ID: 791289
Cookbook: browseurl.jbs
Time: 09:33:36
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

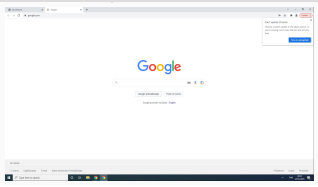
Windows Analysis Report

https://styleselect.com/vts0u

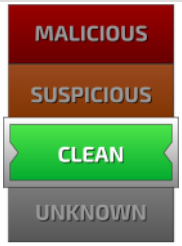
Overview

General Information

Sample URL:	http://https://styleselect.com/vts0u
Analysis ID:	791289
Infos:	



Detection

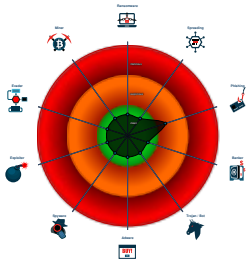


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- Uses insecure TLS / SSL version fo…
- No HTML title found

Classification



Process Tree

- **System is w10x64native**
- chrome.exe (PID: 4608 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 464953824E644F10FFDC9E093FD18F94)
  - chrome.exe (PID: 6564 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2012 /prefetch:8 MD5: 464953824E644F10FFDC9E093FD18F94)
  - chrome.exe (PID: 7236 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5044 /prefetch:8 MD5: 464953824E644F10FFDC9E093FD18F94)
  - chrome.exe (PID: 8196 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=video_capture --mojo-platform-channel-handle=6856 /prefetch:8 MD5: 464953824E644F10FFDC9E093FD18F94)
- chrome.exe (PID: 4264 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://styleselect.com/vts0u MD5: 464953824E644F10FFDC9E093FD18F94)
- **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

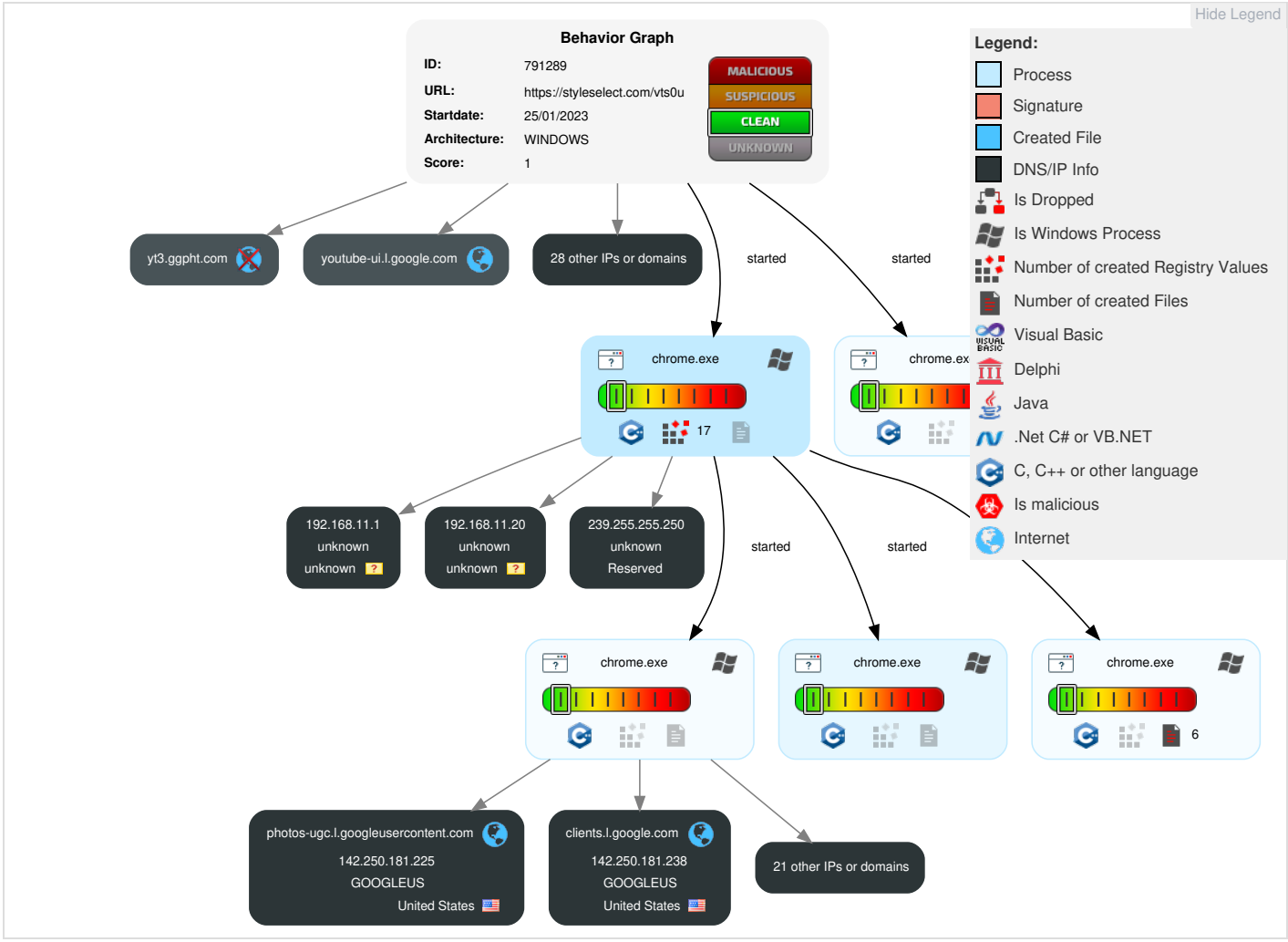
Joe Sandbox Signatures

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
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	1 Network Service Scanning	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	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

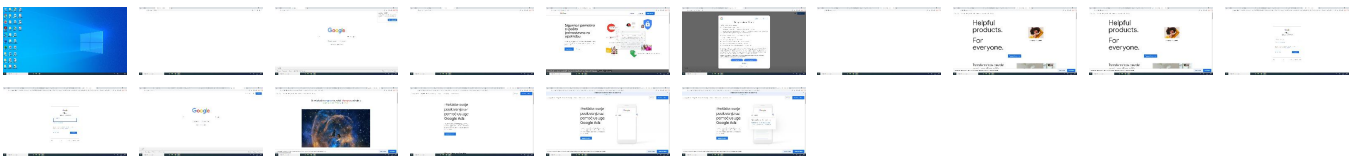
Behavior Graph

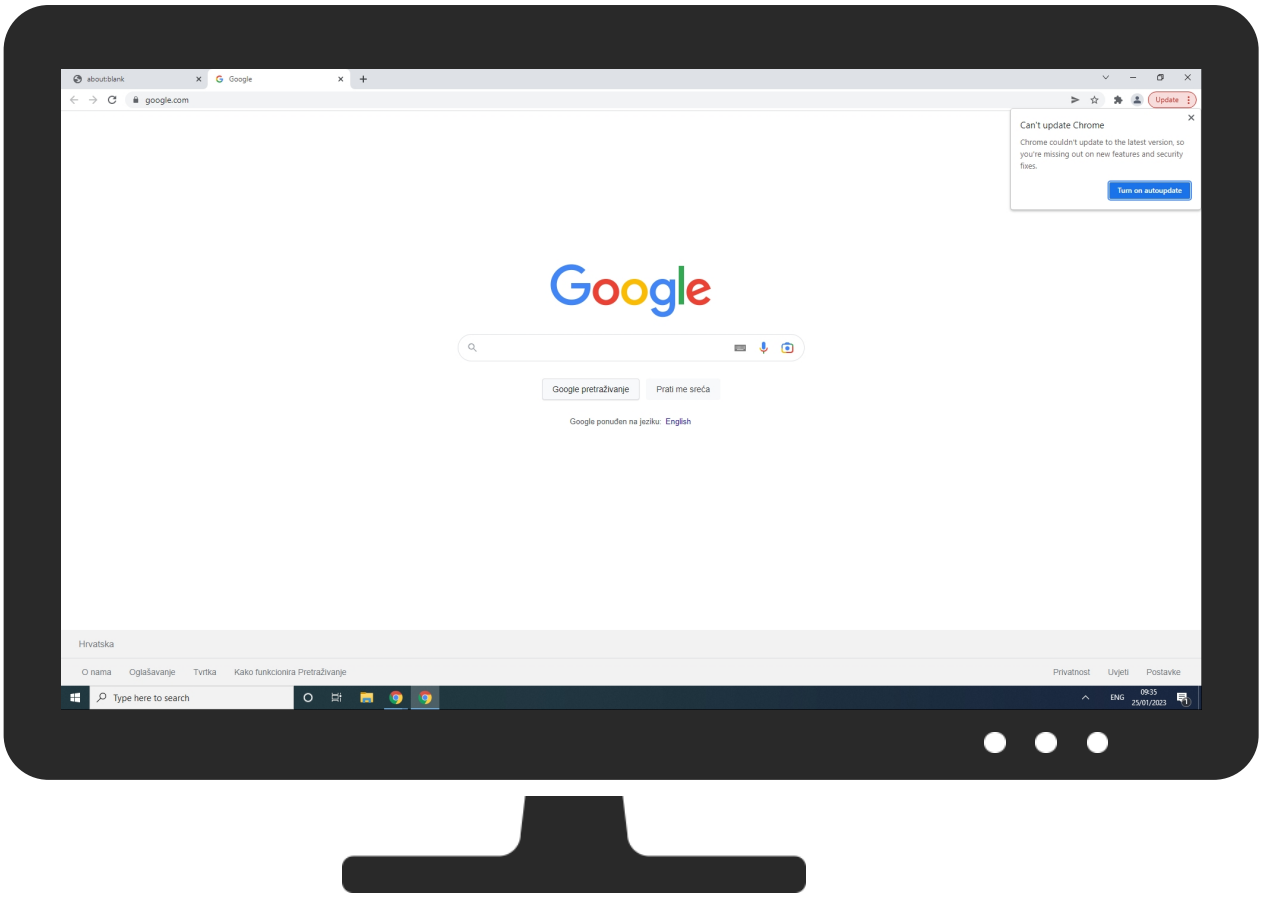


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://styleselect.com/vts0u	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
csp.withgoogle.com	0%	Virustotal		Browse
styleselect.com	0%	Virustotal		Browse
ghs-svc-https-sni.ghs-ssl.googlehosted.com	0%	Virustotal		Browse
about.google	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://about.google/favicon.ico	0%	Avira URL Cloud	safe	
http://https://about.google/assets-products/img/glue-google-color-logo.svg	0%	Avira URL Cloud	safe	
http://https://about.google/assets-main/img/glue-google-solid-logo.svg	0%	Avira URL Cloud	safe	
http://https://about.google/assets-products/img/glue-icons.svg	0%	Avira URL Cloud	safe	
http://https://about.google/assets-products/css/index.min.css?cache=8dee953	0%	Avira URL Cloud	safe	
http://https://about.google/assets-main/img/glue-icons.svg	0%	Avira URL Cloud	safe	
http://https://styleselect.com/favicon.ico	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://about.google/intl/hr/products	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scone-pa.clients6.google.com	142.250.186.138	true	false		high
ads.google.com	142.250.185.238	true	false		high
google.com	172.217.16.142	true	false		high
csp.withgoogle.com	142.250.185.113	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.185.173	true	false		high
plus.l.google.com	142.250.185.142	true	false		high
styleselect.com	178.20.45.197	true	false	• 0%, Virustotal, Browse	unknown
i.ytimg.com	216.58.212.150	true	false		high
mail.google.com	142.250.186.133	true	false		high
adservice.google.com	142.250.186.66	true	false		high
static.doubleclick.net	142.250.185.198	true	false		high
about.google	216.239.32.29	true	false	• 0%, Virustotal, Browse	unknown
stats.g.doubleclick.net	66.102.1.155	true	false		high
youtube-ui.l.google.com	142.250.186.46	true	false		high
googleads.g.doubleclick.net	172.217.16.130	true	false		high
play.google.com	142.250.185.174	true	false		high
www3.l.google.com	142.250.185.238	true	false		high
www.google.hr	142.250.186.131	true	false		high
photos-ugc.l.googleusercontent.com	142.250.181.225	true	false		high
ghs-svc-https-sni.ghs-ssl.googlehosted.com	142.250.185.147	true	false	• 0%, Virustotal, Browse	unknown
www.google.com	142.250.186.132	true	false		high
clients.l.google.com	142.250.181.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.225	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
www.blog.google	unknown	unknown	false		high
lh3.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
accounts.youtube.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/rcQGmayD_9OzAY1gZL3vRvB3Eq5M9ynAiB2P33LAhb27lsmZSl4DQPpELf5VWLkvKBWPSwAmd5-uXnAsiSMQwMvFaCoQinmY6SFhhQ=w0-e60	false		high
http://https://lh3.googleusercontent.com/2noIz2X2ov5fXwxhW8AbSDnLpp8tT3ml3-iV_OQ2UOwX_EhIBBgip7FPRs10DYmPKinVM98Qkjr1uN3BhQ3StGXCp1-O_wPwoLZeDQ=rw-e365-w2880	false		high
http://https://yt3.ggpht.com/ytc/AL5GRJXf7ZV0JSYp1wUp8Uz25FRkwH9PmS9IwGnknCvhO1g=s68-c-k-c0x00ffffff-no-rj	false		high
http://https://apis.google.com/js/client.js	false		high
http://https://lh3.googleusercontent.com/FU-s_R5k9ZDky6RTNWsdrN8xa9Jp7C2mwd_Kj9NHQe6Cw_EipUIFLjv0L7fGBh7KloVVACyAI7AIaXMC_bPGKVkX6aebI-4f-UurLRbk	false		high
http://https://lh3.googleusercontent.com/gQgn9ZUwHn7UyvQHOcAV_AmbPbpo97fRmCqBIGfPpbB-594aiAFfqQgaUwzEAUaI40O23_uJKvXf8_3QDKS1Aj28wVtz6GUTQFLG84oMGEU-BxiVRouO=w1440-l90-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/dMQ1Q4xlLrl3-KsZvX_9v56emij4OkRxzapLM7RSuZVd7PgqfjPxKR4KY8hVHYXqP2ZkS-_ZueXb9ywW66H2oCyTgIApr1ELCy3woOAviTgFP6uyAd0=h120	false		high

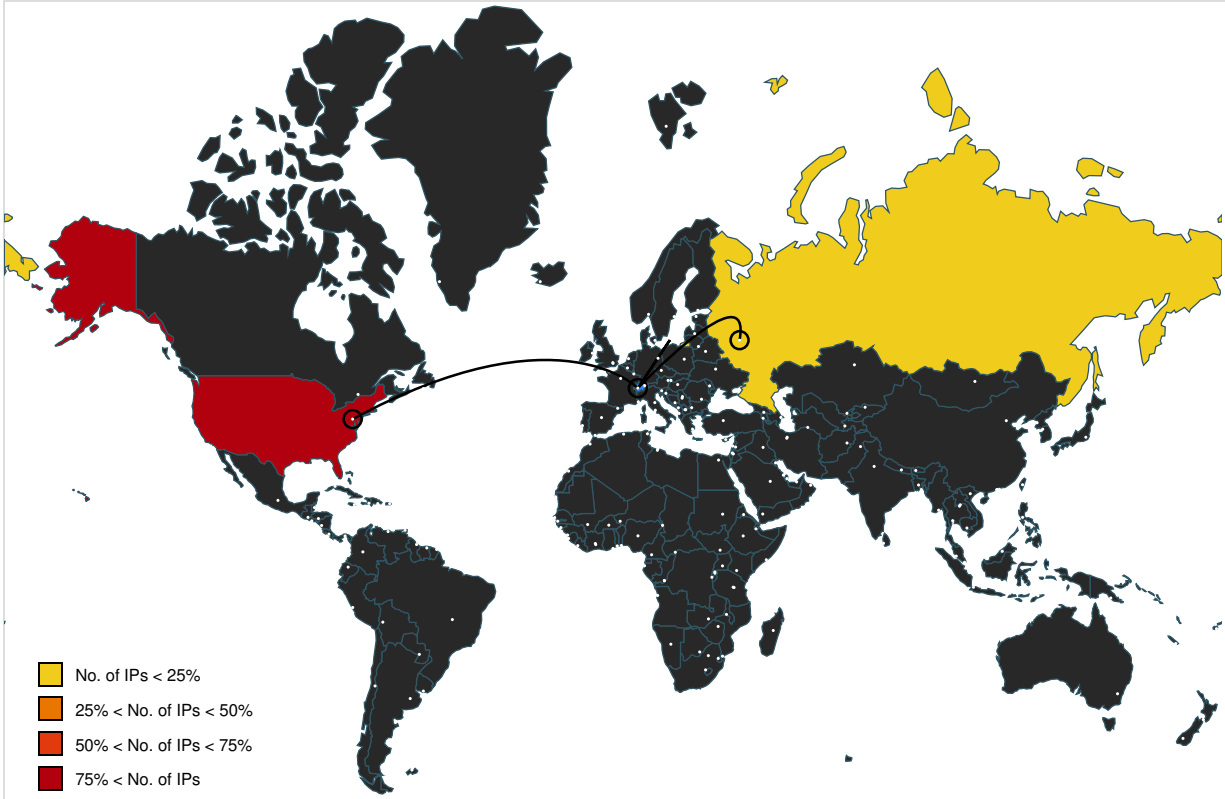
Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/vnSr97Bu2sI2_h334BHmEn1zTPrtv0hM9MLn3YxkN6JVzmir_VH62GiPIKfwtPBTOQ8xH0XNI40xfPAYbwbJEU-1jG09ovlU0f4S1Q=h120	false		high
http://https://www.google.com/gmail/about/static-2.0/css/partials/faq.css?fingerprint=392991776b78fd091779006c96b7384b	false		high
http://https://lh3.googleusercontent.com/NksFVpnLFiAE4YKEh9n84ebvfznogwh0AyAUDpmpLqpBP7h791LS9RcIzWpE8XfsiR0NJiHomxV8FyVO2ccMF2VzB_L3omeUWuHu9d3LGJ4Ww6JKviev	false		high
http://https://www.youtube.com/s/player/4248d311/player_ias.vflset/en_US/embed.js	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://www.google.hr/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-113093516-1&cid=620003221.1674639347&jid=414671037&_u=SACAAEAAQAAAACgBY~&z=1456209430	false		high
http://https://www.google.com/setprefs?sig=0_B5Deox5LjV-nPaZIAoirw4ivz0s%3D&hl=en&source=homepage&sa=X&ved=0ahUKEwijlfOgqOL8AhXSSvEDHRPvAK4Q2ZgBCBA	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://accounts.google.com/v3/signin/_/AccountsSignInUi/data/batchexecute?rpcids=UEkKwb&source-path=%2Fv3%2Fsignin%2Fidentifier&f.sid=-6484487158070746012&bl=boq_identityfrontendauthuiserver_20230115.08_p0&hl=hr&_reqid=34561&rt=c	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zqI8YkHjj90.O/ck=xjs.s.u-rfaHfpfBg.L.W.O/am=AAEqCFcAOAAAIAAAAAAASEAAAAAAAAAQAYAyB4ygYEbAgHiMEAWJYAEAAQxOiHCAAAA4ABDAMAAgAAACB_AAKeAIDBhAUAAAAAAAAACFiCYHCDBAUBIAAAAAAAAABKafLiABAEAQ/d=1/exm=CnSW2d,DPreE,DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,WINQGd,aa,abd,async,cdos,csi,d,dpf,epYOx,fXO0xe,hsm,jsa,kQvlef,mu,nabPbb,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch/ed=1/dg=2/br=1/rs=ACT90oF6V5SFSDHarfUTZb8Bl8x3BhGQvw/ee=Pjplud:PoEs9b;QGR0gd:Mlhmy;uY49fb:COQbmf;EVNhjf:pw70Gc;sTsDMc:kHVSUb;g8nkx:U4MzKc;wQlYve:aLUfP;kbAm9d:MkHyGd;F9mqte:UoRcbe;oUlnpc:RagDlc;YV5bee:IvPZ6d;dtl0hd:lLQWFe;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;R4IIIb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;okUaUd:wItadb;GleZL:J1A7Od;Xeq57c:wZTUNc;eJZqRc:wUwbse;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;kCQyJ:ueyPK;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;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;Oj465e:KG2eXe;Erl4fe:FloWmf;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=aLUfP?xjs=s2	false		high
http://https://lh3.googleusercontent.com/z3dgQsXgGqfadzIUmpGI_ppolUy7H6fgqIbtW_qzLXcBww0nOby8TEE3e_fW84Qa7zeAwe339f5VLkqRD6jk7Z9sEaVh5Y_yaPG9nw=h120	false		high
http://https://lh3.googleusercontent.com/PWXM4hp9IRRezHTV86SqLwhRQMz4_Lk08jll3GkWBvBZy_Uk6kvUvwIrVilwaIW2mHZJoccchG6o9a5UdOJEwQPf9oJGmOGSglo3VW0=rw-e365-w2880	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.3R2S2iMRC9o.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8-ukmJKpOYaCGRb909wNTowBRXFA/cb=gapi.loaded_0	false		high
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://about.google/assets-main/img/glue-google-solid-logo.svg	false	• Avira URL Cloud: safe	unknown
http://https://ads.google.com/home/static/js/butterbar/butterbar.min.js?cache=16cd874	false		high
http://https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j99&tid=UA-113093516-1&cid=620003221.1674639347&jid=414671037&_u=SACAAEAAQAAAACgBY~&z=1456209430	false		high
http://https://about.google/assets-products/css/index.min.css?cache=8dee953	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/kQDv-46ToDkqXJ2DIlr7hKXKalQvL0NJy4oGIhNlUkxX95btXayCKNoZuaY_KT-6U8-Iz35FlDZXRd1U3bNFo99a3k0-vwIIbtElStTKYwD_UxNkjA	false		high
http://https://lh3.googleusercontent.com/Pk8YenR3VOTvN9iNHAGWp3pWYZiaYMXXWUkfAjt_LMrf222t9zn815V-GfMRJ1Hjgq7l2k1KiQmxCw5d687WTfIPgwjVfGvoHaSwRDI=h120	false		high

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=94.0.4606.61&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/4248d311/www-widgetapi.vflset/www-widgetapi.js	false		high
http://https://lh3.googleusercontent.com/gcivdVV-tvxWnRUDNOUocQhsZmT9Was6CexDLkqmigkLzk5ZcNjqcgj3q4UROg4b1xbj63W94SONQIU2n3nBSa1qTQQX1SbJj_tQLR0	false		high
http://https://lh3.googleusercontent.com/C_Ty0aIlJNrRQz5pNFmgA1rsRnhZDj67eVCCHXoJFFot0FQEZydARPRKbBADyHQoA0_Dj6gLITCshiJq6C-H-QM_U2mJwJZVLOQPnwvCL2RerGMEhw0	false		high
http://https://googleads.g.doubleclick.net/pagead/id?slf_rd=1	false		high
http://https://ads.google.com/home/static/js/butterbar/butterbar-config.json?abc12345	false		high
http://https://www.youtube.com/s/player/4248d311/www-embed-player.vflset/www-embed-player.js	false		high
http://https://www.google.com/gen_204?atyp=i&ei=1unQY6PSPNKVxc8Pk96D8Ao&ct=slh&v=t1&pv=0.5158153454166279&me=10:1674639345353,V,0,0,0,0:0,h,1,1,o:19461,V,0,0,1920,969:4,e,B&zx=1674639364818	false		high
http://https://lh3.googleusercontent.com/Q4UDu0hKQgAyUzO0RpJTpTKc2DyaZbU-K96JCJjqKd9_ABetMMpS6LxO6Y7Ypm2CVhCro4n4n9PTF97SlwrSjmJFaHdV-_yDr8MpX1M=h120	false		high
http://https://lh3.googleusercontent.com/rFIOGuWFGvTm427OcRlhQIeB1SqlCZkVh7N7F-q8Rm6b_mtlUebqvFmXHCkvLuV8ebUiIRIQXbg_ujAXlJ9wg02s7L36Us66yyIAotc	false		high
http://https://lh3.googleusercontent.com/WdC-o7ZcZL5WALPSmfUC8H4oYhlhqm1DV45CtHqV06DTRR0rE_P9JXi-J2KXLd9CTyHt_t3ehUm1o_AMltgfAGbvQDku8jsZt0kBSA=h120	false		high
http://https://www.google.com/xjs/_/js/md=1/k=xjs.s.hr.yJTSuyULj1Q.O/am=AAEqCFcAOAAAIAAAAAASEAAAAAAAAQAYAyB4ygYEbAgHiMEAWJYAEAAQxOiHCAAAA4ABDAMAAgAAACB_AAKeAIDBhAUAAAAAAAAACFiCYHCDBAUBIAAAAAAAAABKafLiABAEAQ/rs=ACT90oFiIZaGLQNaU8yyAAwPigiW023qaQ	false		high
http://https://lh3.googleusercontent.com/gi7EU_u6IiuIRSxunfy5LLqsEJrC08L12aufZc3rP_w8hD8ouiVW89vfe7pTQrSsLXQYyQvnlhBfarK9Ul33ccQOSqKgK3i6iyArwg=h120	false		high
http://https://www.youtube.com/embed/by-kTJ0DOLc?rel=0&vq=hd720&start=0&cc_load_policy=1&playsinline=1&origin=https%3A%2F%2Fabout.google&enablejsapi=1&widgetid=1	false		high
http://https://lh3.googleusercontent.com/RwVe2Cm1EjeDmYhdTzr179G0ovq_PCxgPzQ92PO-YxTBEFTHWh0L6Ev8FFDWRgRGrE81vwn95tyg9Ey189OO4kllhhpLAMIsGFZ-UKA=h120	false		high
http://https://about.google/assets-products/img/glue-icons.svg	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/9NuRdiRepVl3n1txfg7Ky2wWzB3DvXkWABXeFMSn2tzDYYkv8T_RMA9R17fWi0ziUDIDTVJx0JruCzOev37c4dkK9Wrgkeyam3pM8ll=h120	false		high
http://https://www.google.com/gen_204?s=webhp&t=aft&atyp=csi&ei=1unQY6PSPNKVxc8Pk96D8Ao&rt=wsrt.308,aft.199,afti.199,prt.39&wh=969&imn=3&ima=2&imad=0&imac=0&aftp=969&bl=PSCp	false		high
http://https://www.google.com/gen_204?atyp=i&ei=1unQY6PSPNKVxc8Pk96D8Ao&ct=slh&v=t1&pv=0.5158153454166279&me=7:1674639336387,V,0,0,0,0:7851,V,0,0,1920,969:1115,e,B&zx=1674639345353	false		high
http://https://lh3.googleusercontent.com/oJtxC9wrYYcStJ4Ds2ylblE6GyJtbi_HWy01cp88xJGkrELh-SZ6N-kdrMmRglHFy7gsFWUNbG0Jth92P8HOVJkYyMMo76yMJ2vS=h120	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://lh3.googleusercontent.com/MtMPcZawFgE7-ZBRg85xFgdpOPtONPwQcoxQDmjmTBEeLQ_0e-Kpq4U5W_TBgpB35xFXb3fWb7b7oXRh4LyQwWWApn1fzp_GGRVGWHYmVWzweBxaicg=w600-l90-sg-rj-c0xffffff	false		high
http://https://about.google/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j99&tid=UA-69658807-1&cid=276779936.1674639353&jid=274801133&gjid=144316634&_gid=1526238992.1674639353&_u=aEDAAEABAAAAACgBY~&z=1860750059	false		high
http://https://www.youtube.com/s/player/4248d311/fetch-polyfill.vflset/fetch-polyfill.js	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://lh3.googleusercontent.com/Amr8tRBfd1Uk8zYm779hnSCwMzArp3LGD1LUhcgPdCOlk0UJczmdKLa42Apx-wzQdrUnsATBiFsyHT5pVit9Al6PwfVewM09FnlwAA=h120	false		high
http://https://lh3.googleusercontent.com/DWpSqn9zih2HKA8jegm1_8iYW5luCKjBQYaPaMeeqxF4wVZGDrG1dSz-ZNEmn9HcxNeHdJ_rWAvfvrNEZ_C9j2QPPhr8it81qoi5rW0_l2z7KPjLxY4=w1440-l90-sg-rj-c0xffffff	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zqI8YkHjj90.O/am=AAEqCFcAOAAAIAAAAAAASEAAAAAAAAQAYAyB4ygYEbAgHiMEAWJYAEAAQxOiHCAAAA4ABDAMAAgAAACB_AAKeAIDBhAUAAAAAAAAACFiCYHCDBAUBIAAAAAAAAABKafLiABAEAQ/d=1/ed=1/dg=2/br=1/rs=ACT90oFISqX-ps5q8wwgkzpCC-98CMK6Uw/m=cdos,dpf,hsm,jsa,d,csi	false		high
http://https://lh3.googleusercontent.com/_M14NRTYPPQYgdKReeicOfwYJfHl-USHThCxb3buQ8dKJ_XBIjR1InzdLQ3vjYrDVdOn79de6u_JkxB0D44hBrZ88olRx1fU8QIe7Cq_VzxUWalNeQ=w1440-l80-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/6xlGJ-dkwosfUisVYzRKNE1Wcr5QDDfRfZ4bXktF-Nn0J0ucHd_JI1wjXTls7lt5mvJvvcvtrNc0MESF98dAx6ivasEsZNxoaUZU-Q=h120	false		high
http://https://lh3.googleusercontent.com/csWtrOkqW8-iYd6fNH5_8YIuE2Y0Qpu6t-lIElGPzwYKnaOZqRwhYOus8iKMxEJGyQUrskBzpyB2rm4HM88fu1JHOcHbRCZOvBmavw=w0-e60	false		high
http://https://www.google.com/gen_204?atyp=csi&ei=8-nQY8rmJq6Cxc8Px66AmAw&s=webhp&t=all&bl=PSCp&wh=969&imn=2&ima=2&imad=0&imac=0&aftp=-1&adh=&ime=2&imex=2&imeh=0&imea=0&imeb=0&imel=0&scp=0&net=dl.10000,ect.4g,rtt.0&mem=ujhs.11,tjhs.15,jhsl.2173,dm.8&sys=hc.16&rt=aft.28,afti.28,aftqf.57,prt.56,xjses.158,xjsee.185,xjs.185,dcl.185,ol.681,lcp.51,fcp.51,wsrt.244,cst.0,dnst.0,rdxt.131,rqst.142,rspt.33,rqstt.135,unt.134,cstt.134,dit.301&zx=1674639364274	false		high
http://https://lh3.googleusercontent.com/hHWA5otDm9mYUJdAqTjo7wBWj8euY-SdEhCffO7oQzG3zpzxm-YExt1VDB8X6_5gchW_Ye3bfhOJXyOWgcUr94GtgqltKP4IxiH02O-Xzw5A1IHsxiw=h120	false		high
http://https://lh3.googleusercontent.com/vNgpLTvnDUr6-QM8s4OuuESGDXs_brbGoPR-7vfwdxQI7M4MVFV0CC_Hil4qRDSp4P66ik85fdv09jKn89kDAJVknIbd6wkl0zGQJQ=h120	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=hr&authuser=0&psi=1unQY6PSPNKVxc8Pk96D8Ao.1674639335382&nolsbt=1&dpr=1	false		high
http://https://lh3.googleusercontent.com/p2EiNuo4FQe3s8dhYgEiejBxjryT3B46OTWNItLqiwF58V0T62GKHa7VrbOhI7BbnQOBvdkPFu-4YGG0Dg3b0moXWWSc_aB1hw67Kts=h120	false		high
http://https://lh3.googleusercontent.com/8v_oGMOj9bgohn50RgLhJ8XGZ2kIUdr0RG4zCkIYnfjK24ORS0WFaTWmnzxXzagUg2fwAmDy1W_Y4oTtIacT2dhQzAqOy5H9Vg23Rq1oVnhUGtOynjY	false		high
http://https://lh3.googleusercontent.com/DEiv6a4elaSehnNAuLu1qmehKSI3gOBNZ8ekBnm02m43j-ugKu0OT248ZbTiAgnkDlZFzycQOY9oiBaIbSxCivN-CkKpnk3kREwN_EDdhKk1O9ehZqY=w600-l90-sg-rj-c0xffffff	false		high
http://https://lh3.googleusercontent.com/R7Wr9OkT5zk4gY2F3-tLiMwhFaMfO_hCU5LpTxztUaTOi8kU7_0QUIvOTlhHLyMol8kvHhVvdWUtjmAZ6cqiwGhwZzdg0fvc-UXtojU=h120	false		high
http://https://styleselect.com/vts0u	false		unknown
http://https://lh3.googleusercontent.com/EUHFjMpMj-UPEu6jfEEP8TPV7QxQerc-n_qulHi3MFPnK_63i5ldHApJsutq7wXqNmN9V2rmk9swsQ9I0eddAv77HIO4uv6gKt8haNAMqjiM9pqNu9w	false		high
http://https://www.google.com/gen_204?atyp=i&ei=8-nQY8rmJq6Cxc8Px66AmAw&ct=slh&v=t1&m=HV&pv=0.43093079954171976&me=1:1674639363619,V,0,0,1920,969:0,B,969:0,N,1,8-nQY8rmJq6Cxc8Px66AmAw:0,R,1,1,0,0,1920,969:444,x:752,e,B&zx=1674639364815	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	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ServiceLogin?hl=hr&passive=true&continue=https://www.google.com/&ec=GAZAmgQ	false		high
http://https://www.google.com/gmail/about/static-2.0/js/main.min.js?fingerprint=3013f65e4814d5914f9a24976b9493a1	false		high
http://https://www.google.com/gen_204?atyp=i&ei=8-nQY8rmJq6Cxc8Px66AmAw&ct=slh&v=t1&pv=0.43093079954171976&me=7:1674639364816,V,0,0,0,0:0,h,1,1,o:9,V,0,0,1920,969:14,h,1,1,i:632,e,B&zx=1674639365471	false		high
http://https://about.google/assets-main/img/glue-icons.svg	false	• Avira URL Cloud: safe	unknown
http://https://lh3.googleusercontent.com/nDCFKerWuvJvG26AZOPsWYFPiw3MRFDYqVJcHzQzK6AgY96TXH50bpQ1IE__BdBxxcXm8ZTaQ6OuJ4pbYF1c-ugOTfOmjhffJXEvJQ=h120	false		high
http://https://lh3.googleusercontent.com/j0mZxqPUZ28oopliF6vSV0okYdXUPZH__5C5_4zuI1eNoLd-JFgAFWu4oPFvxTguMH_Iihh76znHXocGuTuDGVtlaryO0cLZSNPVMA=h120	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/v3/signin/identifier?dsh=S-938658160%3A1674635759284236&continue=https%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&hl=hr&passive=true&flowName=GlifWebSignIn&flowEntry=ServiceLogin&ifkv=AWnogHetu5YjPVq-WCbyCLrIvbdvKTXbIbaMteNWvg6UIekZa-JukOettsnoJspcOECz1zASggBkXg	false		high
http://https://lh3.googleusercontent.com/aD5GNhlaU2d70gmSy5ioL1dMSUZN9cHDWPLkIBLhCsJ-BgcGUm-PD6o8XExZcx1i2iZV6PH0P8v3ceg0x7Tzd_OZ5FV0nXs5mX15sgA=h120	false		high
http://https://lh3.googleusercontent.com/tC78k3bL_DjdIByD4HSnnblCZF0nIR599IWYDDghEJDn7dwg-tuOIXGVR1TwxePI063JTgu9NvrsvRutrqHOfR5AAWduD51R8zuswV8=h120	false		high
http://https://styleselect.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://https://about.google/intl/hr/products	false	• Avira URL Cloud: safe	unknown
http://https://ads.google.com/intl/hr_hr/home/?subid=ww-ww-et-g-awa-a-g_hpafoot1_1!o2&utm_source=google.com&utm_medium=referral&utm_campaign=google_hpafooter&fg=1	false		high
http://https://www.google.com/gen_204?atyp=csi&ei=1unQY6PSPNKVxc8Pk96D8Ao&s=webhp&t=all&bl=PSCp&wh=969&imn=3&ima=2&imad=0&imac=0&aftp=969&adh=&ime=2&imex=2&imeh=1&imea=0&imeb=0&imel=0&scp=0&net=dl.1350,ect.4g,rtt.100&mem=ujhs.11,tjhs.14,jhsl.2173,dm.8&sys=hc.16&rt=aft.199,afti.199,prt.39,aftqf.199,xjses.385,xjsee.411,xjs.411,dcl.411,ol.983,lcp.237,fcp.83,wsrt.308,cst.71,dnst.10,rqst.142,rspt.38,sslt.71,rqstt.204,unt.122,cstt.133,dit.393&zx=1674639335935	false		high
http://https://lh3.googleusercontent.com/gQgn9ZUwHn7UyvQHOcAV_AmbPbpo97fRmCqBIGfPpbB-594aiAFfqQgaUwzEAUaI40O23_uJKvXf8_3QDKS1Aj28wVtz6GUTQFLG84oMGEU-BxiVRouO=w600-l90-sg-rj-c0xffffff	false		high
http://https://www.google.com/gmail/about/static-2.0/images/logo-gmail.png?fingerprint=c2eaf4aae389c3f885e97081bb197b97	false		high
http://https://accounts.google.com/favicon.ico	false		high
http://https://lh3.googleusercontent.com/mjVS_Izc6fGAvuaT0v--gb2so5mZvAbI5EUMUB41cWB7tpy81trBCR8rIlj8NoKgPzDWGN-Hs97NlW0T9W57YJ5z9A8QQWwXUYa_Zg=h120	false		high
http://https://lh3.googleusercontent.com/9KKBHHVmyet6xnci7yplPWQPpv2H7EvPQFmvy_mTShsOMPqbiMpLQHdHAsImNBL39fTnONH302_YC8LDgE2Am8Q81uXccg302NZpsgTjwtdBbNMDNsg=w1440-l80-sg-rp	false		high
http://https://lh3.googleusercontent.com/cS5nvr3r6Q16NoV6IuJLaauz7HNNRPnuHtsHleZ8du594H4EeiOjeNxV-Nq_w-qRA87TUedLQjTmqCG5s6jNZRp29n571FDWyditF-WJhfhQTY_73OM	false		high
http://https://www.google.com/xjs/_/js/k=xjs.s.en_GB.zqI8YkHjj90.O/ck=xjs.s.u-rfaHfpfBg.L.W.O/am=AAEqCFcAOAAAIAAAAAASEAAAAAAAAQAYAyB4ygYEbAgHiMEAWJYAEAAQxOiHCAAAA4ABDAMAAgAAACB_AAKeAIDBhAUAAAAAAAAACFiCYHCDBAUBIAAAAAAAAABKafLiABAEAQ/d=1/exm=cdos,csi,d,dpf,hsm,jsa/ed=1/dg=2/br=1/rs=ACT90oF6V5SFSDHarfUTZb8Bl8x3BhGQvw/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;R4IIlb:QWfeKf;BMxAGc:E5bFse;WDGyFe:jcVOxd;wV5Pjc:L8KGxe;xbe2wc:wbTLEd;DpcR3d:zL72xf;tosKvd:ZCqP3;ESrPQc:mNTJvc;NSEoX:lazG7b;G6wU6e:hezEbd;okUaUd:wItadb;GleZL:J1A7Od;Xeq57c:wZTUNc;eJZqRc:wUwbse;RiX1h:uiAbXc;oSUNyd:fTfGO;SJsSc:H1GVub;SMDL4c:fTfGO;JsbNhc:Xd8iUd;zOsCQe:Ko78Df;KcokUb:KiuZBf;WCEKNd:I46Hvd;LBgRLc:XVMNvd;LsNahb:ucGLNb;UyG7Kb:wQd0G;kCQyJ:ueyPK;TxfV6d:YORN0b;qaS3gd:yiLg6e;aAJE9c:WHW6Ef;BgS6mb:fidj5d;UVmjEd:EesRsb;z97YGf:oug9te;CxXAWb:YyRLvc;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;Oj465e:KG2eXe;Erl4fe:FloWmf;sP4Vbe:VwDzFe;kMFpHd:OTA3Ae;nAFL3:s39S4;iFQyKf:QIhFr/m=DhPYme,EkevXb,GU4Gab,MpJwZc,NzU6V,UUJqVe,aa,abd,async,epYOx,mu,pHXghd,q0xTif,s39S4,sOXFj,sb_wiz,sf,sonic,spch?xjs=s1	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.46	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.99	unknown	United States		15169	GOOGLEUS	false
142.250.185.147	ghs-svc-https-sni.ghs-ssl.googlehosted.com	United States		15169	GOOGLEUS	false
142.250.185.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
64.233.184.157	unknown	United States		15169	GOOGLEUS	false
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
66.102.1.155	stats.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.142	plus.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.132	www.google.com	United States		15169	GOOGLEUS	false
216.58.212.150	i.ytimg.com	United States		15169	GOOGLEUS	false
142.250.186.133	mail.google.com	United States		15169	GOOGLEUS	false
178.20.45.197	styleselect.com	Russian Federation		50627	ASN-FRWInternetServiceProviderIT	false
172.217.16.142	google.com	United States		15169	GOOGLEUS	false
216.239.32.29	about.google	United States		15169	GOOGLEUS	false
142.250.185.113	csp.withgoogle.com	United States		15169	GOOGLEUS	false
142.250.185.198	static.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.238	ads.google.com	United States		15169	GOOGLEUS	false
142.250.181.225	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.174	play.google.com	United States		15169	GOOGLEUS	false
142.250.185.173	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.16.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.66	adservice.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.11.1
192.168.11.20

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791289
Start date and time:	2023-01-25 09:33:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://styleselect.com/vts0u
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@50/0@29/26
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.hr/imghp?hl=hr&ogbl • Browse: https://www.google.hr/intl/hr/about/products • Browse: https://accounts.google.com/ServiceLogin?hl=hr&passive=true&continue=https://www.google.com/&ec=GAZAmgQ • Browse: https://www.google.com/setprefs?sig=0_B5Deox5LjV-nPaZIAoirw4ivz0s%3D&hl=en&source=homepage&sa=X&ved=0ahUKEwijlfOgqOL8AhXSSvEDHRPvAK4Q2ZgBCBA • Browse: https://about.google/?utm_source=google-HR&utm_medium=referral&utm_campaign=hp-footer&fg=1 • Browse: https://www.google.com/intl/hr_hr/ads/?subid=ww-ww-et-g-awa-a-g_hpafoot1_1!o2&utm_source=google.com&utm_medium=referral&utm_campaign=google_hpafooter&fg=1 • Browse: https://www.google.com/services/?subid=ww-ww-et-g-awa-a-g_hpbfoot1_1!o2&utm_source=google.com&utm_medium=referral&utm_campaign=google_hpbfooter&fg=1 • Browse: https://google.com/search/howsearchworks/?fg=1

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, CompPkgSrv.exe, backgroundTaskHost.exe
- Excluded IPs from analysis (whitelisted): 184.24.14.183, 142.250.186.35, 34.104.35.123, 142.250.186.131, 142.250.186.42, 142.250.185.234, 142.250.186.74, 142.250.186.106, 172.217.16.202, 142.250.186.170, 142.250.184.202, 216.58.212.170, 172.217.23.106, 142.250.185.202, 142.250.184.234, 216.58.212.138, 142.250.74.202, 142.250.185.138, 142.250.186.138, 172.217.18.106, 142.250.184.195, 142.250.185.72, 142.250.186.142, 216.239.32.36, 216.239.34.36, 142.250.74.195, 142.250.186.99, 142.250.185.131, 142.250.185.106, 142.250.181.234, 142.250.185.170, 172.217.18.10, 172.217.16.138, 142.250.185.74, 172.217.16.194, 8.253.95.249, 142.250.181.227
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, www.googleadservices.com, content-autofill.googleapis.com, fonts.gstatic.com, ajax.googleapis.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, wdcp.microsoft.com, jnn-pa.googleapis.com, arc.msn.com, region1.google-analytics.com, ris.api.iris.microsoft.com, licensing.mp.microsoft.com, wdcpalt.microsoft.com, edgedl.me.gvt1.com, login.live.com, www.googletagmanager.com, gstatic.com, update.googleapis.com, img-prod-cms-rt-microsoft-com.akamaized.net, 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 NtSetInformationFile 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

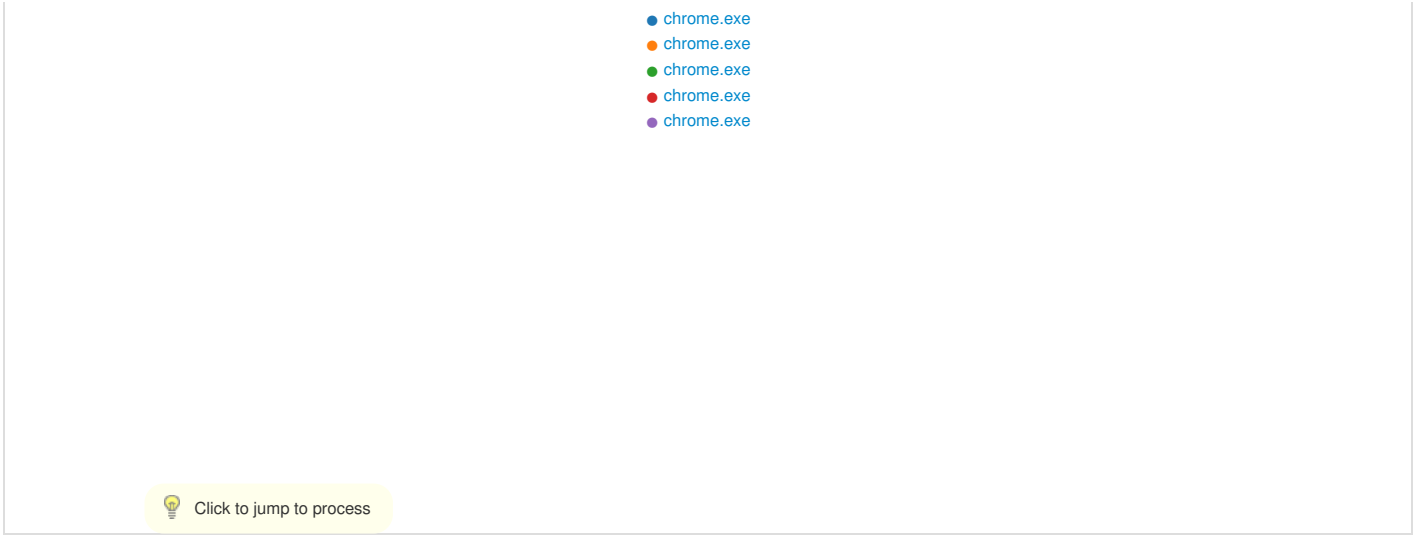
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4608**, Parent PID: **3200**

General

Target ID:	0
Start time:	09:35:33
Start date:	25/01/2023
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:	0x7ff658960000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
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

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

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

Analysis Process: chrome.exe PID: **6564**, Parent PID: **4608**

General	
Target ID:	3
Start time:	09:35:33
Start date:	25/01/2023
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 --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2012 /prefetch:8
Imagebase:	0x7ff658960000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
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: **4264**, Parent PID: **3200**

General	
Target ID:	5
Start time:	09:35:34
Start date:	25/01/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://styleselect.com/vts0u
Imagebase:	0x7ff658960000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
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: **7236**, Parent PID: **4608**

General	
Target ID:	12
Start time:	09:35:54
Start date:	25/01/2023
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 --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5044 /prefetch:8
Imagebase:	0x7ff658960000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **8196**, Parent PID: **4608**

General

Target ID:	13
Start time:	09:35:54
Start date:	25/01/2023
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 --field-trial-handle=1712,6834009655941694944,2695339048696769679,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --lang=en-US --service-sandbox-type=video_capture --mojo-platform-channel-handle=6856 /prefetch:8
Imagebase:	0x7ff658960000
File size:	2509656 bytes
MD5 hash:	464953824E644F10FFDC9E093FD18F94
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

Disassembly

No disassembly