ID: 736962
Cookbook: browseurl.jbs
Time: 12:36:58
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Windows Analysis Report

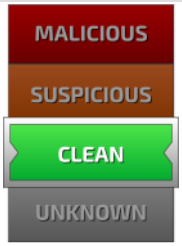
http://www.uniaoquimica.com.br/

Overview

General Information

Sample URL:	http://www.uniaoquimica.com.br/
Analysis ID:	736962
Infos:	

Detection

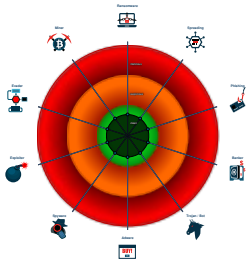


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5920 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6068 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=1936 --field-trial-handle=1620,i,10617228787614194027,5335811723259235483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6412 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=6660 --field-trial-handle=1620,i,10617228787614194027,5335811723259235483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6016 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6636 --field-trial-handle=1620,i,10617228787614194027,5335811723259235483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4768 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://www.uniaoquimica.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

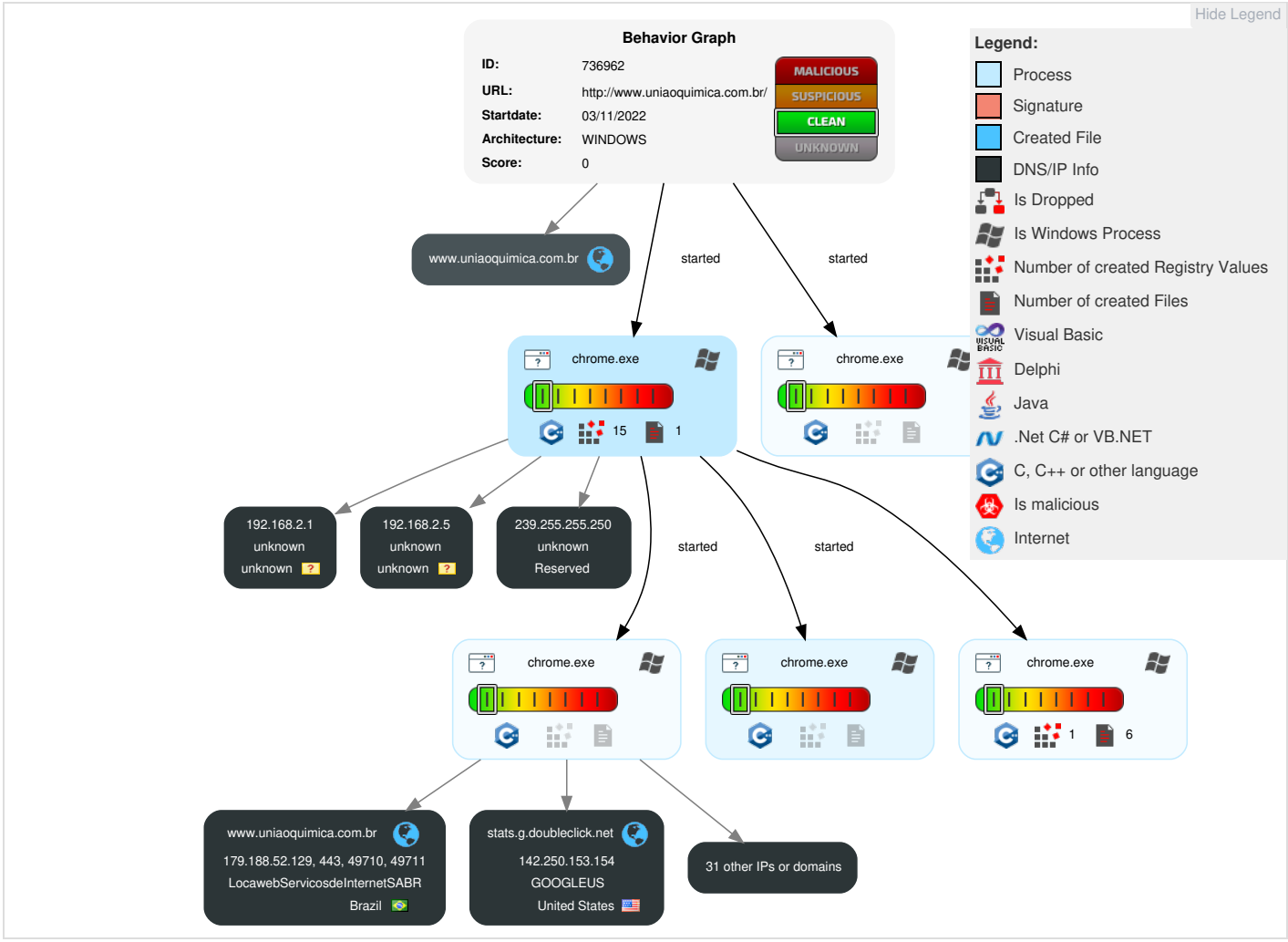
Joe Sandbox Signatures

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	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

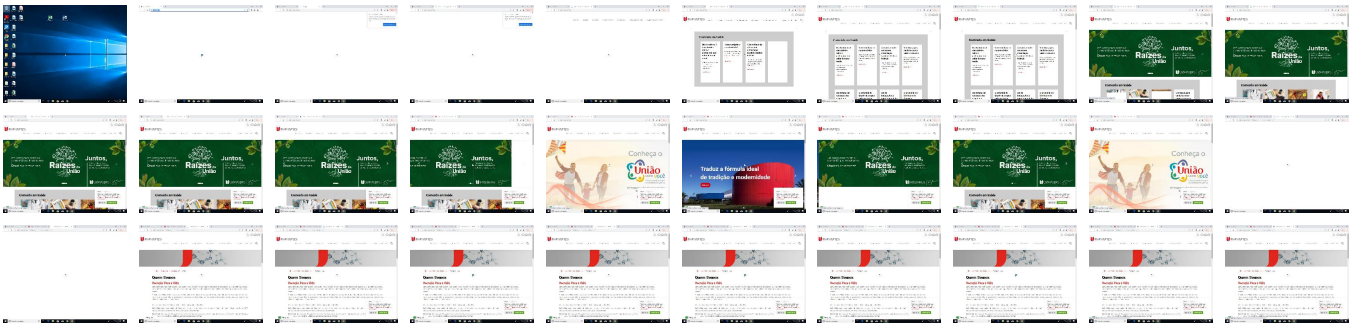
Behavior Graph

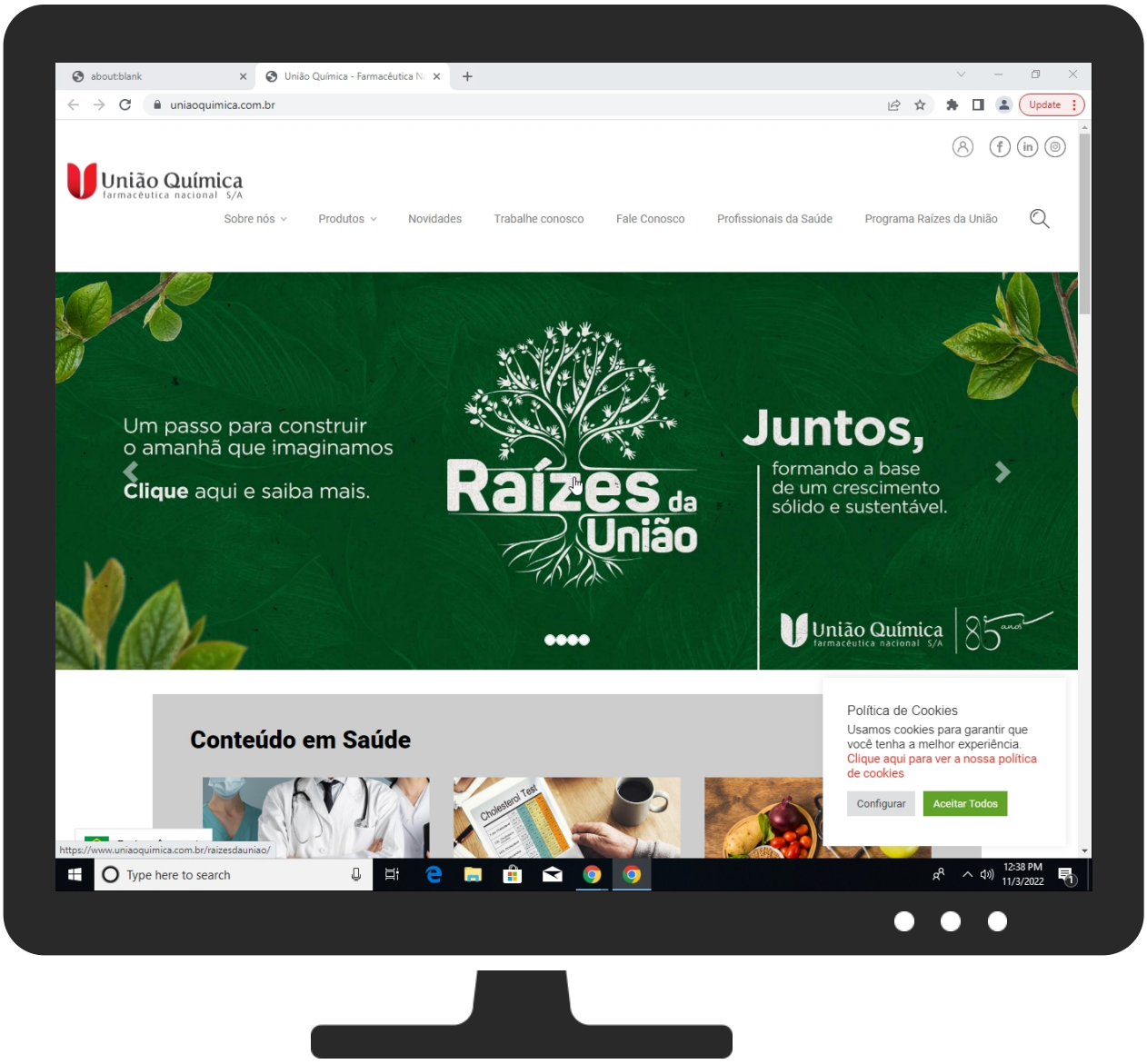


Screenshots

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://www.uniaoquimica.com.br/	0%	Avira URL Cloud	safe	
http://www.uniaoquimica.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://https://www.uniaoquimica.com.br/wp-content/plugins/flexy-breadcrumb/public/css/flexy-breadcrumb-public.css?ver=1.2.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/settings.css	0%	Avira URL Cloud	safe	
http://https://pageview-notify.rdstation.com.br/send	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/cool-timeline/includes/cool-timeline-block/dist/blocks.style.build.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/06/doador_sangue.jpg	0%	Avira URL Cloud	safe	
http://https://popups.rdstation.com.br/popup/show.json?account_id=208266&uniq=_e4cm8w8bi&ref=aHR0cHM6Ly93d3cudW5pYW9xdWltaWNhLmNvbS5ici9zb2JyZS1ub3MvaW5zdGl0dWNpb25hbC9xdWVtLXNvbW9zLw%3D%3D	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/04/Hipertensao-2.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/fonts/slick.woff	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/redes-topo-2.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/06/diaimunizacao.jpg	0%	Avira URL Cloud	safe	
http://https://s2.conveythis.com/javascriptClassic/1/conveythis.js	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/pagead/1p-user-list/10850071326/?random=1667504309894&cv=11&fst=1667502000000&bg=ffffff&guid=ON&async=1>m=2wgav0&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.uniaoquimica.com.br%2F&tiba=Uni%C3%A3o%20Qu%C3%ADmica%20-%20Farmac%C3%AAutica%20Nacional%20SA&fmt=3&is_vtc=1&random=1887520244&rmt_tld=1&ipr=y	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/js/jquery.themepunch.revolution.min.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/navigation.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/sustenta_mobile.jpeg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/selo_dun.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/sobre-nos/institucional/quem-somos/favicon.gif	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/08/colesterol.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/07/alimentacao_saudavel.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-5b.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/jquery-1.11.2.min.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-fone-pt.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/bootstrap/fonts/glyphicons-halflings-regular.woff2	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/novo-home-banner-produtos-1.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/jquery-3.3.1.min.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/respond.src.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/timeline/dist/jquery.roadmap.min.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/stellar.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/instagram-feed/css/sbi-styles.min.css?ver=6.0.8	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/navik.menu.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/07/inverno_UQ.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/03/diasono.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2020/02/cropped-favi_UQ-32x32.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/jQuery-Mask-Plugin-master/dist/jquery.mask.min.js	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/bootstrap/css/bootstrap.min.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-4b.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/modules/bootstrap/dist/css/bootstrap.min.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/05/Barra_UNIAO_QUIMICA_191220.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=5.6.3	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/novo-home-banner-produtos-3.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/sustenta_desk.jpeg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.6.3	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.6.3	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-saude-animal-pt.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-1b.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/flexy-breadcrumb/public/css/font-awesome.min.css?ver=4.7.0	0%	Avira URL Cloud	safe	
http://https://s2.conveythis.com/images/flags/v3/rectangular/1oU.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-saude-humana2-pt3.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/vcSupper-Banner.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-includes/js/wp-emoji-release.min.js?ver=6.0.3	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/05/generico.jpg	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/cookie-law-info/legacy/public/css/cookie-law-info-gdpr.css?ver=3.0.3	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/layers.css	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/plugins/install-fitvids-embed-fluid-width-videos/public/js/jquery.fitvids.js?ver=1.1	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=j98&tid=UA-88580317-2&cid=1895216195.1667504310&jid=996106167&_u=aEDAAEABAAAAACAAI~&z=2105021303	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-3b.jpg	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-F5K74BJJMM&cid=1895216195.1667504310>m=2oeav0&aip=1&z=366986139	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/ajax-loader.gif	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/favicon.gif	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/modules/fontawesome/webfonts/fa-solid-900.woff2	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/seta-rodape.png	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3	0%	Avira URL Cloud	safe	
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/slick-theme.css	0%	Avira URL Cloud	safe	
http://https://popups.rdstation.com.br/popup/show.json?account_id=208266&uniq=_pcwmxj0dg&ref=aHR0cHM6Ly93d3cudW5pYW9xdWltaWNhLmNvbS5ici8%3D	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
k8s-production.rdops.systems	35.223.116.65	true	false		unknown
www.uniaoquimica.com.br	179.188.52.129	true	false		unknown
accounts.google.com	142.251.143.141	true	false		high
i.ytimg.com	142.251.143.118	true	false		high
d335luupugsy2.cloudfront.net	54.230.182.204	true	false		high
region1.analytics.google.com	216.239.34.36	true	false		high
static.doubleclick.net	142.251.143.102	true	false		high
s2.conveythis.com	45.63.41.34	true	false		unknown
stats.g.doubleclick.net	142.250.153.154	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
youtube-ui.l.google.com	142.251.143.110	true	false		high
pages.rdstation.com.br	34.68.90.188	true	false		unknown
www3.l.google.com	142.251.143.110	true	false		high
googleads.g.doubleclick.net	142.251.143.130	true	false		high
www.google.co.uk	142.251.143.99	true	false		unknown
photos-ugc.l.googleusercontent.com	142.251.143.161	true	false		high
www.google.com	142.251.143.132	true	false		high
clients.l.google.com	142.251.143.174	true	false		high
s.w.org	192.0.77.48	true	false		high
www.facebook.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
yt3.ggpht.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
pageview-notify.rdstation.com.br	unknown	unknown	false		unknown
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
translate.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
popups.rdstation.com.br	unknown	unknown	false		unknown

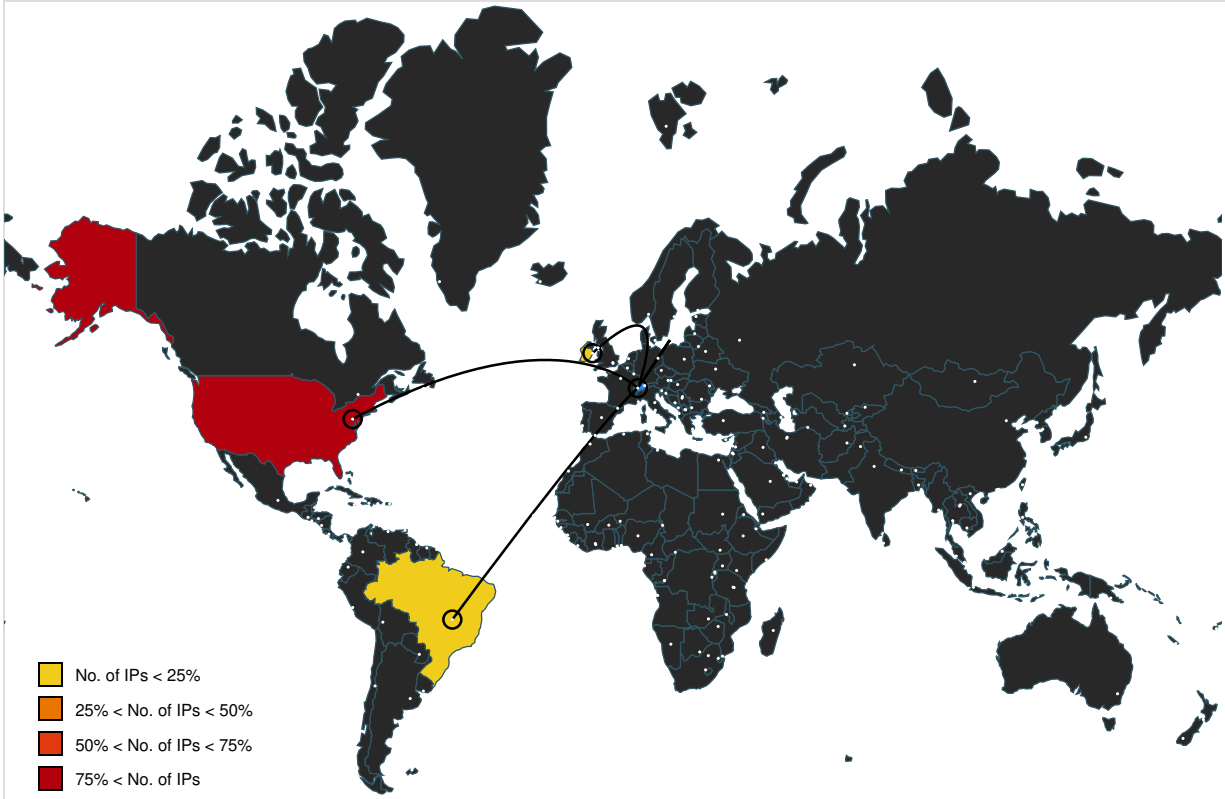
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://pageview-notify.rdstation.com.br/send	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/g/collect?v=2&tid=G-F5K74BJJMM&cid=1895216195.1667504310>m=2oeav0&aip=1	false		high
http://https://popups.rdstation.com.br/popup/show.json?account_id=208266&uniq=_e4cm8w8bi&ref=aHR0cHM6Ly93d3cudW5pYW9xdWltaWNhLmNvbS5ici9zb2JyZS1ub3MvaW5zdGl0dWNpb25hbC9xdWVtLXNvbW9zLw%3D%3D	false	• Avira URL Cloud: safe	unknown
http://https://d335luupugsy2.cloudfront.net/js/integration/stable/rd-js-integration.min.js?v=1	false		high
http://https://d335luupugsy2.cloudfront.net/js/traffic-source-cookie/stable/traffic-source-cookie.min.js	false		high
http://https://www.uniaoquimica.com.br/wp-content/plugins/flexy-breadcrumb/public/css/flexy-breadcrumb-public.css?ver=1.2.1	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/settings.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/06/doador_sangue.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/cool-timeline/includes/cool-timeline-block/dist/blocks.style.build.css	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi_webp/9dzXGEQe64c/sddefault.webp	false		high
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/04/Hipertensao-2.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-includes/js/jquery/jquery.min.js?ver=3.6.0	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/redes-topo-2.png	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j98&tid=UA-88580317-1&cid=1895216195.1667504310&jid=1388453128&gjid=275481333&_gid=1712735038.1667504310&_u=IEBAAEAAAAAAACAAI~&z=647080904	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/fonts/slick.woff	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/06/diaimunizacao.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/js/jquery.themepunch.revolution.min.js	false	• Avira URL Cloud: safe	unknown
http://https://d335luupugsy2.cloudfront.net/js/loader-scripts/47729378-db91-4099-81cc-b83344a23c4f-loader.js	false		high
http://https://s2.conveythis.com/javascriptClassic/1/conveythis.js	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/pagead/1p-user-list/10850071326/?random=1667504309894&cv=11&fst=1667502000000&bg=ffffff&guid=ON&async=1>m=2wgav0&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.uniaoquimica.com.br%2F&tiba=Uni%C3%A3o%20Qu%C3%ADmica%20-%20Farmac%C3%AAutica%20Nacional%20SA&fmt=3&is_vtc=1&random=1887520244&rmt_tld=1&ipr=y	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://yt3.ggpht.com/ZiuHPU7muRMcMSmvZjvzN1htejYMgQ5rs6wc9klbj-zTtvimNqcT2AwRJqHnJnLuTQXS68Q-=s68-c-k-c0x00ffffff-no-rj	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/navigation.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/sustenta_mobile.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/selo_dun.png	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/pagead/1p-user-list/10850071326/?random=1667504346159&cv=11&fst=1667502000000&bg=ffffff&guid=ON&async=1>m=2wgav0&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.uniaoquimica.com.br%2Fsobre-nos%2Finstitucional%2Fquem-somos%2F&tiba=Quem%20Somos%20-%20Uni%C3%A3o%20Qu%C3%ADmica&fmt=3&is_vtc=1&random=4119106531&rmt_tld=0&ipr=y	false		high
http://https://www.uniaoquimica.com.br/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j98&tid=UA-88580317-2&cid=1895216195.1667504310&jid=996106167&gjid=287247570&_gid=1712735038.1667504310&_u=aEDAAEABAAAAACAAI~&z=1472103419	false		high
http://https://connect.facebook.net/en_US/fbevents.js	false		high
http://https://www.uniaoquimica.com.br/sobre-nos/institucional/quem-somos/favicon.gif	false	• Avira URL Cloud: safe	unknown
http://www.uniaoquimica.com.br/	false		unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/08/colesterol.jpg	false	• Avira URL Cloud: safe	unknown
about:srcdoc	false		low
http://https://www.youtube.com/generate_204?diljYw	false		high
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/07/alimentacao_saudavel.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/	false		unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/jquery-1.11.2.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-5b.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/bootstrap/fonts/glyphicons-halflings-regular.woff2	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-fone-pt.png	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/Vi2gT2190YE?feature=oembed	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/jquery-3.3.1.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/novo-home-banner-produtos-1.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/respond.src.js	false	• Avira URL Cloud: safe	unknown
http://https://region1.analytics.google.com/g/collect?v=2&tid=G-F5K74BJJMM>m=2oeav0&_p=955606876&_gaz=1&cid=1895216195.1667504310&ul=en-us&sr=1280x1024&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&sid=1667504311&sct=1&seg=0&dl=https%3A%2F%2Fwww.uniaoquimica.com.br%2F&dt=Uni%C3%A3o%20Qu%C3%ADmica%20-%20Farmac%C3%AAutica%20Nacional%20SA&en=page_view&_fv=1&_ss=1	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/timeline/dist/jquery.roadmap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/stellar.js	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/instagram-feed/css/sbi-styles.min.css?ver=6.0.8	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/navik.menu.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/07/inverno_UQ.jpg	false	• Avira URL Cloud: safe	unknown
http://https://static.doubleclick.net/instream/ad_status.js	false		high
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/03/diasono.jpg	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/id	false		high
http://https://www.uniaoquimica.com.br/wp-content/uploads/2020/02/cropped-favi_UQ-32x32.png	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/jQuery-Mask-Plugin-master/dist/jquery.mask.min.js	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/bootstrap/css/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-4b.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/js/th/EWuoZ_9LU3hL76PT3YFLg_EjKJdTpZ6rgtgTJA98OBY.js	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/modules/bootstrap/dist/css/bootstrap.min.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/05/Barra_UNIAO_QUIMICA_191220.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/swv/js/index.js?ver=5.6.3	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/sustenta_desk.jpeg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/novo-home-banner-produtos-3.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.6.3	false	• Avira URL Cloud: safe	unknown
http://https://s2.conveythis.com/images/flags/v3/rectangular/1oU.png	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-1b.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.facebook.com/tr/	false		high
http://https://www.uniaoquimica.com.br/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.6.3	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-saude-animal-pt.png	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
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.youtube.com/s/player/03bec62d/player_ias.vflset/en_US/remote.js	false		high
http://https://www.uniaoquimica.com.br/wp-content/plugins/flexy-breadcrumb/public/css/font-awesome.min.css?ver=4.7.0	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-sac-saude-humana2-pt3.png	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/03bec62d/player_ias.vflset/en_US/base.js	false		high
http://https://www.facebook.com/tr/?id=265708851437346&ev=PageView&dl=https%3A%2F%2Fwww.uniaoquimica.com.br%2F&rl=&if=false&ts=1667504313270&sw=1280&sh=1024&v=2.9.89&r=stable&ec=0&o=30&fbp=fb.2.1667504313193.1721050976&it=1667504310722&coo=false&rqm=GET	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/vcSupper-Banner.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-includes/js/wp-emoji-release.min.js?ver=6.0.3	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/uploads/2021/05/generico.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/cookie-law-info/legacy/public/css/cookie-law-info-gdpr.css?ver=3.0.3	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/generate_204?yEr0HQ	false		high
http://https://www.youtube.com/s/player/03bec62d/player_ias.vflset/en_US/embed.js	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slider-revolution/revolution/css/layers.css	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/plugins/install-fitvids-embed-fluid-width-videos/public/js/jquery.fitvids.js?ver=1.1	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j98&tid=UA-88580317-2&cid=1895216195.1667504310&jid=996106167&_u=aEDAAEABAAAAACAAI~&z=2105021303	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/s/player/03bec62d/www-embed-player.vflset/www-embed-player.js	false		high
http://https://www.youtube.com/embed/9dzXGEQe64c?start=2&feature=oembed	false		high
http://https://d335luupugsy2.cloudfront.net/js/lead-tracking/stable/lead-tracking.min.js	false		high
http://https://www.google.com/pagead/1p-user-list/10850071326/?random=1667504309894&cv=11&fst=1667502000000&bg=ffffff&guid=ON&async=1>m=2wgav0&u_w=1280&u_h=1024&frm=0&url=https%3A%2F%2Fwww.uniaoquimica.com.br%2F&tiba=Uni%C3%A3o%20Qu%C3%ADmica%20-%20Farmac%C3%AAutica%20Nacional%20SA&fmt=3&is_vtc=1&random=1887520244&rmt_tld=0&ipr=y	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/icone-home-3b.jpg	false	• Avira URL Cloud: safe	unknown
http://https://www.google.co.uk/ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-F5K74BJJMM&cid=1895216195.1667504310>m=2oeav0&aip=1&z=366986139	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/ajax-loader.gif	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/images/seta-rodape.png	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/slick-1.8.1/slick/slick-theme.css	false	• Avira URL Cloud: safe	unknown
http://https://i.ytimg.com/vi/Vi2gT2190YE/maxresdefault.jpg	false		high
http://https://www.uniaoquimica.com.br/wp-content/themes/uniaoquimica/navik_menu/src/modules/fontawesome/webfonts/fa-solid-900.woff2	false	• Avira URL Cloud: safe	unknown
http://https://www.youtube.com/embed/9dzXGEQe64c?start=2&feature=oembed	false		high
http://https://www.uniaoquimica.com.br/favicon.gif	false	• Avira URL Cloud: safe	unknown
http://https://www.uniaoquimica.com.br/wp-includes/css/dist/block-library/style.min.css?ver=6.0.3	false	• Avira URL Cloud: safe	unknown
http://https://popups.rdstation.com.br/popup/show.json?account_id=208266&uniq=_pcwmxj0dg&ref=aHR0cHM6Ly93d3cudW5pYW9xdWltaWNhLmNvbS5ici8%3D	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/recaptcha/api.js	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.230.182.204	d335luupugsy2.cloudfront.net	United States		16509	AMAZON-02US	false
216.239.34.36	region1.analytics.google.com	United States		15169	GOOGLEUS	false
45.63.41.34	s2.conveythis.com	United States		20473	AS-CHOOPAUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
179.188.52.129	www.uniaoquimica.com.br	Brazil		27715	LocawebServicosdeInternet SABR	false
142.251.143.118	i.ytimg.com	United States		15169	GOOGLEUS	false
142.251.143.132	www.google.com	United States		15169	GOOGLEUS	false
142.251.143.110	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.251.143.174	clients.l.google.com	United States		15169	GOOGLEUS	false
142.251.143.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.251.143.161	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
34.68.90.188	pages.rdstation.com.br	United States		15169	GOOGLEUS	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
35.223.116.65	k8s-production.rdops.systems	United States		15169	GOOGLEUS	false
142.250.153.154	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.251.143.99	www.google.co.uk	United States		15169	GOOGLEUS	false
142.251.143.102	static.doubleclick.net	United States		15169	GOOGLEUS	false
142.251.143.141	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736962
Start date and time:	2022-11-03 12:36:58 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://www.uniaoquimica.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:	16
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@34/0@29/22
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.uniaoquimica.com.br/sobre-nos/institucional/quem-somos/ • Browse: https://www.uniaoquimica.com.br/sobre-nos/institucional/nossa-historia/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.143.131, 34.104.35.123, 142.251.143.202, 104.16.87.20, 104.16.85.20, 104.16.89.20, 104.16.86.20, 104.16.88.20, 142.251.143.163, 80.67.82.240, 80.67.82.235, 142.251.143.106, 142.251.143.138, 142.251.143.170, 142.251.143.168, 142.251.143.142, 13.107.42.14
- Excluded domains from analysis (whitelisted): www-linkedin-com.l-0005.l-msedge.net, fonts.googleapis.com, cdn.jsdelivr.net.cdn.cloudflare.net, fs.microsoft.com, content-autofill.googleapis.com, fonts.gstatic.com, clientservices.googleapis.com, od.linkedin.edgesuite.net, jnn-pa.googleapis.com, translate-pa.googleapis.com, l-0005.l-msedge.net, edgedl.me.gvt1.com, www.googletagmanager.com, translate.googleapis.com, update.googleapis.com, www.gstatic.com, a1916.dscg2.akamai.net, www.google-analytics.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many 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

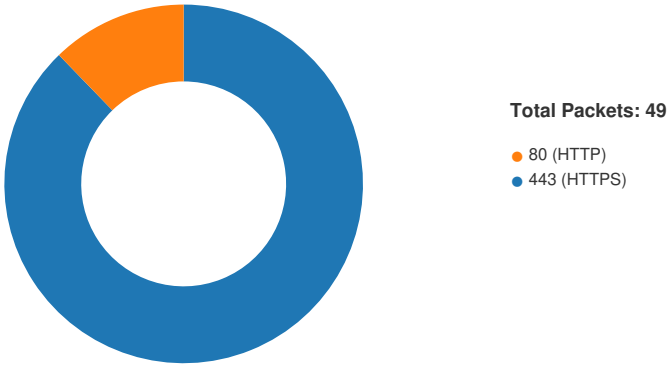
No created / dropped files found

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 12:38:03.054511070 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.054616928 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.054713964 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.057615042 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.057682991 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.057782888 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.058357954 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.058414936 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.058510065 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.059067011 CET	49709	443	192.168.2.3	142.251.143.141

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:03.059109926 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.059201956 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.059464931 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.059490919 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.059880018 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.059899092 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.060214996 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.060244083 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.060431004 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.060456038 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.079505920 CET	49710	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.080827951 CET	49711	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.153882027 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.156040907 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.259186029 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.261639118 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.261681080 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.261985064 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.262041092 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.262314081 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.262372971 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.263408899 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.263525963 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.264589071 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.264606953 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.264672995 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.264687061 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.264774084 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.267647982 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.267767906 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.267790079 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.268398046 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.268479109 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.268512964 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.268673897 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.290139914 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.290213108 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.292538881 CET	80	49710	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.292653084 CET	49710	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.293096066 CET	49710	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.294034958 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.294049025 CET	80	49711	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.294156075 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.294171095 CET	49711	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.375313044 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.375840902 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.505430937 CET	80	49710	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.509803057 CET	80	49710	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.575273991 CET	49710	80	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.786267042 CET	49712	443	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.786345005 CET	443	49712	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.786457062 CET	49712	443	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.786828995 CET	49712	443	192.168.2.3	179.188.52.129
Nov 3, 2022 12:38:03.786855936 CET	443	49712	179.188.52.129	192.168.2.3
Nov 3, 2022 12:38:03.967756033 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.967796087 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.967950106 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.967968941 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.968132973 CET	443	49709	142.251.143.141	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 3, 2022 12:38:03.968281031 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.968504906 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.968530893 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.968699932 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.968704939 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.968728065 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.968995094 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:03.969110012 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:03.969136953 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:03.969268084 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:03.969285011 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.025022984 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.025111914 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:04.025137901 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.025343895 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.025407076 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:04.040504932 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:04.040682077 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:04.040723085 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:04.040839911 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:04.040904999 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:04.042682886 CET	49704	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:04.042706013 CET	443	49704	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.044759989 CET	49709	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:04.044771910 CET	443	49709	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:04.075274944 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:04.075294018 CET	443	49708	142.251.143.174	192.168.2.3
Nov 3, 2022 12:38:04.103959084 CET	49706	443	192.168.2.3	142.251.143.141
Nov 3, 2022 12:38:04.103990078 CET	443	49706	142.251.143.141	192.168.2.3
Nov 3, 2022 12:38:04.175327063 CET	49708	443	192.168.2.3	142.251.143.174
Nov 3, 2022 12:38:04.203469038 CET	49706	443	192.168.2.3	142.251.143.141

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:38:02.763134956 CET	192.168.2.3	8.8.8.8	0xbb15	Standard query (0)	www.uniaoquimica.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:02.765187025 CET	192.168.2.3	8.8.8.8	0xa646	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:02.776900053 CET	192.168.2.3	8.8.8.8	0x1348	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:04.716759920 CET	192.168.2.3	8.8.8.8	0x486b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:06.218952894 CET	192.168.2.3	8.8.8.8	0x202e	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:06.295636892 CET	192.168.2.3	8.8.8.8	0x91f9	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:12.238471985 CET	192.168.2.3	8.8.8.8	0x6470	Standard query (0)	s2.conveythis.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:14.616461039 CET	192.168.2.3	8.8.8.8	0xc09c	Standard query (0)	d335luupugsy2.cloudfront.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:25.407694101 CET	192.168.2.3	8.8.8.8	0x7cd2	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.302727938 CET	192.168.2.3	8.8.8.8	0x818b	Standard query (0)	translate.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.772255898 CET	192.168.2.3	8.8.8.8	0xbf58	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.166184902 CET	192.168.2.3	8.8.8.8	0xd859	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.262981892 CET	192.168.2.3	8.8.8.8	0xf8da	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.386472940 CET	192.168.2.3	8.8.8.8	0xae30	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 3, 2022 12:38:30.684906960 CET	192.168.2.3	8.8.8.8	0x4b61	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.983438015 CET	192.168.2.3	8.8.8.8	0x653a	Standard query (0)	region1.analytics.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:31.720144033 CET	192.168.2.3	8.8.8.8	0xdba8	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:34.244379997 CET	192.168.2.3	8.8.8.8	0x57e6	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:35.180196047 CET	192.168.2.3	8.8.8.8	0xc343	Standard query (0)	pageview-notify.rdstation.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:36.656116962 CET	192.168.2.3	8.8.8.8	0xfede	Standard query (0)	popups.rdstation.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:39.748903990 CET	192.168.2.3	8.8.8.8	0x6dd	Standard query (0)	www.uniaoquimica.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.669617891 CET	192.168.2.3	8.8.8.8	0xf37e	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.920892954 CET	192.168.2.3	8.8.8.8	0x95d8	Standard query (0)	www.uniaoquimica.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:04.821166039 CET	192.168.2.3	8.8.8.8	0x503f	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:09.911422968 CET	192.168.2.3	8.8.8.8	0x4d12	Standard query (0)	static.doubleclick.net	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.897824049 CET	192.168.2.3	8.8.8.8	0x95d3	Standard query (0)	yt3.ggpht.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.910556078 CET	192.168.2.3	8.8.8.8	0x7543	Standard query (0)	i.ytimg.com	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:42.744710922 CET	192.168.2.3	8.8.8.8	0x68dc	Standard query (0)	pageview-notify.rdstation.com.br	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:44.286992073 CET	192.168.2.3	8.8.8.8	0xb169	Standard query (0)	popups.rdstation.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 12:38:02.804567099 CET	8.8.8.8	192.168.2.3	0x1348	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:02.804567099 CET	8.8.8.8	192.168.2.3	0x1348	No error (0)	clients.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:02.805423021 CET	8.8.8.8	192.168.2.3	0xa646	No error (0)	accounts.google.com		142.251.143.141	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:03.004971027 CET	8.8.8.8	192.168.2.3	0xbb15	No error (0)	www.uniaoquimica.com.br		179.188.52.129	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:04.736285925 CET	8.8.8.8	192.168.2.3	0x486b	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:06.235857964 CET	8.8.8.8	192.168.2.3	0x202e	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:06.317971945 CET	8.8.8.8	192.168.2.3	0x91f9	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:12.261549950 CET	8.8.8.8	192.168.2.3	0x6470	No error (0)	s2.conveythis.com		45.63.41.34	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:14.654966116 CET	8.8.8.8	192.168.2.3	0xc09c	No error (0)	d335luupugsy2.cloudfront.net		54.230.182.204	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:14.654966116 CET	8.8.8.8	192.168.2.3	0xc09c	No error (0)	d335luupugsy2.cloudfront.net		54.230.182.63	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:14.654966116 CET	8.8.8.8	192.168.2.3	0xc09c	No error (0)	d335luupugsy2.cloudfront.net		54.230.182.73	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 12:38:14.654966116 CET	8.8.8.8	192.168.2.3	0xc09c	No error (0)	d335luupugsy2.cloudfront.net		54.230.182.56	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:25.427066088 CET	8.8.8.8	192.168.2.3	0x7cd2	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:29.329967022 CET	8.8.8.8	192.168.2.3	0x818b	No error (0)	translate.google.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:29.329967022 CET	8.8.8.8	192.168.2.3	0x818b	No error (0)	www3.l.google.com		142.251.143.110	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.800760031 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	stats.g.doubleclick.net		142.250.153.154	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.800760031 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	stats.g.doubleclick.net		142.250.153.156	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.800760031 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	stats.g.doubleclick.net		142.250.153.155	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:29.800760031 CET	8.8.8.8	192.168.2.3	0xbf58	No error (0)	stats.g.doubleclick.net		142.250.153.157	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.184017897 CET	8.8.8.8	192.168.2.3	0xd859	No error (0)	googleads.g.doubleclick.net		142.251.143.130	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.284811020 CET	8.8.8.8	192.168.2.3	0xf8da	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:30.284811020 CET	8.8.8.8	192.168.2.3	0xf8da	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:30.408044100 CET	8.8.8.8	192.168.2.3	0xae30	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:30.408044100 CET	8.8.8.8	192.168.2.3	0xae30	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:30.710609913 CET	8.8.8.8	192.168.2.3	0x4b61	No error (0)	www.google.co.uk		142.251.143.99	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:31.009038925 CET	8.8.8.8	192.168.2.3	0x653a	No error (0)	region1.analytics.google.com		216.239.34.36	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:31.009038925 CET	8.8.8.8	192.168.2.3	0x653a	No error (0)	region1.analytics.google.com		216.239.32.36	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:31.739311934 CET	8.8.8.8	192.168.2.3	0xdba8	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:34.261548042 CET	8.8.8.8	192.168.2.3	0x57e6	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:34.261548042 CET	8.8.8.8	192.168.2.3	0x57e6	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:35.202302933 CET	8.8.8.8	192.168.2.3	0xc343	No error (0)	pageview-notify.rdstation.com.br	k8s-production.rdops.systems		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:35.202302933 CET	8.8.8.8	192.168.2.3	0xc343	No error (0)	k8s-production.rdops.systems		35.223.116.65	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:36.674926043 CET	8.8.8.8	192.168.2.3	0xfede	No error (0)	popups.rdstation.com.br	pages.rdstation.com.br		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:38:36.674926043 CET	8.8.8.8	192.168.2.3	0xfede	No error (0)	pages.rdstation.com.br		34.68.90.188	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:38:40.011482000 CET	8.8.8.8	192.168.2.3	0x6dd	No error (0)	www.uniaoquimica.com.br		179.188.52.129	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.711034060 CET	8.8.8.8	192.168.2.3	0xf37e	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false

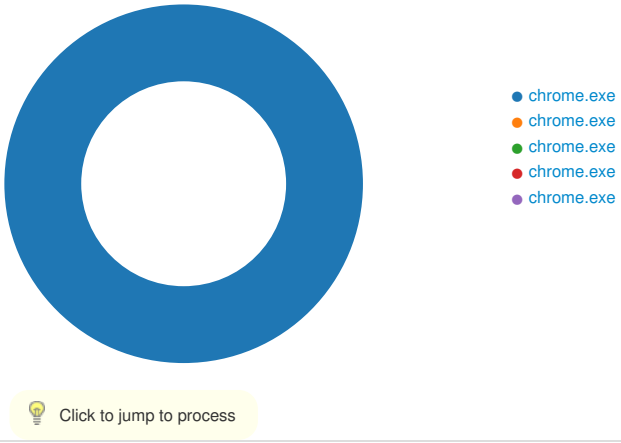
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 3, 2022 12:39:03.711034060 CET	8.8.8.8	192.168.2.3	0xf37e	No error (0)	youtube-ui.l.google.com		142.251.143.110	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.711034060 CET	8.8.8.8	192.168.2.3	0xf37e	No error (0)	youtube-ui.l.google.com		142.251.143.142	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.711034060 CET	8.8.8.8	192.168.2.3	0xf37e	No error (0)	youtube-ui.l.google.com		142.251.143.174	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.711034060 CET	8.8.8.8	192.168.2.3	0xf37e	No error (0)	youtube-ui.l.google.com		142.251.143.206	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:03.940387964 CET	8.8.8.8	192.168.2.3	0x95d8	No error (0)	www.uniaoquimica.com.br		179.188.52.129	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:04.840506077 CET	8.8.8.8	192.168.2.3	0x503f	No error (0)	www.google.com		142.251.143.132	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:09.939060926 CET	8.8.8.8	192.168.2.3	0x4d12	No error (0)	static.doubleclick.net		142.251.143.102	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.926064968 CET	8.8.8.8	192.168.2.3	0x95d3	No error (0)	yt3.ggpht.com	photos-ugc.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:39:18.926064968 CET	8.8.8.8	192.168.2.3	0x95d3	No error (0)	photos-ugc.l.googleusercontent.com		142.251.143.161	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.938695908 CET	8.8.8.8	192.168.2.3	0x7543	No error (0)	i.ytimg.com		142.251.143.118	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.938695908 CET	8.8.8.8	192.168.2.3	0x7543	No error (0)	i.ytimg.com		142.251.143.150	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.938695908 CET	8.8.8.8	192.168.2.3	0x7543	No error (0)	i.ytimg.com		142.251.143.182	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:18.938695908 CET	8.8.8.8	192.168.2.3	0x7543	No error (0)	i.ytimg.com		142.251.143.214	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:42.766096115 CET	8.8.8.8	192.168.2.3	0x68dc	No error (0)	pageview-notify.rdstation.com.br	k8s-production.rdops.systems		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:39:42.766096115 CET	8.8.8.8	192.168.2.3	0x68dc	No error (0)	k8s-production.rdops.systems		35.223.116.65	A (IP address)	IN (0x0001)	false
Nov 3, 2022 12:39:44.308655977 CET	8.8.8.8	192.168.2.3	0xb169	No error (0)	popups.rdstation.com.br	pages.rdstation.com.br		CNAME (Canonical name)	IN (0x0001)	false
Nov 3, 2022 12:39:44.308655977 CET	8.8.8.8	192.168.2.3	0xb169	No error (0)	pages.rdstation.com.br		34.68.90.188	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- www.uniaoquimica.com.br
- https:
  - s2.conveythis.com
  - d335luupugsy2.cloudfront.net
  - translate.google.com
  - stats.g.doubleclick.net
  - googleads.g.doubleclick.net
  - connect.facebook.net
  - www.google.com
  - www.google.co.uk
  - region1.analytics.google.com
  - www.facebook.com
  - pageview-notify.rdstation.com.br
  - popups.rdstation.com.br
  - www.youtube.com
  - static.doubleclick.net
  - i.ytimg.com
  - yt3.ggpht.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **5920**, Parent PID: **2136**

General

Target ID:	0
Start time:	12:37:58
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:	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: **6068**, Parent PID: **5920**

General

Target ID:	1
Start time:	12:37:59
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=1936 --field-trial-handle=1620,i,1061722878761419402 7,5335811723259235483,131072 --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: **4768**, Parent PID: **2136**

General

Target ID:	2
Start time:	12:38:00
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.uniaoquimica.com.br/
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

Analysis Process: chrome.exe PID: **6412**, Parent PID: **5920**

General

Target ID:	12
Start time:	12:39:26
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=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=6660 --field-trial-handle=1620,i,10617228787614194027,5335811723259235483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **6016**, Parent PID: **5920**

General

Target ID:	13
Start time:	12:39:26
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=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=6636 --field-trial-handle=1620,i,10617228787614194027,5335811723259235483,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff745070000
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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly