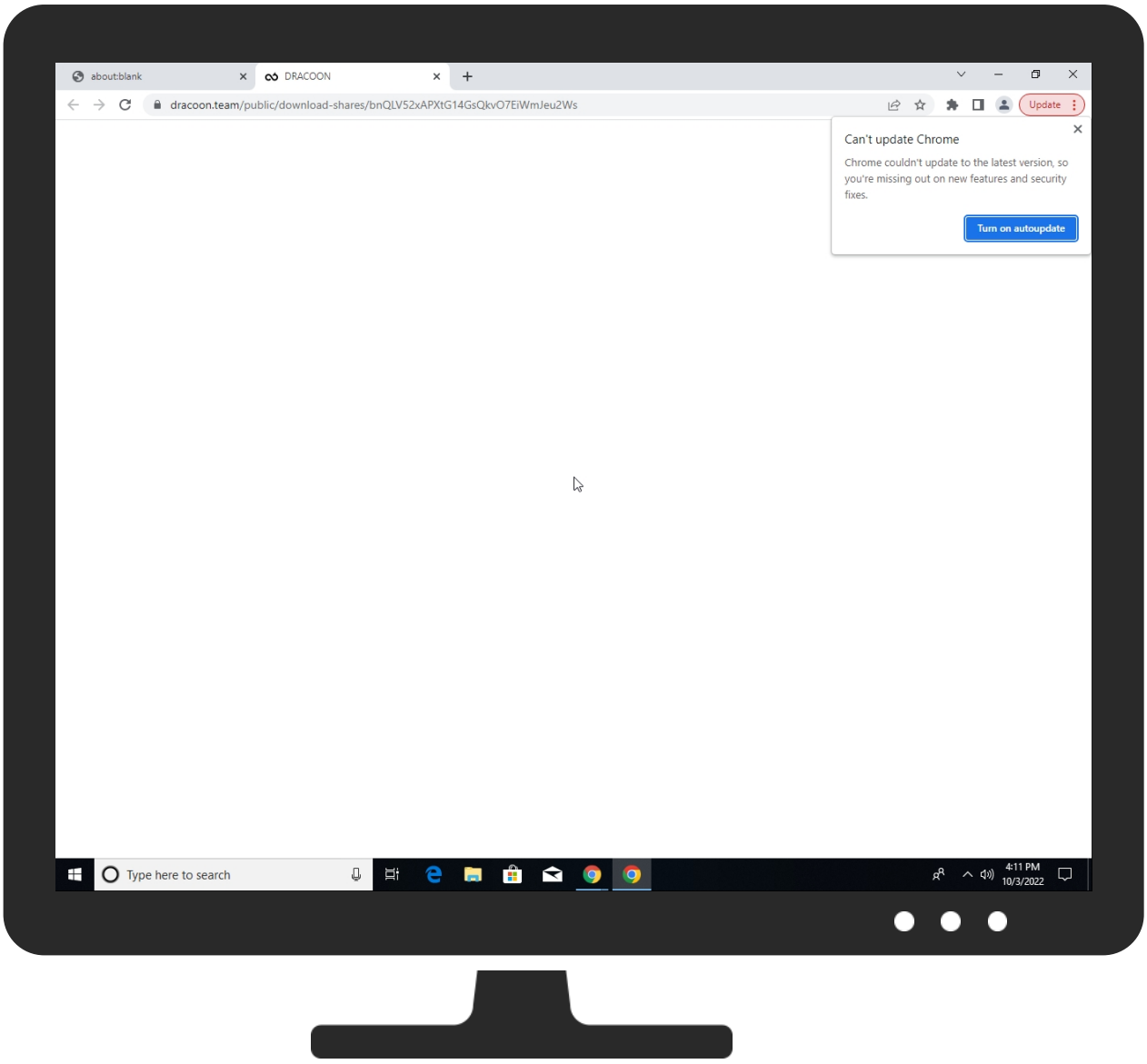


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb29uLnRlYW0lMkZwdWJsaWMlMkZkb3dubG9hZC1zaGFyZXMlMkZibIFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscYTJDrVmNKVcsJMUFqVTiobP6GgMqPFZKzMj&iat=1664797054&a=%7C%7C27821780%7C%7C&account=camservices%2Eactivehosted%2Ecom&email=V1inbcilbyhq5q3GQe2WGyBAWaAotQkn8fTjdS3g5M8%3D&s=d0f7bfb8e988e50796ae4b5ee42e911e&i=1A3A1A3	0%	Virustotal		Browse
http://https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb29uLnRlYW0lMkZwdWJsaWMlMkZkb3dubG9hZC1zaGFyZXMlMkZibIFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscYTJDrVmNKVcsJMUFqVTiobP6GgMqPFZKzMj&iat=1664797054&a=%7C%7C27821780%7C%7C&account=camservices%2Eactivehosted%2Ecom&email=V1inbcilbyhq5q3GQe2WGyBAWaAotQkn8fTjdS3g5M8%3D&s=d0f7bfb8e988e50796ae4b5ee42e911e&i=1A3A1A3	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://dracoon.team/3877.4f677868fd222ecb.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/190.1bb4f6e781a798f0.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/ressourcen/Success-Story_Exficon.png	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f665d544-1412-47fd-a4af-286f2c589a0e<=1664838732797&dt=1664838732798&at=1664838738993&an=1	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=0117add9-99af-4e72-83c5-af0deff39d68<=1664838733387&dt=1664838733391&at=1664838738997&an=1	0%	Avira URL Cloud	safe	
http://https://dracoon.team/2864.ea907e3dd1386ddb.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/4231.3b6476099c2a48b7.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/4188.b8551a46d367493c.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/Logos/pngs/AOK.png	0%	Avira URL Cloud	safe	
http://https://dracoon.team/7156.fc654ef1fb7dcdf6.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/1050.7a3e29784ba9193b.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/general-images/dracoon_fi-n.png	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/_hcms/forms/v2.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/cta/current.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=ea7f3491-9e71-4983-9f36-a28097130bb8<=1664838735840&dt=1664838735841&at=1664838738996&an=1	0%	Avira URL Cloud	safe	
http://https://dracoon.team/main.eb1d981b114c46d5.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/656.90fc8beb93d6422f.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs-fs/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/husare_success-story.png?width=200&name=husare_success-story.png	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Header_Home_Body2.jpg	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90<=1664838733528&dt=1664838733888&at=1664838738972&an=1	0%	Avira URL Cloud	safe	
http://https://dracoon.team/api/v4/public/shares/downloads/bnQLV52xAPXtG14GsQkvO7EiWmJeu2Ws	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs-fs/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Header_Home_neu2.png?width=1280&height=600&name=DRACOON-Header_Home_neu2.png	0%	Avira URL Cloud	safe	
http://https://dracoon.team/217.a9dc19e03d1e7d89.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/hsstatic/cos-LanguageSwitcher/static-1.11/sass/LanguageSwitcher.css	0%	Avira URL Cloud	safe	
http://https://4411134.fs1.hubspotusercontent-na1.net/hubfs/4411134/Dracoon_Files_Website/fonts/roboto-v30-latin-700.woff2	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/Logos/pngs/Barmer.png	0%	Avira URL Cloud	safe	
http://https://f.hubspotusercontent20.net/hubfs/273774/fontawesome/v5/webfonts-5.15.1/fa-regular-400.woff2	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/made-in-germany_bitmi_dracoon.png	0%	Avira URL Cloud	safe	
http://https://dracoon.team/roboto-latin-500.1dfbc3dbf815e3f3.woff2	0%	Avira URL Cloud	safe	
http://https://dracoon.team/dw/config	0%	Avira URL Cloud	safe	
http://https://dracoon.team/3834.12b87329906f4970.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/9572.c39501a51292f670.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/common.0c1ade8bfaddbfcd.js	0%	Avira URL Cloud	safe	
http://https://perf.hsforms.com/embed/v3/counters.gif?key=cta-render-success&value=1	0%	Avira URL Cloud	safe	
http://https://dracoon.team/7994.0154704b87507e1c.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/_hcms/forms//embed/v3/form/4411134/b1725674-94c9-4ea1-9c78-3ecda2c4c517/json?hutk=	0%	Avira URL Cloud	safe	
http://https://dracoon.team/6011.311cd80eb4c9176c.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/materialdesignicons-webfont.2474c2c14c0f85dd.woff2?v=7.0.96	0%	Avira URL Cloud	safe	
http://https://dracoon.team/7157.19049aa40725d135.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/BSI-C5-tested-dracoon.png	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=4f1c8f51-158f-40ea-8430-d60c26c6cbd4<=1664838733733&dt=1664838734045&at=1664838739006&an=1	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/ressourcen/Success-Story_Denton.png	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=088a6243-de76-4914-8eab-0d35a22cef58<=1664838735262&dt=1664838735263&at=1664838739003&an=1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://dracoon.team/3437.993c10fce390fe99.js	0%	Avira URL Cloud	safe	
http://https://273774.fs1.hubspotusercontent-na1.net/hubfs/273774/mp/act2/js/act21.min.js	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-83355137-1&cid=1759904237.1664838737&jid=378263475&_u=YADAAEAAAAAAAC~&z=1189421728	0%	Avira URL Cloud	safe	
http://https://dracoon.team/1713.c828172091a89e20.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/5039.b3b62be475b95dd2.js	0%	Avira URL Cloud	safe	
http://https://f.hubspotusercontent30.net/hubfs/4411134/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Voraussetzungen-Cloudanbieter-Video.mp4	0%	Avira URL Cloud	safe	
http://https://f.hubspotusercontent30.net/hubfs/4411134/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON_Vorschau_Cloudanbieter-Video.jpg	0%	Avira URL Cloud	safe	
http://https://dracoon.team/7756.85d954765b8eee66.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/332.df1034bc37a59a18.js	0%	Avira URL Cloud	safe	
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90<=1664838733528&dt=1664838733888&at=1664838738973&an=1	0%	Avira URL Cloud	safe	
http://https://dracoon.team/8144.9c427fa4d6687c3b.js	0%	Avira URL Cloud	safe	
http://https://dracoon.team/8271.5b19bfdde71aa6f0.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn2.hubspot.net	104.17.241.204	true	false		high
4411134.fs1.hubspotusercontent-na1.net	104.18.33.40	true	false		unknown
group34.sites.hscoscdn30.net	199.60.103.227	true	false		unknown
forms.hubspot.com	104.19.154.83	true	false		high
www.cookiebot.com	141.193.213.20	true	false		high
cta-service-cms2.hubspot.com	104.19.155.83	true	false		high
js.hs-analytics.net	104.17.71.176	true	false		unknown
prod-consentcdneu.b-cdn.net	89.187.165.194	true	false		high
stats.g.doubleclick.net	74.125.143.155	true	false		high
scontent.xx.fbcdn.net	157.240.236.1	true	false		high
track.hubspot.com	104.19.154.83	true	false		high
camservices.lt.acemlnc.com	3.91.141.18	true	false		unknown
0-4007773595.s3.nbg01.de.dracoon.io	62.128.13.176	true	false		unknown
no-cache.hubspot.com	104.19.154.83	true	false		high
perf.hsforms.com	104.16.87.5	true	false		unknown
cdnjs.cloudflare.com	104.17.24.14	true	false		high
prod-consenteu.b-cdn.net	89.187.165.194	true	false		high
www.google.com	142.250.203.100	true	false		high
273774.fs1.hubspotusercontent-na1.net	172.64.154.216	true	false		unknown
dracoon.team	141.95.22.201	true	false		unknown
f.hubspotusercontent30.net	104.16.185.114	true	false		unknown
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
js.hs-banner.com	104.18.33.171	true	false		unknown
a.nel.cloudflare.com	35.190.80.1	true	false		high
static.hsappstatic.net	104.17.6.210	true	false		unknown
accounts.google.com	142.250.203.109	true	false		high
app.hubspot.com	104.19.155.83	true	false		high
group25.sites.hscoscdn20.net	199.60.103.254	true	false		unknown
part-0032.t-0009.t-msedge.net	13.107.246.60	true	false		unknown
js.hsadspixel.net	104.17.112.176	true	false		unknown
l-0005.l-dc-msedge.net	13.107.43.14	true	false		unknown
js.hsleadflows.net	104.17.230.204	true	false		unknown
f.hubspotusercontent20.net	104.16.187.114	true	false		unknown
googleads.g.doubleclick.net	142.250.203.98	true	false		high
api.hubapi.com	104.17.203.204	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.co.uk	172.217.168.35	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
www.dracoon.com	unknown	unknown	false		unknown
design-assets.hubspot.com	unknown	unknown	false		high
static.cognitoforms.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
consentcdn.cookiebot.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
consent.cookiebot.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
www.cognitoforms.com	unknown	unknown	false		high
consentcdn.cookiebot.eu	unknown	unknown	false		unknown
consent.cookiebot.eu	unknown	unknown	false		unknown
snap.licdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://dracoon.team/190.1bb4f6e781a798f0.js	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f665d544-1412-47fd-a4af-286f2c589a0e<=1664838732797&dt=1664838732798&at=1664838738993&an=1	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/3877.4f677868fd222ecb.js	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/px/li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com%2Fcollect%3Fv%3D2%26fmt%3Djs%26pid%3D14979220%26time%3D1664838737864%26url%3Dhttps%253A%252F%252Fwww.dracoon.com%252Fde%252Fhome%253Futm_source%253Ddracoon.team%2526utm_medium%253Dwebapp-public-ingredient%2526utm_campaign%253Dingredient%2526content%253Ddownload-share%26liSync%3Dtrue	false		high
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=0117add9-99af-4e72-83c5-af0deff39d68<=1664838733387&dt=1664838733391&at=1664838738997&an=1	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/ressourcen/Success-Story_Exficon.png	false	• Avira URL Cloud: safe	unknown
http://https://www.cognitoforms.com/f/1hY1LR-SIkCC-lohyPfzGg/1	false		high
http://https://dracoon.team/2864.ea907e3dd1386ddb.js	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/general-images/dracoon_fi-n.png	false	• Avira URL Cloud: safe	unknown
http://https://design-assets.hubspot.com/hubfs/Slick%20Slider/ajax-loader.gif	false		high
http://https://dracoon.team/4231.3b6476099c2a48b7.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/4188.b8551a46d367493c.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/pagead/1p-user-list/1067903788/?random=1664838746852&cv=9&fst=1664838000000&num=1&bg=ffffff&guid=ON&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=0&u_nmime=0>m=2oa9s0&sendb=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&tiba=DRACOON%20%E2%80%93%20Enterprise%20File%20Service%20Plattform&async=1&fmt=3&is_vtc=1&random=878913581&resp=GooglemKTybQhCsO&rmt_tld=0&ipr=y	false		high
http://https://static.cognitoforms.com/form/modern/3.ad5848803136b4e0a540.js	false		high
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/Logos/pngs/AOK.png	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com/img/images/info-price.png	false		high
http://https://www.dracoon.com/_hcms/forms/v2.js	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report/v3?s=r2%2BzqT5Eaxj1Z1JhOGA1ddPa3h21X9vW%2BgSOagFobboympNVTXl5Iw1AHyDSAcCNNPoHLOAYewDZhQli1vgEabrFzTK9TGMcn5msOiamqIwxUN4Zj9jpa8fgZZSBWySLYQ%3D%3D	false		high
http://https://dracoon.team/7156.fc654ef1fb7dcdf6.js	false	• Avira URL Cloud: safe	unknown
http://https://static.cognitoforms.com/form/modern/109.87f2162044a9e0041459.js	false		high
http://https://no-cache.hubspot.com/cta/default/4411134/8c63b838-ba29-4860-b44e-622252ffdb9b.png	false		high
http://https://www.cookiebot.com/wp-content/uploads/sites/7/2022/05/forbes-2-1.svg	false		high
http://https://no-cache.hubspot.com/cta/default/4411134/bec483fc-7570-49fe-ae9b-f5b8782d0820.png	false		high
http://https://dracoon.team/1050.7a3e29784ba9193b.js	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://cta-service-cms2.hubspot.com/ctas/v2/public/cs/cta-json?canon=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&pageId=45396106131&pid=4411134&sv=cta-embed-js-static-1.93&utm_campaign=ingredient&utm_medium=webapp-public-ingredient&rdy=1&cos=1&df=t&pg=f665d544-1412-47fd-a4af-286f2c589a0e&pg=0117add9-99af-4e72-83c5-af0deff39d68&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90&pg=4f1c8f51-158f-40ea-8430-d60c26c6cbd4&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90&pg=4f1c8f51-158f-40ea-8430-d60c26c6cbd4&pg=bec483fc-7570-49fe-ae9b-f5b8782d0820&pg=7be61d8a-fe7c-4bab-bfb3-0e7a6e860049&pg=47a953e5-8807-458e-a4d5-23334307d756&pg=fa2ff578-3833-4c84-9c40-c68c0bf20d6f&pg=814073b8-2446-4f0e-9ff0-4d3821d0c12a&pg=088a6243-de76-4914-8eab-0d35a22cef58&pg=b80ed34f-d053-4a75-ace2-329d20748e44&pg=d2e2b9d1-58b5-4cc9-8ea1-0fc83ab93d01&pg=ea7f3491-9e71-4983-9f36-a28097130bb8&pg=8c63b838-ba29-4860-b44e-622252ffdb9b&pg=d11e1f17-a15c-4876-9db0-9ed9804bfa01	false		high
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=ea7f3491-9e71-4983-9f36-a28097130bb8<=1664838735840&dt=1664838735841&at=1664838738996&an=1	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs/cta/cta/current.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/main.eb1d981b114c46d5.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/656.90fc8beb93d6422f.js	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.9.0/slick.min.js?_=1664838737729	false		high
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Header_Home_Body2.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs-fs/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/husare_success-story.png?width=200&name=husare_success-story.png	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=16&fi=b6528fa1-e321-4f06-bb67-76c7ea70458e&lfi=3036003&ft=1&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=45396106131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838741409&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90<=1664838733528&dt=1664838733888&at=1664838738972&an=1	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com/wp-content/uploads/sites/7/2022/05/bbc-logo-1-1.svg	false		high
http://https://dracoon.team/api/v4/public/shares/downloads/bnQLV52xAPXtG14GsQkvO7EiWmJeu2Ws	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs-fs/hubfs/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Header_Home_neu2.png?width=1280&height=600&name=DRACOON-Header_Home_neu2.png	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=12&aij=%5B%22088a6243-de76-4914-8eab-0d35a22cef58%22%2C%22ac291f39-a546-4982-ac3e-4c282f1852aa%22%5D&rfc=8&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=45396106131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838740197&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://static.cognitoforms.com/form/modern/137.cb0a683ad4506adaaba6.js	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.9.0/slick.min.js?_=1664838737726	false		high
http://https://www.cookiebot.com/wp-content/plugins/uc-leadgen-bubble/assets/css/bubble.css?ver=1.0.13	false		high
http://https://www.cookiebot.com/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.6.3	false		high
http://https://dracoon.team/217.a9dc19e03d1e7d89.js	false	• Avira URL Cloud: safe	unknown
http://https://static.cognitoforms.com/form/modern/57.1dcce137607cda5b1232.js	false		high
http://https://consentcdn.cookiebot.eu/sdk/bc-v4.min.html	false		unknown
http://https://www.dracoon.com/hs/hsstatic/cos-LanguageSwitcher/static-1.11/sass/LanguageSwitcher.css	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=12&aij=%5B%2247a953e5-8807-458e-a4d5-23334307d756%22%2C%222883d8fd-d5e3-4c6f-af97-a067d5048928%22%5D&rfc=8&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=45396106131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838739824&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://4411134.fs1.hubspotusercontent-na1.net/hubfs/4411134/Dracoon_Files_Website/fonts/roboto-v30-latin-700.woff2	false	• Avira URL Cloud: safe	unknown

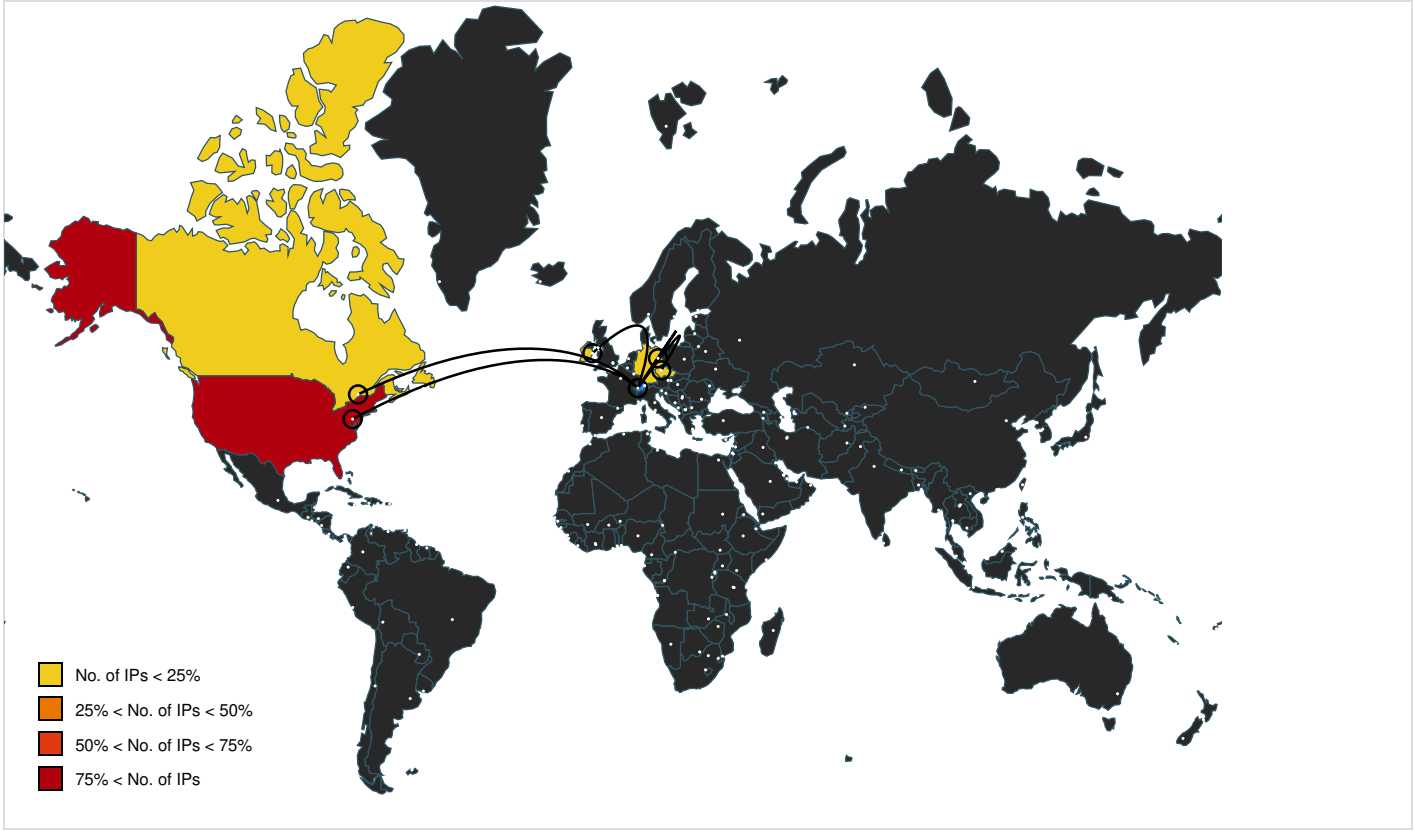
Name	Malicious	Antivirus Detection	Reputation
http://https://connect.facebook.net/signals/plugins/identity.js?v=2.9.84	false		high
http://https://consentcdn.cookiebot.eu/sdk/bc-v4.min.html	false		unknown
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/Logos/pngs/Barmer.png	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report/v3?s=AjRaXMMf4YzCv1D1uREd4nVxUGdJ0NNcMsMH%2FQJ1e37lSJE68qx39XWGkttkl3tALFLyVi%2BjTsMwiC2idvKEh0g4gseVaw%2B1NjzzUunKNpK3c%2FEDCzchxzD0kbkZfKZ7q%2BDe1j2D	false		high
http://https://f.hubspotusercontent20.net/hubfs/273774/fontawesome/v5/webfonts-5.15.1/fa-regular-400.woff2	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/made-in-germany_bitmi_dracoon.png	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/public/download-shares/bnQLV52xAPXtG14GsQkvO7EiWmJeu2Ws	false		unknown
http://https://dracoon.team/roboto-latin-500.1dfbc3dbf815e3f3.woff2	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/dw/config	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/3834.12b87329906f4970.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/9572.c39501a51292f670.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/common.0c1ade8bfaddbfcd.js	false	• Avira URL Cloud: safe	unknown
http://https://perf.hsforms.com/embed/v3/counters.gif?key=cta-render-success&value=1	false	• Avira URL Cloud: safe	unknown
file:///C:/Users/user/Downloads/Work%20Place%20Rating%20For%20Top%20100%20Nominees.html	false		low
http://https://dracoon.team/7994.0154704b87507e1c.js	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/_hcms/forms//embed/v3/form/4411134/b1725674-94c9-4ea1-9c78-3ecda2c4c517/json?hutk=	false	• Avira URL Cloud: safe	unknown
http://https://static.cognitoforms.com/form/modern/153.b3e43d96920ebce0f30d.js	false		high
http://https://dracoon.team/6011.311cd80eb4c9176c.js	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/de/home?utm_source=dracoon.team&utm_medium=webapp-public-ingredient&utm_campaign=ingredient&content=download-share	false		unknown
http://https://dracoon.team/materialdesignicons-webfont.2474c2c14c0f85dd.woff2?v=7.0.96	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=12&aij=%5B%228c63b838-ba29-4860-b44e-622252ffdb9b%22%2C%22f170512b-888f-4a93-9eac-c7a7e321df9a%22%5D&rfc=8&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=453961061316131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838739816&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://consentcdn.cookiebot.com/sdk/bc-v4.min.html	false		high
http://https://dracoon.team/7157.19049aa40725d135.js	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com/en/wp-content/themes/cookiebot/components/templates/cb-pricing-selector/css/cb-pricing-selector.css?ver=1664771652	false		high
http://https://www.cookiebot.com/wp-content/uploads/sites/7/2022/05/techcrunch-logo.svg	false		high
http://https://no-cache.hubspot.com/cta/default/4411134/fa2ff578-3833-4c84-9c40-c68c0bf20d6f.png	false		high
http://https://www.cookiebot.com/wp-content/themes/cookiebot/js/cb-main-pricing.js?ver=1664771651	false		high
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/home/BSI-C5-tested-dracoon.png	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=4f1c8f51-158f-40ea-8430-d60c26c6cbd4<=1664838733733&dt=1664838734045&at=1664838739006&an=1	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hubfs/Dracoon_Files_Website/images/ressourcen/Success-Story_Denton.png	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=088a6243-de76-4914-8eab-0d35a22cef58<=1664838735262&dt=1664838735263&at=1664838739003&an=1	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=12&aij=%5B%22b80ed34f-d053-4a75-ace2-329d20748e44%22%2C%226e140672-a19b-46c4-b441-202ef0a69f10%22%5D&rfc=8&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=453961061316131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838739830&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://dracoon.team/3437.993c10fce390fe99.js	false	• Avira URL Cloud: safe	unknown
http://https://273774.fs1.hubspotusercontent-na1.net/hubfs/273774/mp/act2/js/act21.min.js	false	• Avira URL Cloud: safe	unknown
http://https://no-cache.hubspot.com/cta/default/4411134/d11e1f17-a15c-4876-9db0-9ed9804bfa01.png	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j97&tid=UA-83355137-1&cid=1759904237.1664838737&jid=378263475&_u=YADAAEAAAAAAAC~&z=1189421728	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/1713.c828172091a89e20.js	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com/wp-content/uploads/sites/7/2022/05/financial-times.svg	false		high
http://https://dracoon.team/5039.b3b62be475b95dd2.js	false	• Avira URL Cloud: safe	unknown
http://https://track.hubspot.com/__ptq.gif?k=17&fi=b1725674-94c9-4ea1-9c78-3ecda2c4c517&fci=c53a35e1-f966-4703-bda0-8b5a02f6894d&ft=0&sd=1280x1024&cd=24-bit&cs=UTF-8&ln=en-us&bfp=4285505810&v=1.1&a=4411134&pi=45396106131&ct=standard-page&ccu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome&cpi=45396106131&lpi=45396106131&abi=59236623921&lvi=45396106131&lvc=de&pu=https%3A%2F%2Fwww.dracoon.com%2Fde%2Fhome%3Futm_source%3Ddracoon.team%26utm_medium%3Dwebapp-public-ingredient%26utm_campaign%3Dingredient%26content%3Ddownload-share&t=DRACOON+%E2%80%93+Enterprise+File+Service+Plattform&cts=1664838739774&vi=37546955804357582f90e505db2bd357&nc=true&u=46543416.37546955804357582f90e505db2bd357.1664838739744.1664838739744.1664838739744.1&b=46543416.1.1664838739744&cc=15	false		high
http://https://f.hubspotusercontent30.net/hubfs/4411134/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON-Voraussetzungen-Cloudanbieter-Video.mp4	false	• Avira URL Cloud: safe	unknown
http://https://f.hubspotusercontent30.net/hubfs/4411134/Dracoon_Files_Website/images/home/Home%20neu%202021-10/DRACOON_Vorschau_Cloudanbieter-Video.jpg	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/7756.85d954765b8eee66.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/8271.5b19bfdde71aa6f0.js	false	• Avira URL Cloud: safe	unknown
http://https://dracoon.team/332.df1034bc37a59a18.js	false	• Avira URL Cloud: safe	unknown
http://https://no-cache.hubspot.com/cta/default/4411134/b80ed34f-d053-4a75-ace2-329d20748e44.png	false		high
http://https://www.cookiebot.com/en/wp-content/themes/cookiebot/components/templates/cb-header-old/css/cb-header-old.css?ver=1664771653	false		high
http://https://dracoon.team/8144.9c427fa4d6687c3b.js	false	• Avira URL Cloud: safe	unknown
http://https://www.dracoon.com/hs/cta/ctas/v2/public/cs/cta-loaded.js?pid=4411134&pg=f8ed3fa4-2418-4d93-a1c0-0047ea7a5e90<=1664838733528&dt=1664838733888&at=1664838738973&an=1	false	• Avira URL Cloud: safe	unknown
http://https://www.cookiebot.com/wp-content/plugins/uc-leadgen-bubble/assets/js/uc_lg.js?ver=1.0.13	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.cognitoforms.com/f/1hY1LR-SlkCC-lohyPfzGg/1	d6d53501-dfe0-43e7-8b5d-47ddb527e5ae.tmp.0.dr	false		high
http://https://www.cognitoforms.com/f/iframe.js	d6d53501-dfe0-43e7-8b5d-47ddb527e5ae.tmp.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	cta-service-cms2.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.16.187.114	f.hubspotusercontent20.net	United States		13335	CLOUDFLARENETUS	false
104.18.33.171	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
104.17.230.204	js.hsleadflows.net	United States		13335	CLOUDFLARENETUS	false
141.95.22.201	dracoon.team	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
141.193.213.20	www.cookiebot.com	United States		396845	DV-PRIMARY-ASN1US	false
172.64.154.216	273774.fs1.hubspotusercontent-na1.net	United States		13335	CLOUDFLARENETUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
104.17.6.210	static.hsappstatic.net	United States		13335	CLOUDFLARENETUS	false
104.19.154.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.16.185.114	f.hubspotusercontent30.net	United States		13335	CLOUDFLARENETUS	false
199.60.103.227	group34.sites.hscoscdn30.net	Canada		23181	QUICKSILVER1CA	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
104.17.241.204	cdn2.hubspot.net	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.17.112.176	js.hsadspixel.net	United States		13335	CLOUDFLARENETUS	false
89.187.165.194	prod-consentcdneu.b-cdn.net	Czech Republic		60068	CDN77GB	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
3.91.141.18	camservices.lt.acemlnc.com	United States		14618	AMAZON-AESUS	false
13.107.246.60	part-0032.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
199.60.103.254	group25.sites.hscoscdn20.net	Canada		23181	QUICKSILVER1CA	false
13.107.43.14	l-0005.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.17.71.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.17.203.204	api.hubapi.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
74.125.143.155	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.18.33.40	4411134.fs1.hubspotusercontent-na1.net	United States		13335	CLOUDFLARENETUS	false
157.240.236.1	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.35	www.google.co.uk	United States		15169	GOOGLEUS	false
62.128.13.176	0-4007773595.s3.nbg01.de.dracoon.io	Germany		12337	NORIS-NETWORKITServiceProviderlocatedinNuernbergGerm	false
104.16.87.5	perf.hsforms.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.7
192.168.2.6
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715089
Start date and time:	2022-10-03 16:10:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb29uLnRlYW0lMkZwdWJsaWMlMkZkb3dubG9hZC1zaGFyZXMlMkZibIFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscYTJDrVmNKVcsJMUFqVTiobP6GgMqPFZKzMj&iat=1664797054&a=||27821780||&account=camservices.activehosted.com&email=V1inbcilbyhq5q3GQe2WGyBAWaAotQkn8fTjdS3g5M8%3D&s=d0f7bfb8e988e50796ae4b5ee42e911e&i=1A3A1A3
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:	14
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@34/3@52/38
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://www.dracoon.com/?utm_source=dracoon.team&utm_medium=webapp-public-ingredient&utm_campaign=ingredient&content=download-share • Browse: https://www.cookiebot.com/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 23.96.4.241, 80.67.82.33, 80.67.82.50, 172.217.168.10, 23.205.179.154, 172.217.168.42, 172.217.168.74, 142.250.203.106, 216.58.215.234, 142.250.203.104, 80.67.82.235, 172.217.168.78, 216.239.32.36, 216.239.34.36, 13.107.42.14, 142.250.203.98
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, cognito-services.cloudapp.net, fonts.googleapis.com, fs.microsoft.com, e3849.dsca.akamaiedge.net, www.googleadservices.com, content-autofill.googleapis.com, fonts.gstatic.com, clientservices.googleapis.com, pagead2.googlesyndication.com, star-azureedge-prod.trafficmanager.net, od.linkedin.edgesuite.net, region1.google-analytics.com, l-0005.l-msedge.net, cognito-static.afd.azureedge.net, edgedl.me.gvt1.com, www.googletagmanager.com, cognito-static.azureedge.net, update.googleapis.com, consent.cookiebot.com-v2.edgekey.net, a1916.dscg2.akamai.net, consentcdn.cookiebot.com-v1.edgekey.net, e110990.dsca.akamaiedge.net, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Downloads\Work Place Rating For Top 100 Nominees.html (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.097921803898891
Encrypted:	false
SSDEEP:	3:QXEWXG5SLueYmDKlC2ENqfiaM6OqtwN4Xs+qRDJvzbv8SLueYmDKMd9NGXIb:QtrLueYzlCFNraMjqtwwt+h3vDLueYzO
MD5:	084C44A91A9EE3AF05710133F702FE90
SHA1:	36C01BAB5961861244EBD264CC886A8BDA84A36C
SHA-256:	52978005186C512E1143347D42F791E9771D13F94AC266BC1AFE6932D63484E2
SHA-512:	71D54F16C37B6A8D9A600588C1E65D60A8777FDBB6E7588DC863294E26252B643626213711B0699626D6CB2FE48E500ACD41B92FFF646EE394A3AC2D7C70CEDB
Malicious:	false
Reputation:	low

Preview:	<iframe src="https://www.cognitoforms.com/f/1hY1LR-SIkCC-lohyPfzGg/1" style="border:0;width:100%;" height="508"></iframe>..<script src="https://www.cognitoforms.com/f/iframe.js"></script>

C:\Users\user\Downloads\Work Place Rating For Top 100 Nominees.html.crdownload (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.097921803898891
Encrypted:	false
SSDEEP:	3:QXEWXG5SLueYmDKlC2ENqfiaM6OqtwN4Xs+qRDJvzbv8SLueYmDKMd9NGXlb:QtrLueYzlCFNraMjqtwwt+h3vDLueYzO
MD5:	084C44A91A9EE3AF05710133F702FE90
SHA1:	36C01BAB5961861244EBD264CC886A8BDA84A36C
SHA-256:	52978005186C512E1143347D42F791E9771D13F94AC266BC1AFE6932D63484E2
SHA-512:	71D54F16C37B6A8D9A600588C1E65D60A8777FDBB6E7588DC863294E26252B643626213711B0699626D6CB2FE48E500ACD41B92FFF646EE394A3AC2D7C70CEDB
Malicious:	false
Reputation:	low
Preview:	<iframe src="https://www.cognitoforms.com/f/1hY1LR-SIkCC-lohyPfzGg/1" style="border:0;width:100%;" height="508"></iframe>..<script src="https://www.cognitoforms.com/f/iframe.js"></script>

C:\Users\user\Downloads\d6d53501-dfe0-43e7-8b5d-47ddb527e5ae.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.097921803898891
Encrypted:	false
SSDEEP:	3:QXEWXG5SLueYmDKlC2ENqfiaM6OqtwN4Xs+qRDJvzbv8SLueYmDKMd9NGXlb:QtrLueYzlCFNraMjqtwwt+h3vDLueYzO
MD5:	084C44A91A9EE3AF05710133F702FE90
SHA1:	36C01BAB5961861244EBD264CC886A8BDA84A36C
SHA-256:	52978005186C512E1143347D42F791E9771D13F94AC266BC1AFE6932D63484E2
SHA-512:	71D54F16C37B6A8D9A600588C1E65D60A8777FDBB6E7588DC863294E26252B643626213711B0699626D6CB2FE48E500ACD41B92FFF646EE394A3AC2D7C70CEDB
Malicious:	false
Reputation:	low
Preview:	<iframe src="https://www.cognitoforms.com/f/1hY1LR-SIkCC-lohyPfzGg/1" style="border:0;width:100%;" height="508"></iframe>..<script src="https://www.cognitoforms.com/f/iframe.js"></script>

Static File Info

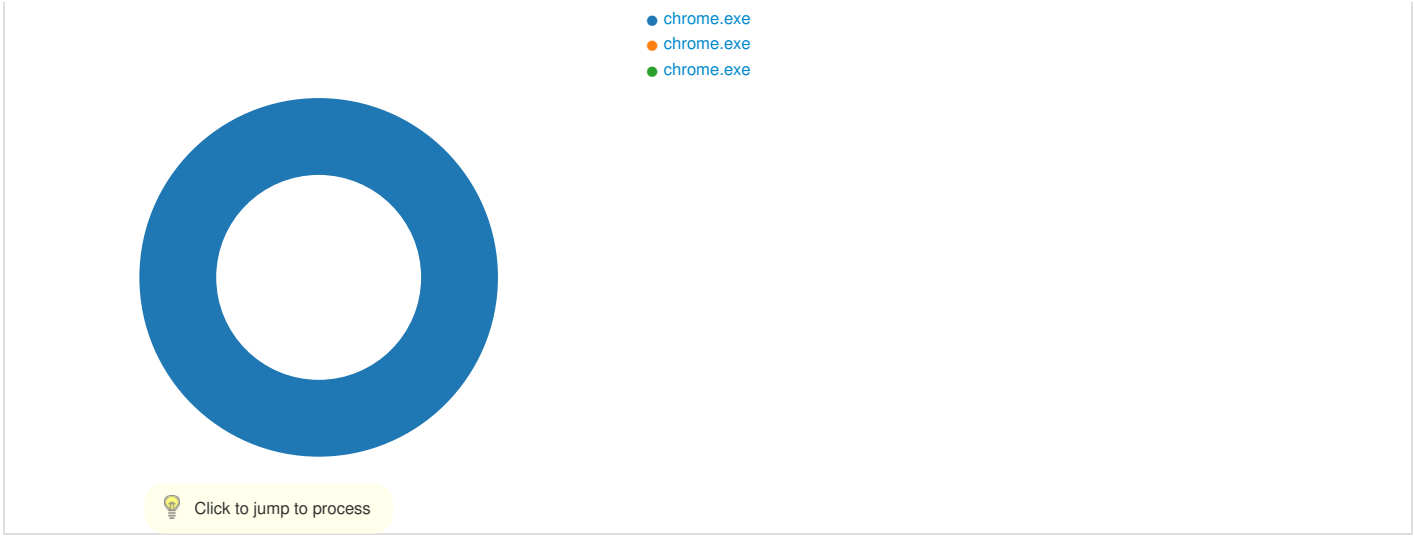
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 6128, Parent PID: 1844

General

Target ID:	0
Start time:	16:11:35
Start date:	03/10/2022
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:	0x7ff614650000
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: 5200, Parent PID: 6128

General

Target ID:	1
Start time:	16:11:36
Start date:	03/10/2022
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=1944 --field-trial-handle=1808,i,10812047769471386771,6805671885659538109,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
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: **2792**, Parent PID: **1844**

General

Target ID:	2
Start time:	16:11:37
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://camservices.lt.acemlnc.com/Prod/link-tracker?redirectUrl=aHR0cHMlM0ElMkYlMkZkcmFjb29uLnRlYW0lMkZwdWJsaWMlMkZkb3dubG9hZC1zaGFyZXMlMkZibIFMVjUyeEFQWHRHMTRHc1Frdk83RWlXbUpldTJXcw==&sig=7BXGdPpscYTJDrVmNKVcsJMUFqVTiobP6GgMqPFZKzMj&iat=1664797054&a=%7C%7C27821780%7C%7C&account=camservices%2Eactivehosted%2Ecom&email=V1inbcilbyhq5q3GQe2WGyBAWaAotQkn8fTjdS3g5M8%3D&s=d0f7bfb8e988e50796ae4b5ee42e911e&i=1A3A1A3
Imagebase:	0x7ff614650000
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