ID: 778235
Cookbook: browseurl.jbs
Time: 09:07:06
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://t.co/d3aQAddN4Z?ssr=true 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 11
Public IPs 11
Private 12
General Information 12
Warnings 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 13
Network Behavior 13
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: chrome.exePID: 5996, Parent PID: 2300 14
General 14
File Activities 14
Registry Activities 14
Analysis Process: chrome.exePID: 3388, Parent PID: 5996 14
General 14
File Activities 15
Analysis Process: chrome.exePID: 1212, Parent PID: 2300 15
General 15
Registry Activities 15
Analysis Process: chrome.exePID: 5204, Parent PID: 5996 15
General 15
Analysis Process: chrome.exePID: 5256, Parent PID: 5996 16
General 16
File Activities 16
Registry Activities 16
Disassembly 16

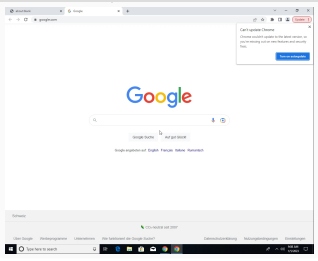
Windows Analysis Report

https://t.co/d3aQAddN4Z?ssr=true

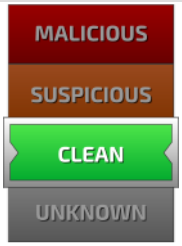
Overview

General Information

Sample URL:	http://https://t.co/d3aQAddN4Z?ssr=true
Analysis ID:	778235
Infos:	



Detection

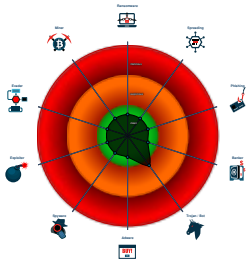


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

HTTP GET or POST without a user …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5996 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 3388 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=1824 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5204 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=6684 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5256 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=3984 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 1212 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://t.co/d3aQAddN4Z?ssr=true 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

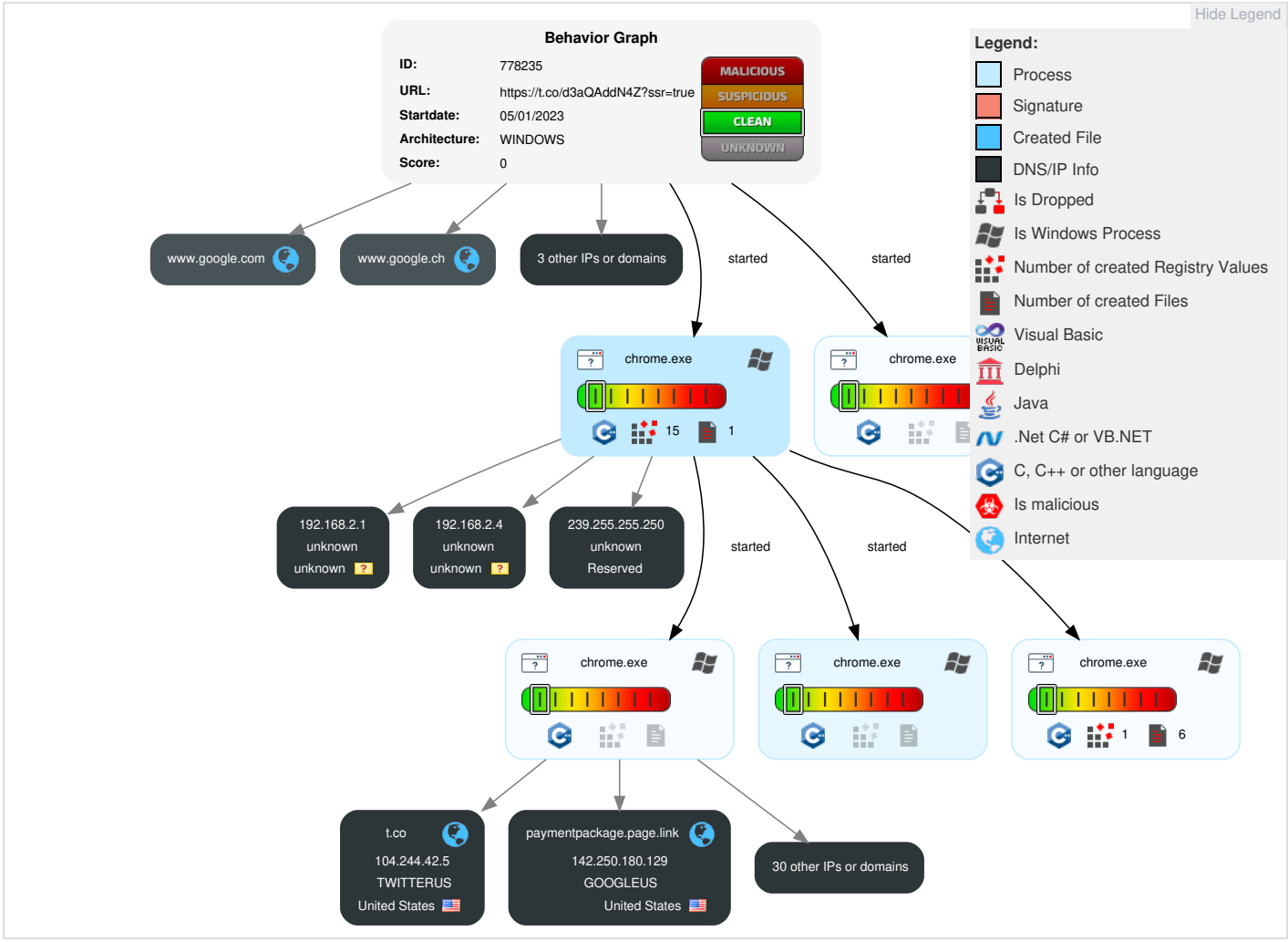
Joe Sandbox Signatures

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

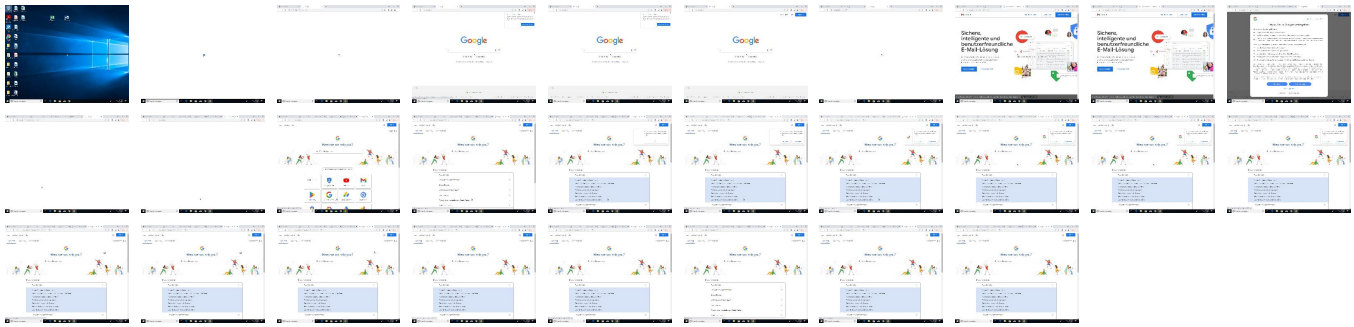
Behavior Graph

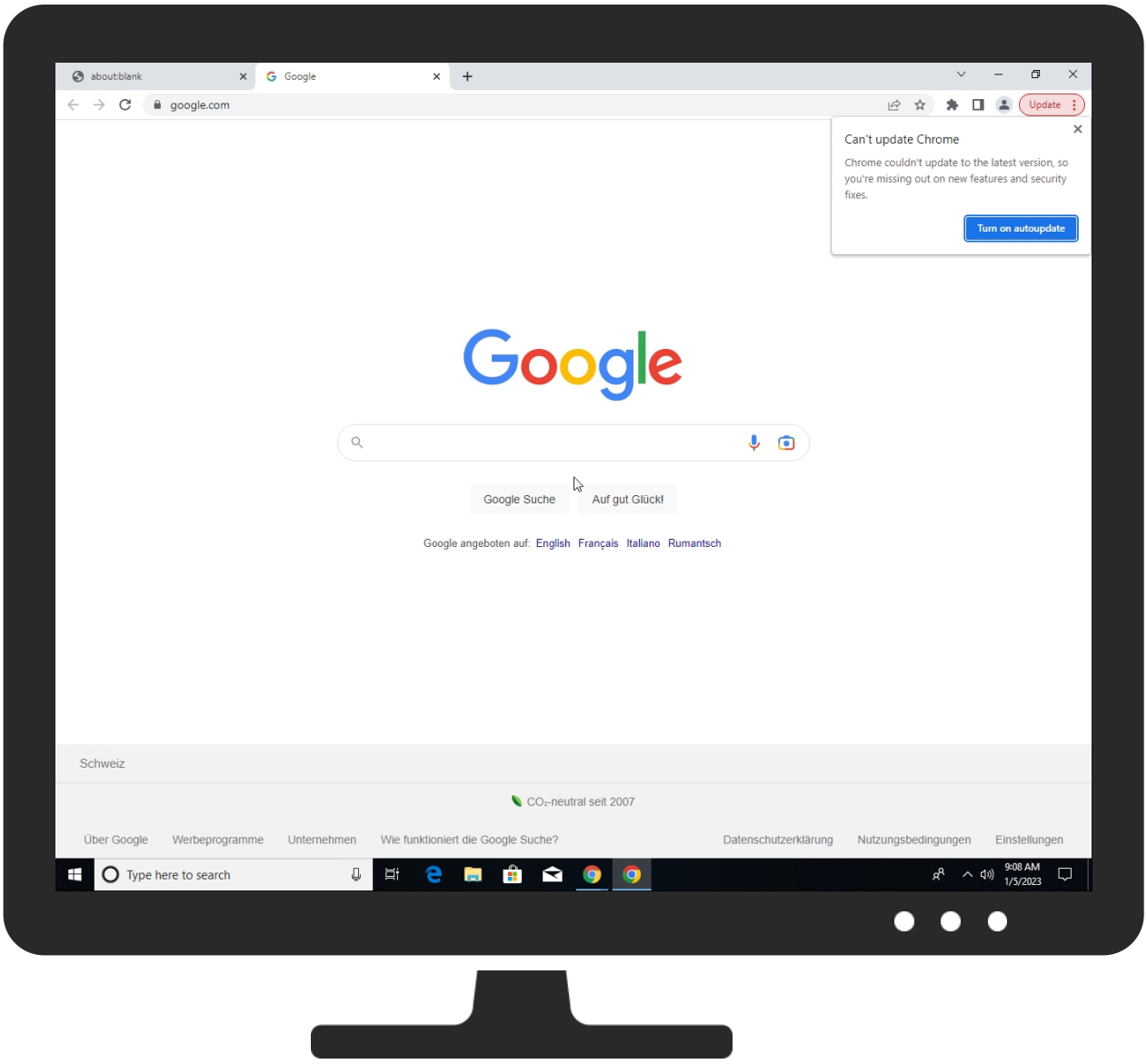


Screenshots

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://https://t.co/d3aQAddN4Z?ssr=true	0%	Virustotal		Browse
http://https://t.co/d3aQAddN4Z?ssr=true	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://about.google/products/	0%	URL Reputation	safe	
http://https://about.google/assets-products/img/glue-icons.svg	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://about.google/favicon.ico	0%	URL Reputation	safe	
http://https://about.google/assets-products/img/glue-google-color-logo.svg	0%	URL Reputation	safe	
http://https://about.google/assets-products/img/glue-google-solid-logo.svg	0%	URL Reputation	safe	
http://https://www.frohn-sanitaetshaus.de/wp-admin/user/sudafric/manage/pay.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scone-pa.clients6.google.com	142.251.209.10	true	false		high
csp.withgoogle.com	142.250.180.145	true	false		unknown
accounts.google.com	142.251.209.13	true	false		high
plus.l.google.com	142.251.209.46	true	false		high
i.ytimg.com	142.250.184.118	true	false		high
www.frohn-sanitaetshaus.de	178.77.76.15	true	false		unknown
mail.google.com	142.250.180.165	true	false		high
support.google.com	142.250.184.78	true	false		high
paymentpackage.page.link	142.250.180.129	true	false		unknown
adservice.google.com	142.250.180.162	true	false		high
static.doubleclick.net	142.250.180.166	true	false		high
about.google	216.239.32.29	true	false		unknown
stats.g.doubleclick.net	142.251.31.156	true	false		high
youtube-ui.l.google.com	142.250.180.174	true	false		high
t.co	104.244.42.5	true	false		high
play.google.com	142.251.209.46	true	false		high
www3.l.google.com	142.250.184.78	true	false		high
googleads.g.doubleclick.net	142.250.180.130	true	false		high
ghs-svc-https-sni.ghs-ssl.googlehosted.com	142.250.184.83	true	false		unknown
photos-ugc.l.googleusercontent.com	142.250.180.161	true	false		high
www.google.com	142.250.184.36	true	false		high
clients.l.google.com	142.250.184.78	true	false		high
www.google.ch	142.251.209.35	true	false		high
googlehosted.l.googleusercontent.com	142.250.184.65	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
www.blog.google	unknown	unknown	false		high
ogs.google.com	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
apis.google.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://apis.google.com/js/googleapis.proxy.js?onload=startup	false		high
http://https://lh3.googleusercontent.com/2noIz2X2ov5fXwxhW8AbSDnLpp8tT3ml3-iV_OQ2UOwX_EhIBBgip7FPRs10DYmPKinVM98Qkjr1uN3BhQ3StGXCp1-O_wPwoLZeDQ=rw-e365-w2880	false		high
http://https://www.google.com/js/th/ayf-ZXn06Q-bf2kvL7HvZn-6GmgIdMcaNWCzb_-s5mI.js	false		high
http://https://lh3.googleusercontent.com/FU-s_R5k9ZDky6RTNWsdrN8xa9Jp7C2mwd_Kj9NHQe6Cw_EipUIFLjv0L7fGBh7KloVVACyAI7AIaXMC_bPGKVkX6aebI-4f-UurLRbk	false		high
http://https://lh3.googleusercontent.com/dMQ1Q4xlLrl3-KsZvX_9v56emij4OkRxzapLM7RSuZVd7PgqfjPxKR4KY8hVHYXqP2ZkS-_ZueXb9ywW66H2oCyTgIApr1ELCy3woOAviTgFP6uyAd0=h120	false		high
http://https://lh3.googleusercontent.com/vnSr97Bu2sI2_h334BHmEn1zTPrtv0hM9MLn3YxkN6JVzmir_VH62GiPIKfwtPBTOQ8xH0XNI40xfPAYbwbJEU-1jG09ovlU0f4S1Q=h120	false		high

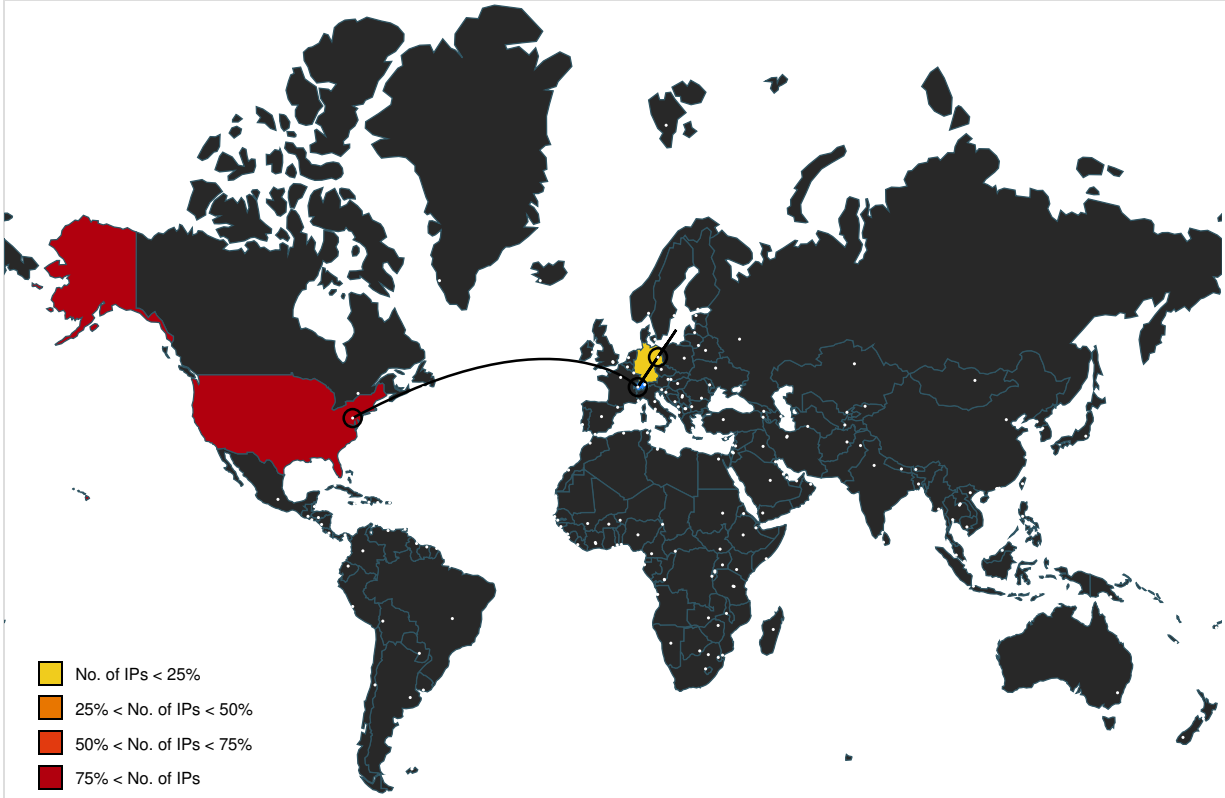
Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/fz3K-mqQSYE1C7OPtUEXqiyvtHS6vy8ZyNzdDIm2f3RaXR6jPMfakJgEdty-I5NIJe--oUqeAp9u8u3cg4QN07motgAiN-2U-mYEWgkU56yaKJqYbw	false		high
http://https://www.google.com/gmail/about/static-2.0/css/partials/faq.css?fingerprint=392991776b78fd091779006c96b7384b	false		high
http://https://lh3.googleusercontent.com/NksFVpnLFiAE4YKEh9n84ebvfznogwh0AyAUDpmpLqpBP7h791LS9RcIzWpE8XfsiR0NJiHomxV8FyVO2ccMF2VzB_L3omeUWuHu9d3LGJ4Ww6JKviev	false		high
http://https://lh3.googleusercontent.com/tUfd9tmqYw7QFa0Nnpde9SawF7tIAhwDw_ZM5YwuG0FmBTzjStOVQu1In41aEdg0FoXcXYEVk4L_FQDbPrXsJy-sg1BMEkU14M89=h120	false		high
http://https://lh3.googleusercontent.com/VdXRrd_xoiTD2oe-7FBLg5HOxC0evZYSk9glkZ9etAT5LNvCfL4tPySadjV9l32Y73wAauBLo6HCv4yTX7G9SYE8NG5-LFwNVBpfZw=h120	false		high
http://https://lh3.googleusercontent.com/YqGm39Z5sh9A5xtQbH_iZFAKj6kwCkY447q5cjzGcb85qccGrZn5xO_N_XwKpx1nd3XA-l6tJyz2qk7Xxk8ThS1-W78mBoEfPVKF4hm4=rw-e365-w2880	false		high
http://https://lh3.googleusercontent.com/yfNHOlqQb-_BbTsGZle4fmncMyM2kTjYQzub_Hucf27LCQPNwJiqiOMr39an6X_yB3gCKVExXGgtYm1morm8jkXY53W8h75Z0nUepg=h120	false		high
http://https://www.google.com/gen_204?atyp=i&ei=ZYW2Y5iLE9eH8gLrv7agCg&dt19=2&zx=1672938486460	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.WEPncdil2Uw.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo-eOecLLtOXEl3I3kIuMsKXRkDMmA/cb=gapi.loaded_0?le=scs	false		high
http://https://lh3.googleusercontent.com/z3dgQsXgGqfadzIUmpGI_ppolUy7H6fgqIbtW_qzLXcBww0nOby8TEE3e_fW84Qa7zeAwe339f5VLkqRD6jk7Z9sEaVh5Y_yaPG9nw=h120	false		high
http://https://www.youtube.com/embed/KKfAuQrwzTY?rel=0&vq=hd720&start=0&cc_load_policy=1&playsinline=1&origin=https%3A%2F%2Fabout.google&enablejsapi=1&widgetid=3	false		high
http://https://lh3.googleusercontent.com/PWXM4hp9lRRezHTV86SqLwhRQMz4_Lk08jll3GkWBvBZy_Uk6kvUvwIrVilwaIW2mHZJoccchG6o9a5UdOJEwQPf9oJGmOGSglo3VW0=rw-e365-w2880	false		high
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://www.google.ch/imghp?hl=de&ogbl	false		high
http://https://lh3.googleusercontent.com/kQDv-46ToDkqXJ2DIlr7hKXKalQvL0NJy4oGIhNlUkxX95btXayCKNoZuaY_KT-6U8-Iz35FlDZXRd1U3bNFo99a3k0-vwIIbtElStTKYwD_UxNkjA	false		high
http://https://lh3.googleusercontent.com/gcivdVV-tvxWnRUDNOUocQhsZmT9Was6CexDLkqmigkLzk5ZcNjqcgj3q4UROg4b1xbj63W94SONQIU2n3nBSa1qTQQX1SbJj_tQLR0	false		high
http://https://lh3.googleusercontent.com/4Ae0zBYFQOJlGcRaDFUatVMPtUP7L-EcbwRa2p1o2tD5xISasgZmgKCgfIyMVYcsUPs5YHOUsDfy8T07EPP7mvL8h9NhmnVbRpOKq4v7jXLZ6yzVHN0q	false		high
http://https://www.youtube.com/s/player/e5f6cbd5/fetch-polyfill.vflset/fetch-polyfill.js	false		high
http://https://www.youtube.com/s/player/e5f6cbd5/player_ias.vflset/en_US/remote.js	false		high
http://https://www.google.com/gen_204?atyp=i&ct=psnt&cad=&nt=navigate&ei=ZYW2Y5iLE9eH8gLrv7agCg&zx=1672938486874	false		high
http://https://i.ytimg.com/vi/ne8De4m_SbE/mqdefault.jpg	false		high
http://https://lh3.googleusercontent.com/zRGXRSFD6qZikPYwqGIAYh9gaBIR1Byc837RMp1yCsirHxy3I2Ciwf8Wndw3iWcDqOnDkFU8HE-E9i3YVITG115o4_QhRmfHdJGGdw=h120	false		high
http://https://lh3.googleusercontent.com/KH3C4y2owNGLC1dCMI0oFaTCpZP0t3veS_oVM0vTHW8_A4jFa7lhuXqyzG88fovna8OLY6_RHzjPAuoNnRXLjQ5m2KeEoQM8Gg79lq29KflJPgCaRSc=w1440-l90-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/Q4UDu0hKQgAyUzO0RpJTpTKc2DyaZbU-K96JCJjqKd9_ABetMMpS6LxO6Y7Ypm2CVhCro4n4n9PTF97SlwrSjmJFaHdV-_yDr8MpX1M=h120	false		high
http://https://lh3.googleusercontent.com/rFIOGuWFGvTm427OcRlhQIeB1SqlCZkVh7N7F-q8Rm6b_mtlUebqvFmXHCkvLuV8ebUiIRlQXbg_ujAXlJ9wg02s7L36Us66yyIAotc	false		high
http://https://lh3.googleusercontent.com/WdC-o7ZcZL5WALPSmfUC8H4oYhlhqm1DV45CtHqV06DTRR0rE_P9JXi-J2KXLd9CTyHt_t3ehUm1o_AMltgfAGbvQDku8jsZt0kBSA=h120	false		high
http://https://lh3.googleusercontent.com/gi7EU_u6liuIRSxunfy5LLqsEJrC08L12aufZc3rP_w8hD8ouiVW89vfe7pTQrSsLXQYyQvnlhBfarK9Ul33ccQOSqKgK3i6iyArwg=h120	false		high
http://https://lh3.googleusercontent.com/RwVe2Cm1EjeDmYhdTzr179G0ovq_PCxgPzQ92PO-YxTBEFTHWh0L6Ev8FFDWRgRGrE81vwn95tyg9Ey189OO4kllhhpLAMIsGFZ-UKA=h120	false		high
http://https://mail.google.com/intl/de/mail/help/about.html	false		high
http://https://www.google.ch/imghp?hl=de&ogbl	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/9LNPff6rAyFvnqKt8TeIKttGeivF94FziDoAqo4qLU0jrOAE23M1Fpz3-dRrqGWp-vRqcq-7BkXeAO90iSo3lxY-nhR3YnGwcGlHz-WS-4Pfomn3	false		high
http://https://www.google.com/intl/de/mail/help/about.html	false		high
http://https://www.google.com/gen_204?s=webhp&t=aft&atyp=csi&ei=ZYW2Y5iLE9eH8gLrv7agCg&rt=wsrt.2127,aft.337,afti.337,cbt.91,prt.247&wh=913&imn=3&ima=1&imad=0&imac=2&aftp=913&bl=5roH	false		high
http://https://about.google/assets-products/img/glue-icons.svg	false	• URL Reputation: safe	unknown
http://https://www.google.com/gen_204?use_corp=on&atyp=i&zx=1672938551029&ogsr=1&ei=pIW2Y77QNJWDur4PqqidwAo&ct=7&cad=ed&id=19022645&loc=undefined&prid=117&ogd=ch&ogprm=up&ap=1	false		high
http://https://lh3.googleusercontent.com/9NuRdiRepVl3n1txfg7Ky2wWzB3DvXkWABXeFMSn2tzDYYkv8T_RMA9R17fWi0ziUDIDTVJx0JruCzOev37c4dkK9Wrgkeyam3pM8ll=h120	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.de_CH.ZwbqFKinE5Y.O/am=AAFUEKAAcAAAgAAACAAkQAAAAAAAAEACAEQDBUyYAAUAeEIMBsEwCQABAEKEfIgAAGAAMYDEAEAAAAAD5AxDwBAAMJiwAAAAAAAAAgIAICAY3SFAQAAIAAAAAAABQSpMXB4AgCA/d=1/ed=1/dg=2/br=1/rs=ACT90oFOagiyKkJ2j8FQ5HG7O2TZtIZvsQ/m=cdos,dpf,hsm,jsa,d,csi	false		high
http://https://lh3.googleusercontent.com/6nGdwtbmSCuuGF5fSCqvv0f-GOsp927ZXRFxC1NNEqlH-EwAGEqlHXN2rcarUTB7C8Tj8shbcg-9z-CO4XJGTVSaLbT5FPsq0rKET0ZlfWNsj9_f424=h120	false		high
http://https://lh3.googleusercontent.com/hcfrojgqkbroG2ScJ_n6ofwCdSOkC6Uk-NPWaI_0zQuyKcQrNTgoZpe4bbtJOFuI0Sir0JkrQrKAEhlPbiAnM8v9Hr8xtP47T4saBg=h120	false		high
http://https://www.google.com/favicon.ico	false		high
http://https://lh3.googleusercontent.com/XfxlbB7Imi28_w277XeVC0u8Yngn8e1bQxhd6YK2snOdqt_uiwripgSEl5VNxgS2cJP2kf0dHv6LfSq8AG6YeJf9cpu1BE1kP36R=h120	false		high
http://https://lh3.googleusercontent.com/moWtYpo1G3n-1QfF5rNSy7n2IIQs785-H9DStefngR0kWMsmnPkzMu-SKH3eUxHVddekMttIA5olrn_wo3p50z04NyRZYPHYBc2cxvE=h120	false		high
http://https://lh3.googleusercontent.com/2qz9gwasYkOhPEumfqd3_x8HiiRu6fIQR1d-1DRAV8qfkqmQx7Rygzohal7DXbB-urTun2B0thBnpY3BRfqXnJOm4b9QQFk3L4VK=h120	false		high
http://https://i.ytimg.com/vi_webp/5amGvnxGO54/maxresdefault.webp	false		high
http://https://about.google/favicon.ico	false	• URL Reputation: safe	unknown
http://https://support.google.com/websearch/?hl=en#topic=3378866	false		high
http://https://www.youtube.com/s/player/e5f6cbd5/www-embed-player.vflset/www-embed-player.js	false		high
http://https://lh3.googleusercontent.com/Jqo0sXz5HJpnbEwCf5qwcWSbwXbKiivjx2e1WpRjAg3pAPaj2DiOHs42I1zwyhvtXdHwTuGYXQWkNMIYGGUnXT5fiSbnwlVB1WYhdg=h120	false		high
http://https://www.google.com/intl/de/gmail/about/	false		high
http://https://lh3.googleusercontent.com/gRnEKp2-zZSQepcLE4cSa3IdUqkZBTlvmWnmaYdPh9ERKmjx02WLRWxJMALPOGlwQEl4FgQZcogJERKTDx1JrZLVbdg_---gFavOqw=h120	false		high
http://https://lh3.googleusercontent.com/6xlGJ-dkwosfUisVYzRKNE1Wcr5QDDfRfZ4bXktF-Nn0J0ucHd_JI1wjXTls7lt5mvJvvcvtrNc0MESF98dAx6ivasEsZNxoaUZU-Q=h120	false		high
http://https://lh3.googleusercontent.com/sq57GaRCOEk-TcLHr8ZeehZOkRrOLLv0ZIL34gOO2TNqeQjAcLqZM_YvwoZCLFQbW1DS0K28QakL4JTKArVVV4pp-PtTltns7K25Pu5d7v-6dRSh-g=w1440-l90-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/oTsTVqWan-UskrnBTBexES9-OwwuQnoV4EtEk3t1Ywt9SZJZp24pdRXbrp0YEalXW_eyFSKSVFEgoMwKcGRbsM6HnxfJbr4RWNAvNxw=h120	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.de_CH.ZwbqFKinE5Y.O/ck=xjs.s.-bBqenOyPv8.L.W.O/am=AAFUEKAAcAAAgAAACAAkQAAAAAAAAEACAEQDBUyYAAUAeEIMBsEwCQABAEKEfIgAAGAAMYDEAEAAAAAD5AxDwBAAMJiwAAAAAAAAAgIAICAY3SFAQAAIAAAAAAABQSpMXB4AgCA/d=1/exm=DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,aa,abd,async,cdos,csi,d,dpf,epYOx,hsm,jsa,mu,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch/ed=1/dg=2/br=1/rs=ACT90oENeooOvR7HaOl9p2vF8jxkzEPNvg/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:COQbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:U4MzKc;wQlYve:aLUfP;kbAm9d:MkHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;YV5bee:IvPZ6d;dtl0hd:ILQWFe;yGxLoc:FmAr0c;dIoSBb:ZgGg9b;pXdRYb:JKoKVe;wR5FRb:TtcOte;KpRAue:Tia57b;aZ61od:arTwJ;JXS8fb:Qj0suc;rQSrae:C6D5Fc;qavrXe:zQzcXe;UDrY1c:eps46d;w3bZCb:ZPGaIb;VGRfx:VFqbr;imqimf:jKGL2e;Np8Qkd:Dpx6qc;BjwMce:cXX2Wb;oGtAuc:sOXFj;NPKaK:PVlQOd;EmZ2Bf:zr1jrb;daB6be:lMxGPd;Fmv9Nc:O1Tzwc;hK67qb:QWEO5b;b0fxEe:YZBsef;R4IIIb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;kCQyJ:ueyPK;okUaUd:wItadb;GleZL:J1A7Od;x8qzwe:C7TSxd;RdFZ3b:xdTsF;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;Pguwyb:Xm4ZCd;VN6jIc:ddQyuf;SLtqO:Kh1xYe;VxQ32b:k0XsBb;DULqB:RKfG5c;bcPXSc:gSZLJb;cFTWae:gT8qnd;gaub4:TN6bMe;hjRo6e:F62sG;whEZac:F4AmNb;qddgKe:x4FYXe;eBAeSb:Ck63tb;vfVwPd:OXTqFb;w9w86d:dt4g2b;lkq0A:Z0MWEf;KQzWid:mB4wNe;pNsl2d:j9Yuyc;eHDfl:ofjVkb;Nyt6ic:jn2sGd;SNUn3:x8cHvb;LEikZe:byfTOb,lsjVmc;io8t5d:sgY6Zb;j7137d:KG2eXe;Oj465e:KG2eXe;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=CnSW2d,DPreE,WINQGd,fXO0xe,kQvlef,nabPbb?xjs=s2	false		high
http://https://lh3.googleusercontent.com/hHWA5otDm9mYUJdAqTjo7wBWj8euY-SdEhCffO7oQzG3zpzxm-YExt1VDB8X6_5gchW_Ye3bfhOJXyOWgcUr94GtgqltKP4IxiH02O-Xzw5A1IHsxiw=h120	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/vNgpLTvnDUr6-QM8s4OuuESGDXs_brbGoPR-7vfwdxQl7M4MVFV0CC_Hil4qRDSp4P66ik85fdv09jKn89kDAJVknIbd6wkl0zGQJQ=h120	false		high
http://https://lh3.googleusercontent.com/8-8c0-eOE_lwNBcLp9SQGZ0r51WUGA8EFf9Uc8CG2TTtdXVVfxFSiFLUx4LOgroKU5M9DCm3aFCYgkcXDPYb7NpKZkH7ttQGwzPFEAA=h120	false		high
http://https://lh3.googleusercontent.com/J-V0oji6tedu_ZNhQxcwCBWfIl6Lu4HmbEAsRyYxU0LhuYpaJj9gxMahPVHbrMEOFe7NTTjoJOTTtLtBoAtWMz1hRN5a2CHWlG01dP3j0YYHw6XUScHP=w600-l80-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/xeVlvzZX32eg9zc9V7MLUWaEeOnwoa5OQfrgI10U4ub8QA6iwdq1TgcOpLTBiKQTosiNxtMBtpOvh_z7fq7eoISf53UZqZMd0dZR0gSLAAMFkK9vVfQ	false		high
http://https://lh3.googleusercontent.com/Cle-1GLl4P8zbJafbrnN8-7CgfVSduAR1j2DACNepAm5JL37GANl8tIM1h72Cyga71wO2lGcNPONnQl5MKFi_1TGSBQM8mV9qaKdQw=rw-e365-w2880	false		high
http://https://www.google.com/complete/search?q&cp=0&client=gws-wiz&xssi=t&hl=de-CH&authuser=0&psi=ZYW2Y5iLE9eH8gLrv7agCg.1672938485835&nolsbt=1&dpr=1	false		high
http://https://lh3.googleusercontent.com/Gv2bjAdDXiaD0ZvvA3ppmC905aIYb4EAVLUkRbYSUvHWepf6G9G4-k_9fNVogA7bmc8qjr9z8V5bLcfo8iBR7SKqaH8kBn3P1hi_tA=h120	false		high
http://https://support.google.com/websearch/?hl=en	false		high
http://https://lh3.googleusercontent.com/uzkOxzfGFGjzRx0FK6B541qcv469wNDTQf_TUu4oqH_oPUGJoajTkqHLJ9DD188Kmocg_DJg2OBf1FxyRc6MLK_gMFFRmm7n7XTreZU=h120	false		high
http://https://lh3.googleusercontent.com/wz7zNnjtq287NYmYMvqxQclQ8YkLJCtl1HtHbXYkLy8lQOeNUU1vPPIXI6BqlYW1iTHMyB4_RAMUzCTOc-O5RNGyoYN1FTSA93MJ=h120	false		high
http://https://lh3.googleusercontent.com/5CsRqfMEP1Rv-PPv9G4962lyEuvb4roSLJHJQWPbmCa51AmvynfoGfoKsKiS87QhX07xQMZAeLp8qoSy7CjVZkXJ1WapQiJkroCeJw=h120	false		high
http://https://about.google/assets-products/img/glue-google-color-logo.svg	false	• URL Reputation: safe	unknown
http://https://lh3.googleusercontent.com/vDsTCfe65gxBEgVg6o8wEUHAFWledbJfpFECgr-HiSjZ4PdpvOkZZpCX3-dsZVRtiEcoU_O_W9zA1ceI8WmLrJ1ZI1vVSTLNuUPlvNSKbB6FDJq2xXc	false		high
http://https://www.google.com/gmail/about/static-2.0/js/main.min.js?fingerprint=3013f65e4814d5914f9a24976b9493a1	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.WEPncdil2Uw.O/m=client/exm=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo-eOecLLtOXEl3l3kluMsKXRkDMmA/cb=gapi.loaded_1	false		high
http://https://www.google.com/client_204?&atyp=i&biw=1280&bih=913&dpr=1&ei=ZYW2Y5iLE9eH8gLrv7agCg	false		high
http://https://lh3.googleusercontent.com/nDCFKerWuvJvG26AZOPsWYFPiw3MRFDYqVJcHzQzK6AgY96TXH50bpQ1IE__BdBxxcXm8ZTaQ6OuJ4pbYF1c-ugOTfOmjhffJXEvJQ=h120	false		high
http://https://i.ytimg.com/vi/KKfAuQrwzTY/sddefault.jpg	false		high
http://https://lh3.googleusercontent.com/eO6nD1O47tirNw4TM76SfwotF_tP25t_TASE2l8_Gyw4xLr7ckkcg4PuEb8cxngaWwks2XZqVMT-et2ZGUU9W648mg7_hSfl6kv93uyvXvvjwCVzRXw=w600-l90-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/Oe2QYUUWNPyW_D_LI_dusuUymZNPTkO1yxx1j_61Wkv9nllw8APPCZEXKL3nCdqQGaAQVYC7ldr2WsYgrZ2doG7Gt2OnfimbNK5GSQ=h120	false		high
http://https://lh3.googleusercontent.com/aD5GNhlaU2d70gmSy5ioL1dMSUZN9cHDWPLkIBLhCsJ-BgcGUm-PD6o8XExZcx1i2iZV6PH0P8v3ceg0x7Tzd_OZ5FV0nXs5mX15sgA=h120	false		high
http://https://www.frohn-sanitaetshaus.de/wp-admin/user/sudafric/manage/pay.php	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/tC78k3bL_DjdIByD4HSnnblCZF0nlR599IWYDDghEJDn7dwg-tuOIXGVR1TwxePI063JTgu9NvrsvRutrqHOfR5AAWduD51R8zuswV8=h120	false		high
http://https://lh3.googleusercontent.com/qxRgIf3Uxj9_dZHnmBqqals8VdtoZxxj6ES8uS6TSmSqyxz5ROq_EYsUpwfsOwuLH0_cbJjLhxYDfeyhU9rTlTn6psVRO5hC-U-2jWg=h120	false		high
http://https://i.ytimg.com/vi/nvIXGeB1WgE/mqdefault.jpg	false		high
http://https://www.google.com/gmail/about/static-2.0/images/logo-gmail.png?fingerprint=c2eaf4aae389c3f885e97081bb197b97	false		high
http://https://lh3.googleusercontent.com/7Urnou3LIFcohl-pZtLtAZKIRy_aEmZd1yrcKmrgZXIAUPsHcriy5Spcn49cCZyz_MeqU13JTHtmStlJGAAWti1x-ZG4rgMhEH5O_w=h120	false		high
http://https://lh3.googleusercontent.com/mjVS_lzc6fGAvuaT0v--gb2so5mZvAbI5EUMUB41cWB7tpy81trBCR8rIlj8NoKgPzDWGN-Hs97NlW0T9W57YJ5z9A8QQWwXUYa_Zg=h120	false		high
http://https://lh3.googleusercontent.com/7j1-9AjGTjyFcEDU5lJw2BpZNYWNKgkxegHVv012Pm5OPBratN5ZsNVtpILRwXqE5Givogcj2VMswYdKR1dKvLvo2EQFSM0p7yTxYw=h120	false		high
http://https://lh3.googleusercontent.com/AJL2tHF75z0uJsFroqze8E1OZA6bysiaPcEpAv3XHPxURkfdfHQ1MCQmYEwhTJlT4_mEygCw4cpBkr6bMUQfQ8g-XxAjgDNwkF4t=h120	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://i.ytimg.com/vi/oIMTM168BK8/mqdefault.jpg	false		high
http://https://ogs.google.com/widget/callout?prid=19022645&pgid=1151720448&puid=723e1a40d4cc6173&cce=1&dc=1&origin=https%3A%2F%2Fsupport.google.com&cn=callout&pid=117&spid=117&hl=en	false		high
http://https://lh3.googleusercontent.com/O53jgarLMMs6WBjROWgvDFWD1SrzVxc3yLfpI8Lk7_2zUwmgzDi4T-y3QxFTABRkzXKG385ZSkknvOcbL0dt0S5XiAAqEzUO06gy6koJDSCxLERtlJw	false		high
http://https://lh3.googleusercontent.com/UqqZocZvjGksiGtlRkKb5NsuhpQkMLt3A85lMQ81Pms9tSZ3lLpymbAeinPIe5qUJRdmOKqL9InBBVsh6_gK-1QcNGppeUa7owoKgqo=h120	false		high
http://https://www.google.ch/gen_204?atyp=i&ct=bxjs&cad=&b=0&ei=e4W2Y7CqDM-Vxc8PxcSPiAM&zx=1672938506791	false		high
http://https://lh3.googleusercontent.com/Ucxl6g9AKLX3XmK7an_99LzivIJsXn5cvQdIMM_g4nNFZdULnGa4TH45WVIFu3vKd_c41R28NdjDzCEWgAwb5wjONbIPR4agLFUO1w=h120	false		high
http://https://about.google/assets-products/img/glue-google-solid-logo.svg	false	• URL Reputation: safe	unknown
http://https://www.google.com/manifest?pwa=webhp	false		high
http://https://lh3.googleusercontent.com/xDakliA_6hjirY-kSiTQFdrVRcRxYDMDdVWFOQtp97xidbk-At7EwGfV7YQqzSgbpfmpBw6etaT20SIzenYlyyretLrgN1PbR7_OTos=h120	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.180.129	paymentpackage.page.link	United States		15169	GOOGLEUS	false
142.251.209.13	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.209.35	www.google.ch	United States		15169	GOOGLEUS	false
142.250.180.161	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
178.77.76.15	www.frohn-sanitaetshaus.de	Germany		8972	GD-EMEA-DC-SXB1DE	false
142.250.180.166	static.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.180.145	csp.withgoogle.com	United States		15169	GOOGLEUS	false
142.250.180.162	adservice.google.com	United States		15169	GOOGLEUS	false
142.250.180.165	mail.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
142.250.184.78	support.google.com	United States		15169	GOOGLEUS	false
142.250.184.36	www.google.com	United States		15169	GOOGLEUS	false
142.251.31.156	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.244.42.5	t.co	United States		13414	TWITTERUS	false
142.251.209.46	plus.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.184.118	i.ytimg.com	United States		15169	GOOGLEUS	false
142.250.184.83	ghs-svc-https-sni.ghs-ssl.googlehosted.com	United States		15169	GOOGLEUS	false
142.250.180.174	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.250.180.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778235
Start date and time:	2023-01-05 09:07:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://t.co/d3aQAddN4Z?ssr=true
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@36/0@30/24
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://mail.google.com/mail/&ogbl • Browse: https://www.google.ch/imghp?hl=de&ogbl • Browse: https://www.google.ch/intl/de/about/products • Browse: https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAmgQ • Browse: https://www.google.com/setprefs?sig=0_cuxEtScnf6LDU09XfN6eN8u72ug%3D&hl=en&source=homepage&sa=X&ved=0ahUKEwjY0dTn_K_8AhXXg1wKHeufDaQQ2ZgBCBA

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 8.248.147.254, 8.248.143.254, 67.26.139.254, 8.238.85.254, 8.238.88.254, 142.250.184.35, 34.104.35.123, 142.250.184.99, 142.251.209.10, 142.251.209.42, 216.58.209.42, 142.250.184.42, 142.250.184.74, 142.250.184.106, 142.250.180.138, 142.250.180.170, 142.251.209.3, 142.250.184.104, 142.250.184.46, 216.239.34.36, 216.239.32.36, 142.250.180.176, 142.251.209.16, 142.251.209.48, 216.58.209.48, 142.250.184.48, 142.250.184.80, 142.250.184.112, 142.250.180.144, 142.250.184.67
- Excluded domains from analysis (whitelisted): fg.download.windowsupdate.com.c.footprint.net, fonts.googleapis.com, ssl.gstatic.com, fs.microsoft.com, content-autofill.googleapis.com, storage.googleapis.com, fonts.gstatic.com, ajax.googleapis.com, ctldl.windowsupdate.com, clientservices.googleapis.com, www.googleapis.com, jnn-pa.googleapis.com, wu-bg-shim.trafficmanager.net, region1.google-analytics.com, edgedl.me.gvt1.com, www.googletagmanager.com, gstatic.com, update.googleapis.com, www.gstatic.com, 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

No created / dropped files found

Static File Info

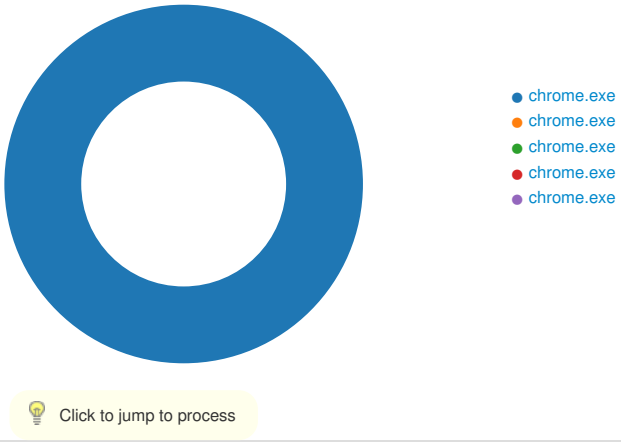
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5996, Parent PID: 2300

General

Target ID:	0
Start time:	09:07:57
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "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: 3388, Parent PID: 5996

General

Target ID:	1

Start time:	09:07:59
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1824 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --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: **1212**, Parent PID: **2300**

General

Target ID:	2
Start time:	09:08:00
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://t.co/d3aQAddN4Z?ssr=true
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: **5204**, Parent PID: **5996**

General

Target ID:	12
Start time:	09:09:23
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=6684 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --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: **5256**, Parent PID: **5996**

General

Target ID:	13
Start time:	09:09:23
Start date:	05/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=3984 --field-trial-handle=1688,i,2487878068628390314,14740040529577819228,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff68f300000
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