ID: 736963
Cookbook: browseurl.jbs
Time: 12:37:29
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

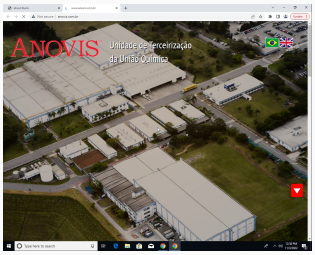
Windows Analysis Report

http://www.anovis.com.br/

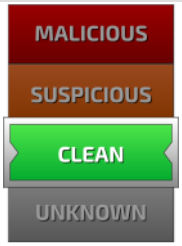
Overview

General Information

Sample URL:	http://www.anovis.com.br/
Analysis ID:	736963
Infos:	



Detection

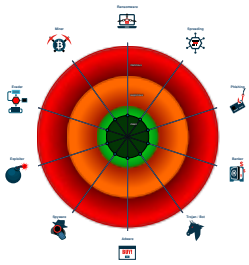


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 4520 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2148 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1960 --field-trial-handle=1772,i,17406513271277565 12,7249462608667158532,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 1812 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.anovis.com.br/ 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

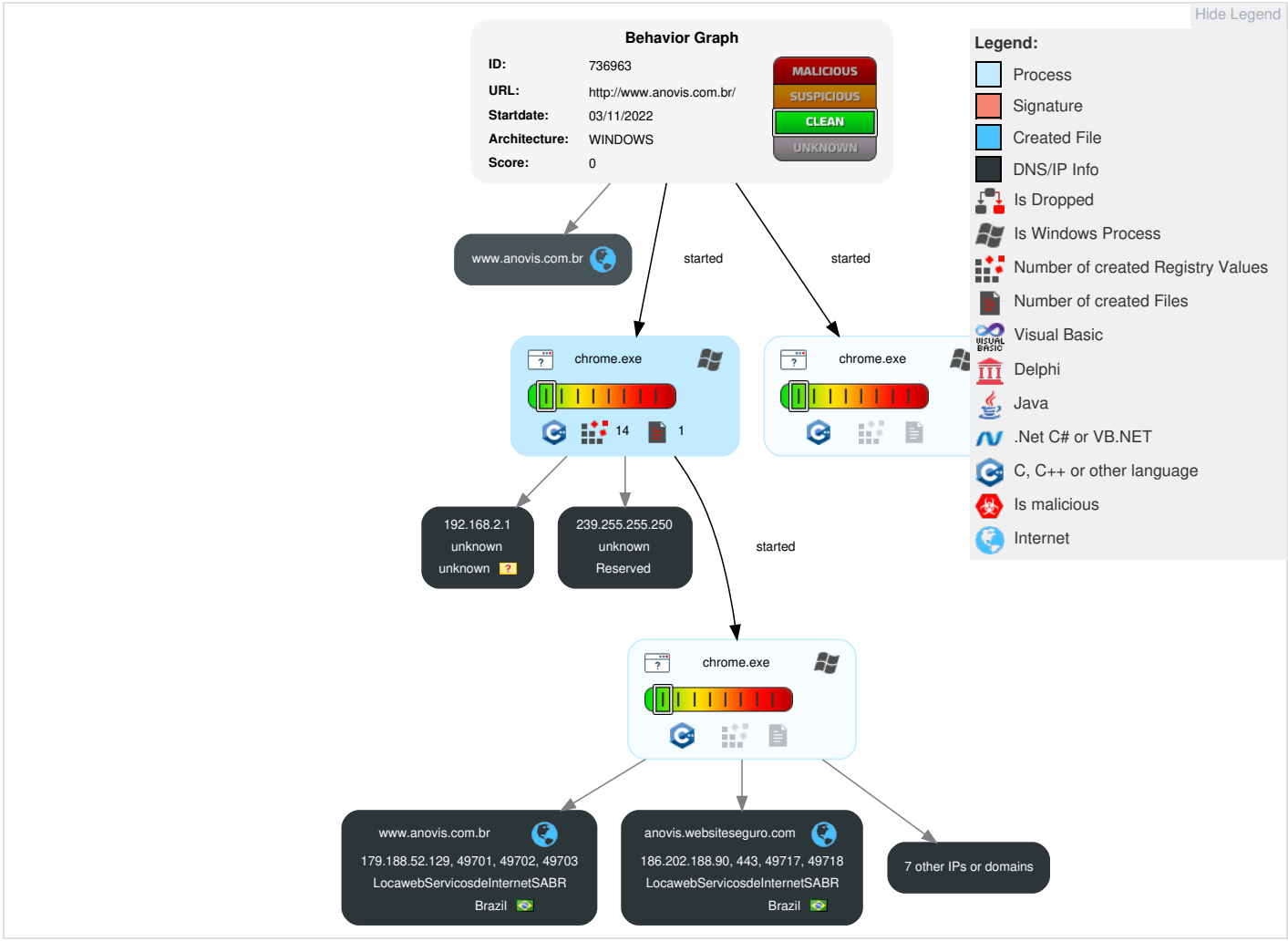
Joe Sandbox Signatures

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	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

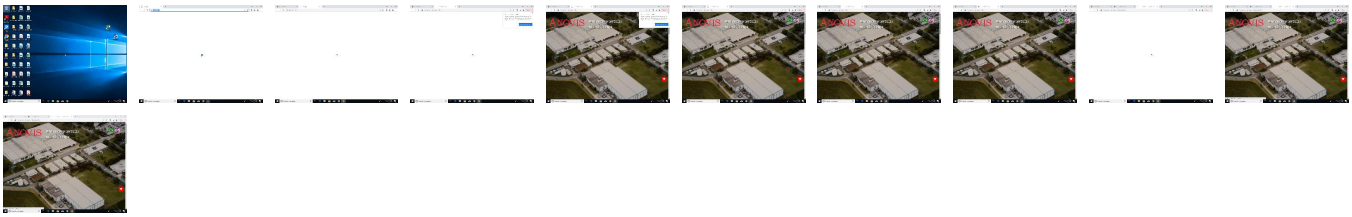
Behavior Graph

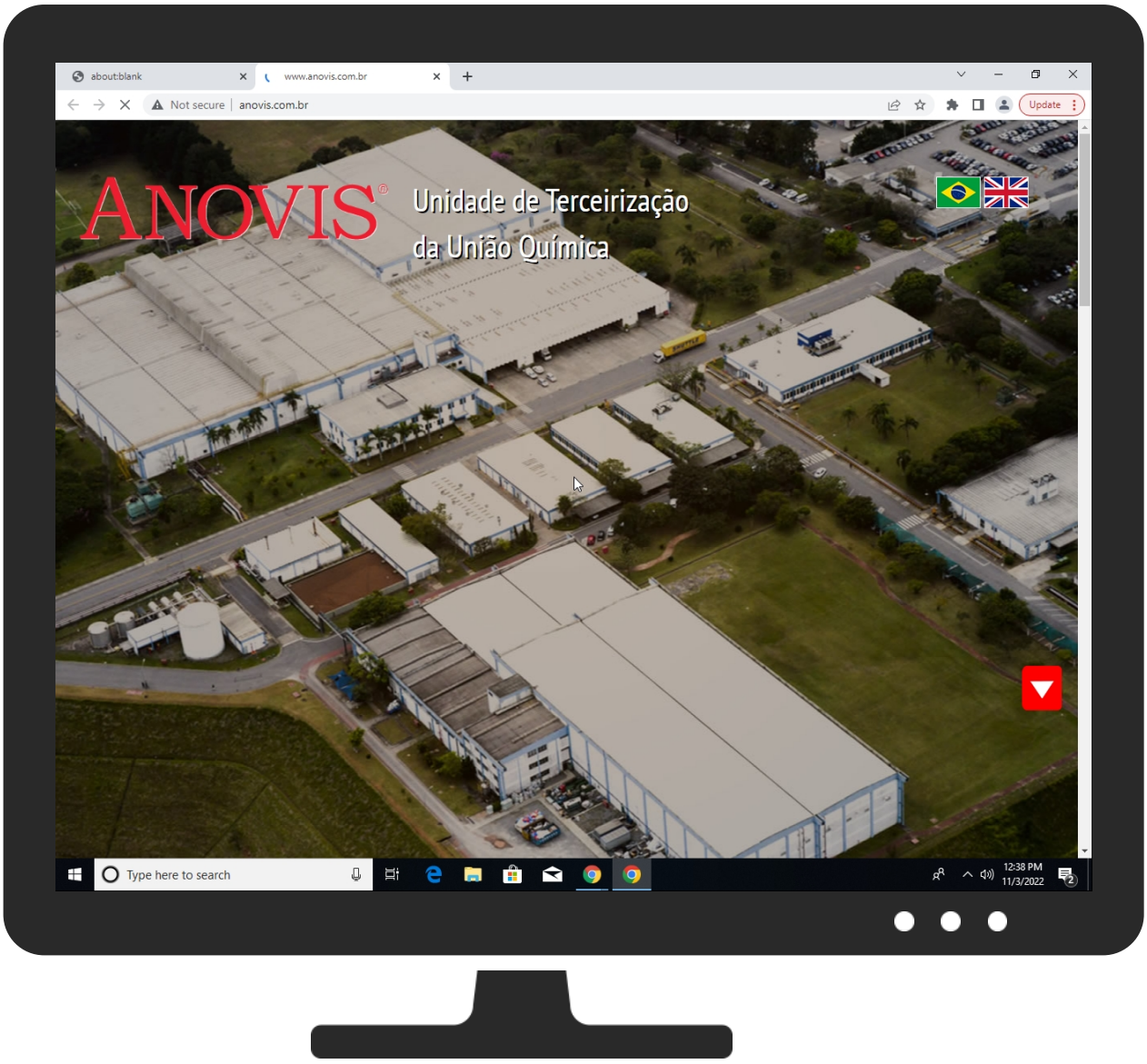


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://www.anovis.com.br/	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.anovis.com.br/images/galeria-2.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/unidade-embu.jpg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.anovis.com.br/ilightbox/src/js/jquery.requestAnimationFrame.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/bootstrap/css/bootstrap.min.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/icone-liquidos-orais.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/stellar.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/rodape-site-anovis.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/light-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/novo-logo-uniao5.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/bootstrap/js/bootstrap.min.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/rodape-site-anovis-mobile.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/band_en.gif	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/metro-black-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/seta-naveg-baixo-2.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/metro-white-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/mac-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/icone-solidos-orais.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/js/ilightbox.packed.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/css/ilightbox.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/home1.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/slide-footer-2.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/smooth-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/dark-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/galeria-4.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/respond.src.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/band_br.gif	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/js/jquery.mousewheel.js	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/logo-anovis.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/unidade-brasilia-2.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/unidade-taboao.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/unidade-pouso.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/slide-footer-1.jpg	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/ilightbox/src/parade-skin/skin.css	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/favicon.ico	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/icone-semi-solidos.png	0%	Avira URL Cloud	safe	
http://www.anovis.com.br/images/galeria-1.jpg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

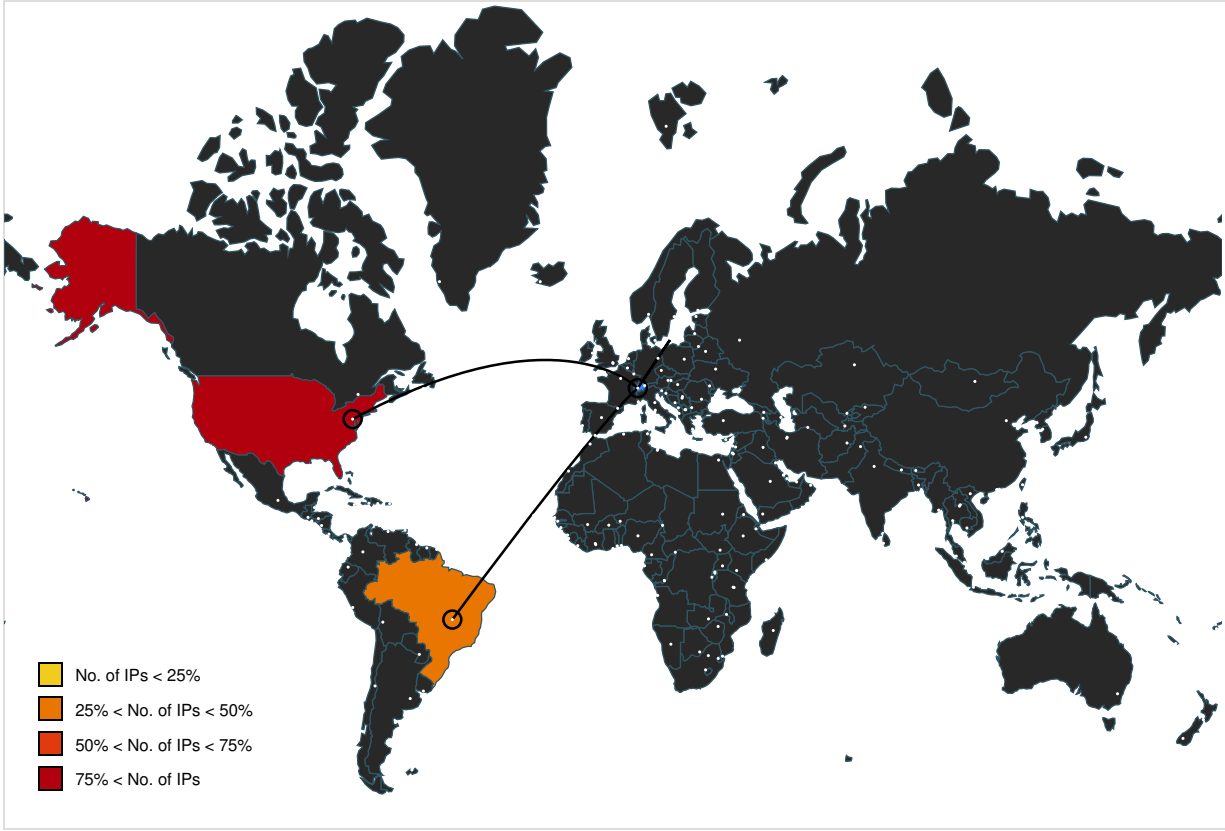
Name	IP	Active	Malicious	Antivirus Detection	Reputation
anovis.websiteseguro.com	186.202.188.90	true	false		high
accounts.google.com	142.251.143.141	true	false		high
www.anovis.com.br	179.188.52.129	true	false		unknown
www.google.com	142.251.143.132	true	false		high
clients.l.google.com	142.251.143.174	true	false		high
osscdn.netdnasa9.netdna-cdn.com	23.111.8.154	true	false		high
clients2.google.com	unknown	unknown	false		high
oss.maxcdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.anovis.com.br/images/icone-liquidos-orais.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/galeria-2.jpg	false	• Avira URL Cloud: safe	unknown
http://https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js	false		high
http://www.anovis.com.br/ilightbox/src/js/jquery.requestAnimationFrame.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/bootstrap/css/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/unidade-embu.jpg	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.anovis.com.br/images/rodape-site-anovis.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/stellar.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/light-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/novo-logo-uniao5.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/bootstrap/js/bootstrap.min.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/rodape-site-anovis-mobile.jpg	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://www.anovis.com.br/index.php	false		unknown
http://www.anovis.com.br/images/band_en.gif	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/	false		unknown
http://www.anovis.com.br/	false		unknown
http://www.anovis.com.br/ilightbox/src/metro-black-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/seta-naveg-baixo-2.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/metro-white-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/mac-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://https://oss.maxcdn.com/respond/1.4.2/respond.min.js	false		high
http://www.anovis.com.br/ilightbox/src/js/ilightbox.packed.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/css/ilightbox.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/icone-solidos-orais.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/home1.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/slide-footer-2.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/smooth-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/dark-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/galeria-4.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/respond.src.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/band_br.gif	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/js/jquery.mousewheel.js	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/logo-anovis.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/unidade-brasilia-2.jpg	false	• Avira URL Cloud: safe	unknown
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://www.anovis.com.br/images/unidade-taboao.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/unidade-pouso.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/index.php	false		unknown
http://www.anovis.com.br/images/slide-footer-1.jpg	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/ilightbox/src/parade-skin/skin.css	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/icone-semi-solidos.png	false	• Avira URL Cloud: safe	unknown
http://www.anovis.com.br/images/galeria-1.jpg	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
186.202.188.90	anovis.websiteseguro.com	Brazil		27715	LocawebServicosdeInternet SABR	false
179.188.52.129	www.anovis.com.br	Brazil		27715	LocawebServicosdeInternet SABR	false
23.111.8.154	osscdn.netdnasa9.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736963
Start date and time:	2022-11-03 12:37:29 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.anovis.com.br/
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@25/0@7/9
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: http://www.anovis.com.br/index.php

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.143.131, 142.251.143.202, 34.104.35.123, 142.251.143.163, 142.251.143.142
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, edgedl.me.gvt1.com, ajax.googleapis.com, fonts.gstatic.com, update.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.google-analytics.com
- 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

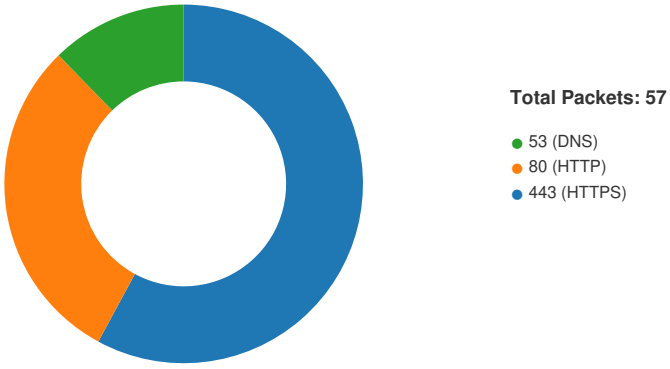
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:33.693859100 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:33.693908930 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:33.694014072 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:33.694293976 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.694377899 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.694511890 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.698904991 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:33.698947906 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:33.699203968 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.699235916 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.745382071 CET	49701	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:33.746265888 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:33.846199989 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:33.848047018 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:33.848097086 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:33.851237059 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.851816893 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.851876020 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.852222919 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:33.852304935 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:33.852569103 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.852643013 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.853524923 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:33.853601933 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:33.888387918 CET	49703	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:33.959619045 CET	80	49701	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:33.959717035 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:33.959871054 CET	49701	80	192.168.2.5	179.188.52.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:33.959950924 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:33.962268114 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.103055000 CET	80	49703	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.103153944 CET	49703	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.147751093 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.147810936 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.147881031 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.148160934 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.148178101 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.177541971 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177606106 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177650928 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177692890 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177736044 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177755117 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.177778959 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177819967 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177824974 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.177865028 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177902937 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.177913904 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177958965 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.177966118 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.178134918 CET	80	49702	179.188.52.129	192.168.2.5
Nov 3, 2022 12:38:34.178186893 CET	49702	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.187979937 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:34.188047886 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.188265085 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:34.188281059 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.188441038 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.188930988 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:34.189042091 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.189285994 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.189333916 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:34.189358950 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.236529112 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.240012884 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.240048885 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.242371082 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.242554903 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.245021105 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.245167017 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:34.245196104 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.245342016 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.245424032 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:34.245528936 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.245543003 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.245763063 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.247982025 CET	49700	443	192.168.2.5	142.251.143.174
Nov 3, 2022 12:38:34.248004913 CET	443	49700	142.251.143.174	192.168.2.5
Nov 3, 2022 12:38:34.262506008 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.262643099 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:34.262686014 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.263084888 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.263211966 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:34.267077923 CET	49699	443	192.168.2.5	142.251.143.141
Nov 3, 2022 12:38:34.267132044 CET	443	49699	142.251.143.141	192.168.2.5
Nov 3, 2022 12:38:34.285434961 CET	49701	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.286411047 CET	49703	80	192.168.2.5	179.188.52.129

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:34.288014889 CET	49705	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.289190054 CET	49706	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.290496111 CET	49707	80	192.168.2.5	179.188.52.129
Nov 3, 2022 12:38:34.316392899 CET	49704	443	192.168.2.5	142.251.143.132
Nov 3, 2022 12:38:34.316420078 CET	443	49704	142.251.143.132	192.168.2.5
Nov 3, 2022 12:38:34.368261099 CET	49710	443	192.168.2.5	23.111.8.154
Nov 3, 2022 12:38:34.368325949 CET	443	49710	23.111.8.154	192.168.2.5
Nov 3, 2022 12:38:34.368432999 CET	49710	443	192.168.2.5	23.111.8.154
Nov 3, 2022 12:38:34.368568897 CET	49711	443	192.168.2.5	23.111.8.154
Nov 3, 2022 12:38:34.368634939 CET	443	49711	23.111.8.154	192.168.2.5
Nov 3, 2022 12:38:34.368694067 CET	49711	443	192.168.2.5	23.111.8.154
Nov 3, 2022 12:38:34.369052887 CET	49710	443	192.168.2.5	23.111.8.154
Nov 3, 2022 12:38:34.369082928 CET	443	49710	23.111.8.154	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:33.492523909 CET	60649	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:33.502151966 CET	51441	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:33.504219055 CET	49177	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:33.520628929 CET	53	60649	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:33.521831036 CET	53	49177	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:33.739866972 CET	53	51441	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:34.083246946 CET	61452	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:34.103108883 CET	53	61452	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:34.301270962 CET	56751	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:34.321058035 CET	53	56751	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:35.970410109 CET	55068	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:36.215053082 CET	53	55068	8.8.8.8	192.168.2.5
Nov 3, 2022 12:38:41.266324997 CET	65513	53	192.168.2.5	8.8.8.8
Nov 3, 2022 12:38:41.532474041 CET	53	65513	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:38:33.492523909 CET	192.168.2.5	8.8.8.8	0x397a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:33.502151966 CET	192.168.2.5	8.8.8.8	0xe735	Standard query (0)	www.anovis.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:33.504219055 CET	192.168.2.5	8.8.8.8	0xa996	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:34.083246946 CET	192.168.2.5	8.8.8.8	0xaf99	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:34.301270962 CET	192.168.2.5	8.8.8.8	0x3c91	Standard query (0)	oss.maxcdn.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:35.970410109 CET	192.168.2.5	8.8.8.8	0x38ca	Standard query (0)	anovis.websiteseguro.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:41.266324997 CET	192.168.2.5	8.8.8.8	0x609e	Standard query (0)	www.anovis.com.br	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
Nov 3, 2022 12:38:33.520628929 CET	8.8.8.8	192.168.2.5	0x397a	No error (0)	accounts.google.com		142.251.143.141	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:33.521831036 CET	8.8.8.8	192.168.2.5	0xa996	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:33.521831036 CET	8.8.8.8	192.168.2.5	0xa996	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false

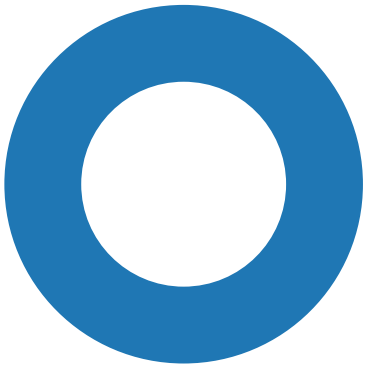
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:38:33.739866972 CET	8.8.8.8	192.168.2.5	0xe735	No error (0)	www.anovis.com.br		179.188.52.129	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:34.103108883 CET	8.8.8.8	192.168.2.5	0xaf99	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:34.321058035 CET	8.8.8.8	192.168.2.5	0x3c91	No error (0)	oss.maxcdn.com	osscdn.netdnasa9.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:34.321058035 CET	8.8.8.8	192.168.2.5	0x3c91	No error (0)	osscdn.netdnasa9.netdna-cdn.com		23.111.8.154	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:36.215053082 CET	8.8.8.8	192.168.2.5	0x38ca	No error (0)	anovis.websiteseguro.com		186.202.188.90	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:41.532474041 CET	8.8.8.8	192.168.2.5	0x609e	No error (0)	www.anovis.com.br		179.188.52.129	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- www.anovis.com.br
  - oss.maxcdn.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4520**, Parent PID: **4728**

General

Target ID:	0
Start time:	12:38:27
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: **2148**, Parent PID: **4520**

General

Target ID:	1
Start time:	12:38:28
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=1960 --field-trial-handle=1772,i,1740651327127756512,7249462608667158532,131072 --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: **1812**, Parent PID: **4728**

General

Target ID:	2
Start time:	12:38:29
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://www.anovis.com.br/
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