ID: 876168
Cookbook: browseurl.jbs
Time: 11:51:24
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

Copyright Joe Security LLC 2023

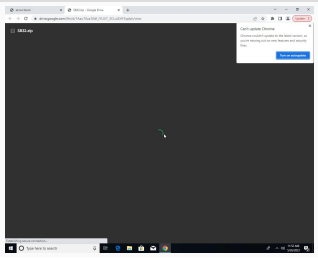
Windows Analysis Report

https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web

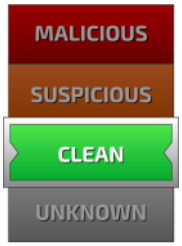
Overview

General Information

Sample URL:	http://https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web
Analysis ID:	876168
Infos:	



Detection

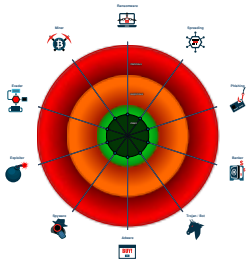


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5288 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5780 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1944 --field-trial-handle=1720,i,4096288064433636703,17727572675558076264,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5508 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

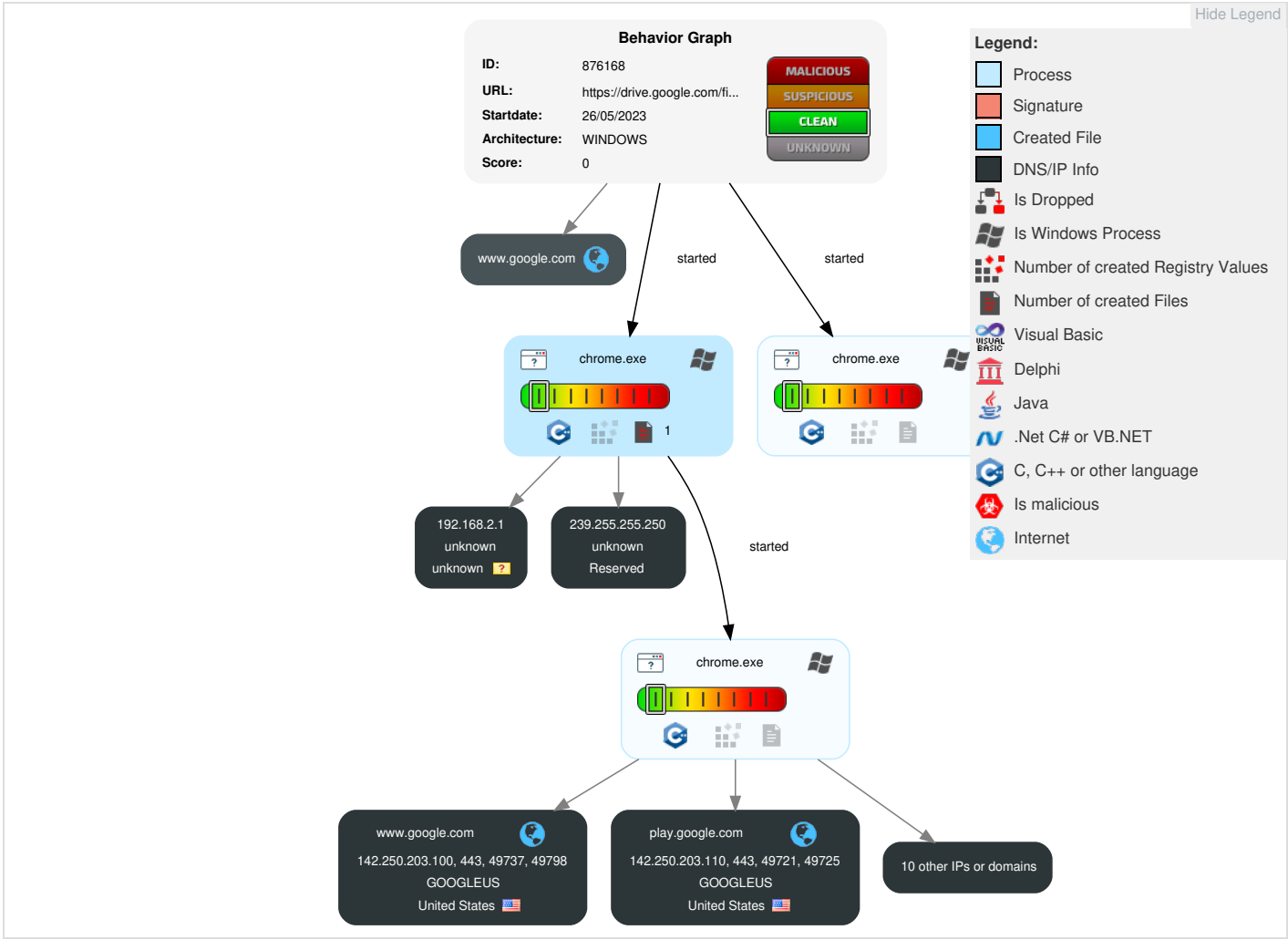
There are no malicious signatures, click here to show all signatures.

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

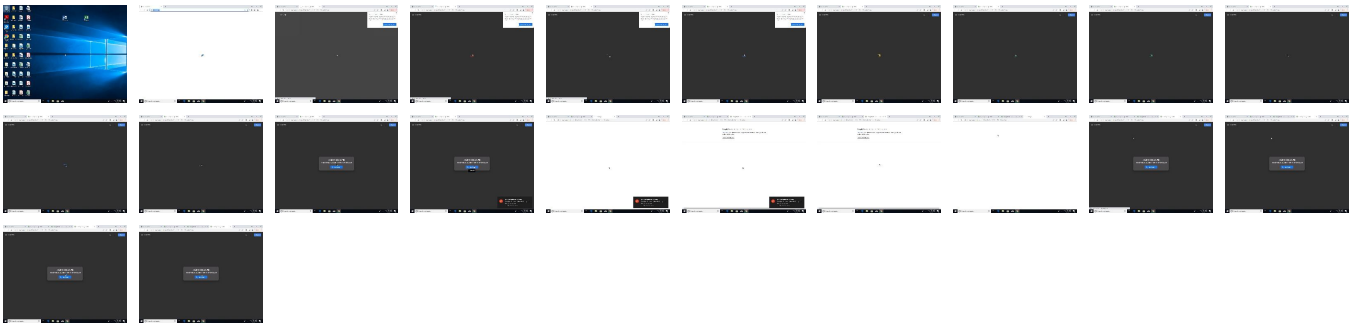
Copyright Joe Security LLC 2023

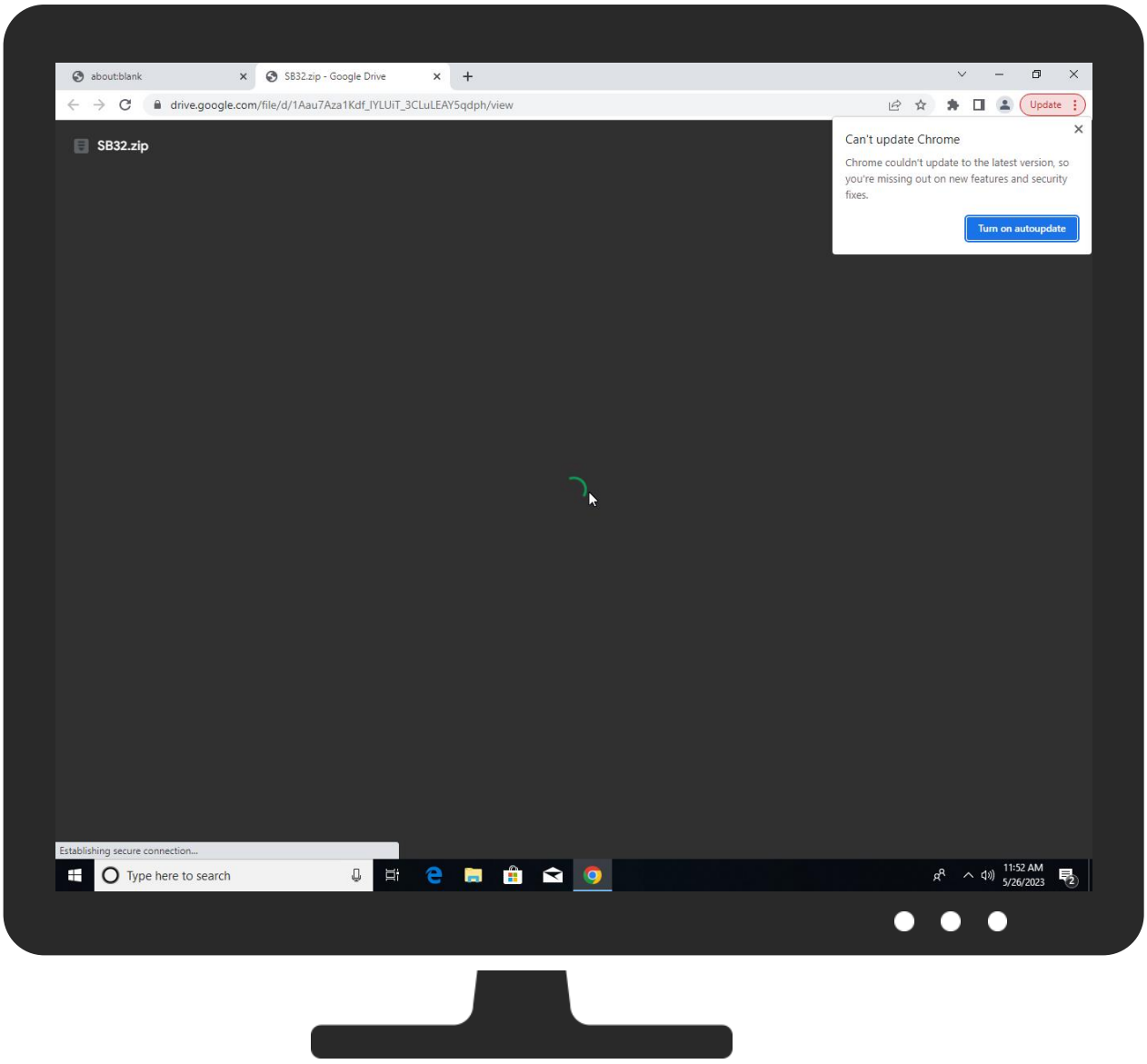


Screenshots

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://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web	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://www.broofa.com	0%	URL Reputation	safe	
http://www.broofa.com	0%	URL Reputation	safe	
http://https://csp.withgoogle.com/csp/lcreport/	0%	URL Reputation	safe	

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
http://www.bohemiancoding.com/sketch	0%	URL Reputation	safe	
http://www.bohemiancoding.com/sketch/ns	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
blobcomments-pa.clients6.google.com	142.250.203.106	true	false		high
accounts.google.com	172.217.168.45	true	false		high
plus.l.google.com	172.217.168.78	true	false		high
play.google.com	142.250.203.110	true	false		high
drive.google.com	172.217.168.14	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
peoplestackwebexperiments-pa.clients6.google.com	216.58.215.234	true	false		high
googlehosted.l.googleusercontent.com	216.58.215.225	true	false		high
clients2.google.com	unknown	unknown	false		high
lh3.googleusercontent.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://drive.google.com/open?id=1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph	false		high
http://https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=client/exm=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_1	false		high
http://https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/docos/p/sync?resourcekey&id=1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph&reqid=0	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_0?le=scs	false		high
http://https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web	false		high
http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_0	false		high
http://https://play.google.com/log?format=json&hasfast=true	false		high
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://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_open	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://drive.google.com/viewer2/prod-03/archive?ck=drive&ds=APznzaasIqez7CAZvd1AzdJZuQm7sAdnJFT4Z0_CBcEG2R0grRTcX1ow_i5lRsOx8Pwjj7KZ-wouRSRinrMEdiAe5R_1DNYrcKb8QFVhEBPcz_cMH29r1n_hnU8oOGhog0cddqJ_jHVH7evVvIZJvgAKAiSLfhKf3JE8uTLEpLxqnh5T-lqQm3phfEU0Ruothy555pIaKxoXlj3onLbT8dfeR8MIbNRoeqVyzbpFWx9BV1ui0FpEE8OZ-xkCGDqoQUnrvFgQJ_pb8xuzUQH6t2HmKnwZpckBi2tOBcehcwGSMafk5Z1lyc6q2nEI1KibcVn4ZnldI005nJrb_LhYxOXFCFfAj75WifM8jhamuJ_hMbkTgG6wic4lD32CBifJkJJ4oKIE1hCY&authuser=0&page=0	false		high
http://https://drive.google.com/viewer2/prod-03/archive?ck=drive&ds=APznzaZ4EnWmVlJt_JumJy33reBjJaVafEoqWavi_7pl0Gz0VsIk1PlJDEos8ZDf7dkGBiBsRZL_dKEfhJpvuv7cep5A0kCpuAGl6K6FyarLPhVXAO2p_uPsnnf_GkouiT__PKNuVQFJfh-dkxBGAIx6lOz5QJFQgv_CIlKD-GbFKhd-lm3U-RX_OPqqIPkYrxM6knd8S2_ux__co0pWYzcBB3CbRNT90t4XZkLgXiv4kl1FIo8cBA2HvnCw-K88yIE2fb9m3FqbaiMQtE0xKaLMJrumvGBM5MDWcQYleBYsJWziLdDpGZf96WCzoiPHZZohCOnfcfiJftbwY7I7jbeWq3_pwi6MsZQkXOM1g6u5Ns3FpZKEFsWWnelKaASry6bbENn-o3PW&authuser=0&page=0	false		high
http://https://lh3.googleusercontent.com/a-/AD_cMMSAfLQ3pvUn0ke3ZHFy0ZF-iRjAux4sy-U_uwY3=s64	false		high

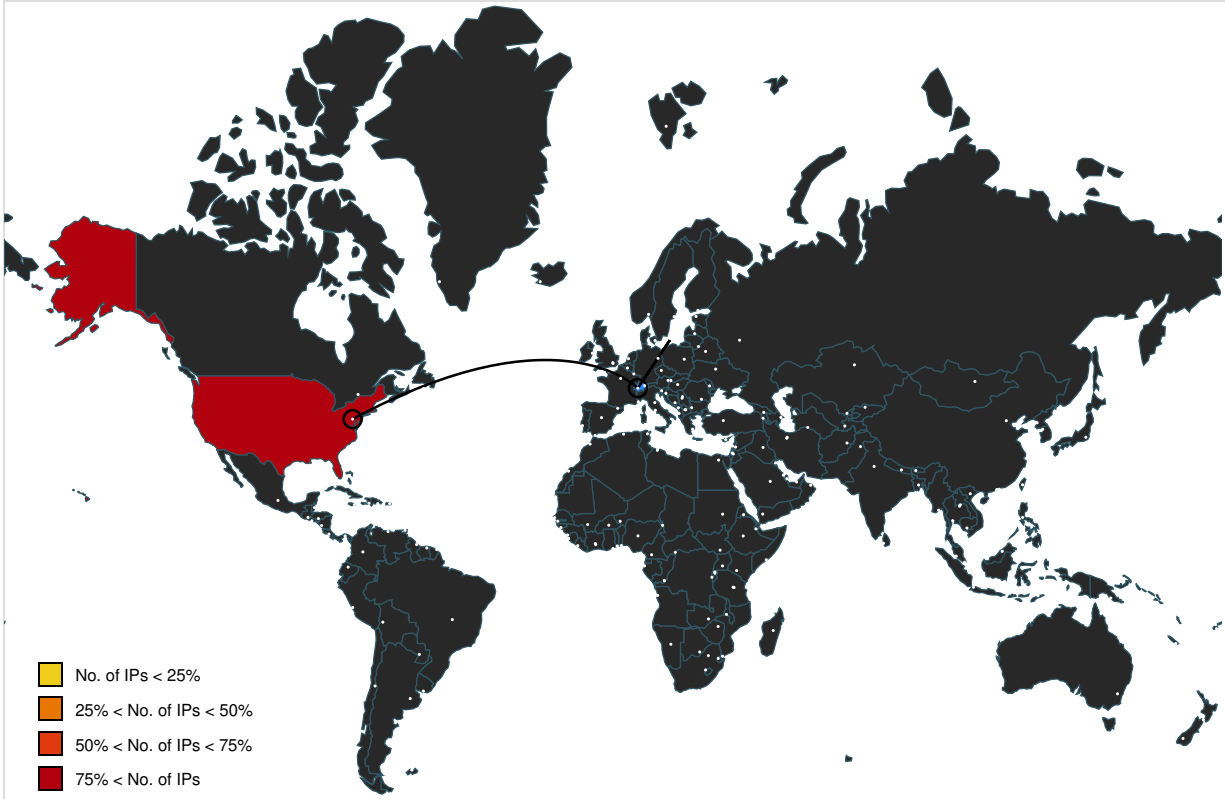
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://signaler-staging.sandbox.google.com	chromecache_150.1.dr	false		high
http://www.broofa.com	chromecache_176.1.dr, chromecache_150.1.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://apis.google.com/js/client.js	chromecache_166.1.dr, chromecache_150.1.dr	false		high
http://https://feedback2-test.corp.googleusercontent.com/tools/feedback/%	chromecache_166.1.dr	false		high
http://https://apis.google.com/js/googleapis.proxy.js	chromecache_155.1.dr	false		high
http://https://dataconnector.corp.google.com/:session_prefix:ui/widgetview?usegapi=1	chromecache_155.1.dr	false		high
http://https://support.google.com/drive/answer/2423485?hl=%s	chromecache_150.1.dr	false		high
http://https://onepick-autopush.sandbox.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://workspace.google.com/:session_prefix:marketplace/appfinder?usegapi=1	chromecache_146.1.dr, chromecache_154.1.dr, chromecache_155.1.dr	false		high
http://https://www.youtube.com	chromecache_150.1.dr	false		high
http://https://support.google.com/drive/answer/2407404?hl=en	chromecache_150.1.dr	false		high
http://https://pay.google.com/gp/v/widget/save	chromecache_155.1.dr	false		high
http://https://workspace.google.com	chromecache_150.1.dr	false		high
http://https://onepick-staging.sandbox.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://support.google.com/docs/answer/49114	chromecache_150.1.dr	false		high
http://https://support.google.com/drive/answer/2423694	chromecache_150.1.dr	false		high
http://https://support.google.com/google-workspace-individual/?p=esignature_signer_terms	chromecache_150.1.dr	false		high
http://https://drive-thirdparty.googleusercontent.com/	chromecache_150.1.dr	false		high
http://https://content-googleapis-test.sandbox.google.com	chromecache_166.1.dr	false		high
http://https://www.google.com/shopping/customerreviews/optin?usegapi=1	chromecache_155.1.dr	false		high
http://https://onepick-preprod.sandbox.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://developers.google.com/	chromecache_182.1.dr	false		high
http://https://onepick-staging-drivequal.sandbox.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://developers.google.com/identity/gsi/web/guides/gis-migration)	chromecache_182.1.dr	false		high
http://https://www.google.com/tools/feedback	chromecache_166.1.dr, chromecache_150.1.dr	false		high
http://https://sandbox.google.com/inapp/%	chromecache_166.1.dr	false		high
http://https://www.google.com/recaptcha/api.js?trustedtypes=true	chromecache_150.1.dr	false		high
http://https://apis.google.com/js/api.js	chromecache_156.1.dr, chromecache_150.1.dr	false		high
http://https://docs.google.com/picker	chromecache_150.1.dr	false		high
http://https://www.youtube.com/subscribe_embed?usegapi=1	chromecache_155.1.dr	false		high
http://https://feedback2-test.corp.google.com/tools/feedback/%	chromecache_166.1.dr	false		high
http://https://punctual-dev.corp.google.com	chromecache_150.1.dr	false		high
http://https://plus.google.com	chromecache_154.1.dr, chromecache_155.1.dr	false		high
http://https://clients5.google.com/webstore/wall/widget	chromecache_150.1.dr	false		high
http://https://sandbox.google.com/tools/feedback/%	chromecache_166.1.dr	false		high
http://https://content-googleapis-staging.sandbox.google.com	chromecache_166.1.dr	false		high
http://https://support.google.com/drive/answer/7650301	chromecache_150.1.dr	false		high
http://https://play.google.com/work/embedded/search?usegapi=1&usegapi=1	chromecache_155.1.dr	false		high
http://https://drive.google.com/requestreview?id=	chromecache_150.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://drive.google.com/drive/my-drive	chromecache_150.1.dr	false		high
http://https://fonts.google.com/license/googlerestricted	chromecache_147.1.dr	false		high
http://https://clients6.google.com	chromecache_166.1.dr, chromecache_154.1.dr, chromecache_155.1.dr	false		high
http://https://accounts.google.com/o/oauth2/iframe	chromecache_182.1.dr, chromecache_155.1.dr	false		high
http://https://clients5.google.com	chromecache_150.1.dr	false		high
http://https://www.google.com/log?format=json&hasfast=true	chromecache_176.1.dr, chromecache_150.1.dr	false		high
http://https://console.developers.google.com/	chromecache_182.1.dr	false		high
http://https://signaler-pa.youtube.com	chromecache_150.1.dr	false		high
http://https://support.google.com/docs/answer/65129?hl=en-GB	chromecache_156.1.dr	false		high
http://https://support.google.com/inapp/%	chromecache_166.1.dr	false		high
http://https://accounts.google.com/o/oauth2/postmessageRelay	chromecache_146.1.dr, chromecache_154.1.dr, chromecache_155.1.dr	false		high
http://https://drivemetadata.clients6.google.com	chromecache_150.1.dr	false		high
http://https://support.google.com/docs/answer/148505	chromecache_150.1.dr	false		high
http://https://support.google.com/	chromecache_166.1.dr, chromecache_150.1.dr	false		high
http://https://support.google.com/docs/answer/37603	chromecache_150.1.dr	false		high
http://https://www.google.com/shopping/customerreviews/badge?usegapi=1	chromecache_155.1.dr	false		high
http://https://csp.withgoogle.com/csp/lcreport/	chromecache_182.1.dr	false	• URL Reputation: safe	unknown
http://https://drive.google.com/savetodrivebutton?usegapi=1	chromecache_155.1.dr	false		high
http://https://scone-pa.clients6.google.com	chromecache_166.1.dr	false		high
http://https://lh3.googleusercontent.com/a/default-user	chromecache_156.1.dr	false		high
http://https://accounts.google.com/o/oauth2/auth	chromecache_182.1.dr, chromecache_154.1.dr, chromecache_155.1.dr	false		high
http://https://developers.google.com/api-client-library/javascript/reference/referencedocs	chromecache_182.1.dr	false		high
http://https://apis.google.com	chromecache_155.1.dr	false		high
http://https://domains.google.com/suggest/flow	chromecache_146.1.dr, chromecache_154.1.dr	false		high
http://https://apps-drive-picker-dev.corp.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://feedback2-test.corp.google.com/inapp/%	chromecache_166.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	chromecache_150.1.dr	false		high
http://https://signaler-pa.clients6.google.com	chromecache_150.1.dr	false		high
http://https://classroom.google.com/sharewidget?usegapi=1	chromecache_155.1.dr	false		high
http://https://support.google.com/docs/answer/65129	chromecache_156.1.dr	false		high
http://www.bohemiancoding.com/sketch	chromecache_163.1.dr, chromecache_177.1.dr	false	• URL Reputation: safe	unknown
http://https://developers.googleblog.com/2018/03/discontinuing-support-for-json-rpc-and.html	chromecache_182.1.dr	false		high
http://https://feedback2-test.corp.googleusercontent.com/inapp/%	chromecache_166.1.dr	false		high
http://https://drive.google.com/viewer	chromecache_150.1.dr	false		high
http://www.bohemiancoding.com/sketch/ns	chromecache_163.1.dr, chromecache_177.1.dr	false	• URL Reputation: safe	unknown
http://https://www.google.cn/tools/feedback/%	chromecache_166.1.dr	false		high
http://https://www.google.com/tools/feedback/help_panel_binary.js	chromecache_166.1.dr	false		high
http://creativecommons.org/ns#	chromecache_163.1.dr, chromecache_177.1.dr	false		high
http://https://uberproxy-pen-redirect.corp.google.com/uberproxy/pen?url=	chromecache_150.1.dr	false		high
http://https://clients3.google.com/cast/chromecast/home/widget/backdrop?usegapi=1	chromecache_155.1.dr	false		high
http://https://test-scone-pa-googleapis.sandbox.google.com	chromecache_166.1.dr	false		high
http://https://support.google.com/docs?p=comments_guide	chromecache_156.1.dr	false		high
http://https://talkgadget.google.com/:session_prefix:talkgadget/_/widget	chromecache_155.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://drive.google.com/picker/minpick/main	chromecache_150.1.dr	false		high
http://https://www.google.com/tools/feedback/%	chromecache_166.1.dr	false		high
http://https://families.google.com/webcreation?usegapi=1&usegapi=1	chromecache_155.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
216.58.215.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.203.110	play.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.78	plus.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.14	drive.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876168
Start date and time:	2023-05-26 11:51:24 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Copyright Joe Security LLC 2023

Sample URL:	http://https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web
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:	4
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@29/40@14/9
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Browse: https://drive.google.com/open?id=1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.3, 34.104.35.123, 172.217.168.74, 142.250.203.99, 172.217.168.67, 142.250.203.106, 216.58.215.234, 172.217.168.10, 172.217.168.42
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, ssl.gstatic.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, fonts.gstatic.com, content.googleapis.com, update.googleapis.com, clientservices.googleapis.com, www.gstatic.com
- Not all processes where analyzed, report is missing behavior information

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

Chrome Cache Entry: 146

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1530)
Category:	downloaded
Size (bytes):	114695
Entropy (8bit):	5.503626315759982
Encrypted:	false
SSDEEP:	3072:qpyvjFWER3DPbjh7f19c3cMGvMIoOZoYbgJ:UyT3DJmGvHoYbgJ
MD5:	74C0C2DCC8511894F3FCA6F0F98BFDA5
SHA1:	C3364A29B9380734073CEC8551F517C1BB173CEA
SHA-256:	5862AB09D5DB3D464EB0341AB9011DA490352223B6A02FB5F23216E15C092230
SHA-512:	87E99AB5C6A6E181FC8CA910C1F5A711D6A5AC8AF9F4A1A817F43A20B47DA31068FE70FEDD900E5DC8D5687ED324E4FED39931A8B6C5331FF25DFBE6A0889 E2
Malicious:	false
Reputation:	low
URL:	"https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_0"
Preview:	gapi.loaded_0(function(_){var window=this;.var ea,ia,ja,ka,la,qa,Aa;_.ca=function(a){return function(){return _.ba[a].apply(this,arguments)}};_.ba=[];ea=function(a){var b =0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};ia="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array. prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ja=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"obj ect"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};ka=ja(this);la=function(a,b) {if(b)a:{var c=ka;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ia(c,a,{configurable:! 0,writable:!0,value:b})}};.la("Symbol",function(a){if(a)return a;var b=function(f,h){this.OT=f;ia(this,"description",{configurable:!0,writable:!0,value:h})};b.p

Chrome Cache Entry: 147

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	13175
Entropy (8bit):	5.592164369000966
Encrypted:	false
SSDEEP:	192:o9XnWVG9yf1HwiqWzHk9s8JV5a101cbiNJzc29euvVf47G1OViTvzOr:CO5LMxjxbfvtk
MD5:	057322E1547A7C64ACE48E17502DD9B7
SHA1:	A3DC7D3745978E3421347E46223BBA9C2B513115
SHA-256:	3D7644E531AF0ACFA2E8A51057464362F2144E4A0742409CCEA03799E7016AB8
SHA-512:	2A0B56AB56AD03CFDD7D10AB67FABEE1CB584723A11C36D5EDA1B30832AE2DA1399EF8CBFCEC86076B60EFAC43EFAA286CDF6B61D90B245A03F31993F574 520D
Malicious:	false
Reputation:	low
URL:	"https://fonts.googleapis.com/css?family=Google+Sans_old:300,400,500,700"
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */./* armenian */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(http s://fonts.gstatic.com/s/googlesans/v46/4UasrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iqcsih3SAyH6cAwhX9RPiIUvaYr.woff2) format('woff2');. unicode-range: U+0308, U+0530-058F, U+2010, U+2024, U+25CC, U+FB13-FB17;.}./* cyrillic */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(http s://fonts.gstatic.com/s/googlesans/v46/4UasrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iqcsih3SAyH6cAwhX9RPjYUvaYr.woff2) format('woff2');. unicode-range: U+0301, U+0400-045F, U+0490-0491, U+04B0-04B1, U+2116;.}./* devanagari */.@font-face {. font-family: 'Google Sans';. font-style: normal;. font-weight: 400;. src: url(https ://fonts.gstatic.com/s/googlesans/v46/4UasrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iqcsih3SAyH6cAwhX9RPjMUvaYr.woff2) format('woff2');. unicode-range: U+0900-097F, U+1CD0-1CF9, U+200C-200

Chrome Cache Entry: 148

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765

SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=geljkvfdq7l6
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 149

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 150

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (585)
Category:	downloaded
Size (bytes):	1357470
Entropy (8bit):	5.571831016968806
Encrypted:	false
SSDEEP:	12288:MX0Av3U/CxM4IVs6GdENhFi2c1Sn7307N7Yb7Jbkbwt7FY:jA24As6GaNXi2c1I307N7YbNQkI
MD5:	0289DA937E282A20FF8EA61574917C4A
SHA1:	7467F7093BE9E29142AF3A6D06F518EB3F586FE8
SHA-256:	1F183975B70B6BBF53ECC3B2400F266A0C41EE0B2D579EA1A5A88D9CE96F529F
SHA-512:	EFBCE5EACD1012E0DA35FCF4868B35802950F7C69661C54FCB4458A2869855A14D019B47A64B56BC41BAAC0725DC044132D8F7B419703F3262A30FF23A5056D
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/apps-fileview/_/js/k=apps-fileview.v.en_GB.9qdjxbpIjH4.O/am=AAAC/d=1/rs=AO0039tRi3xSxgh5nYQ8l2yLn0fJCJAQgg/m=v,wb"
Preview:	try{./*.. Copyright 2013 Google LLC.. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2011 Google LLC.. SPDX-License-Identifier: Apache-2.0.*/./*... Copyright (c) 2 015-2018 Google, Inc., Netflix, Inc., Microsoft Corp. and contributors.. Licensed under the Apache License, Version 2.0 (the "License");. you may not use this file except in compliance with the License.. You may obtain a copy of the License at.. http://www.apache.org/licenses/LICENSE-2.0.. Unless required by applicable law or agreed to in writing, software. distributed under the License is distributed on an "AS IS" BASIS,. WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or impli ed.. See the License for the specific language governing permissions and. limitations under the License..*/./*. SPDX-License-Identifier: Apache-2.0 */./*. Copyright The C losure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-Li

Chrome Cache Entry: 151

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E B57E
Malicious:	false

Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=ulhix295cloo
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 152

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 153

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1594
Entropy (8bit):	7.862952554761723
Encrypted:	false
SSDEEP:	24:M5DhErRsW6OTfolVFt/qRyFQCB0RxgawoIqH4B36zPiX9/YhtdHft7:M5dIWGbofFBq+GR2eITl6sf9
MD5:	C66F20F2E39EB2F6A0A4CDBE0D955E5F
SHA1:	575EF086CE461E0EF83662E3ACB3C1A789EBB0A8
SHA-256:	2AB9CD0FFDDDF7BF060620AE328FE626BFA2C004739ADEDB74EC894FAF9BEE31
SHA-512:	B9C44A2113FB078D83E968DC0AF2E78995BB6DD4CA25ABFF31E9AB180849C5DE3036B69931CCA295AC64155D5B168B634E35B7699F3FE65D4A30E9058A2639BD
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/doclist/images/drive_2022q3_32dp.png
Preview:	.PNG.....IHDR... ... .szz.....IDATX.WkLSg.....65..A-f....lOk..."2..f[T...9.3q.q.....CnaKX.4.A/\D.l....m1qY....~ik+..F.i..;.A..,.<.NN.....~..B..1.f..V....7....?.R..<.r3./...d...*..A..h....S.....W^...`...0.....?_M...L.....`M.V.muG.$.e.J+.~Y.....B.g?aF.+..M1..[.1. .?2O ...n.y.....XuQ.H. ...A.....+.....b..D..D.y.....E.....M o4....R.w..b;`...R..#.\.t.%..]..[....%X< .L.Eo5Umm?..F.Oa1...W`uU:..L<..k..C....7a..1../QD3..U.D.l.T.5H.....4...v.....=t.."D?b.Pr.~....d#.Q.R.....)9'F/B. ....U.k'...p.!..J...O4.J.)G./"9.6.)@....4.h.(B2l.fB...AD..... ..7eK.%.O$gP.v.... y.t"9.E...h[...z{.C..[....7.....4.....-....X.....tJ...a.y....o<P..."..H\MI(Y....Y..A.,.D.$6B..`.Y..B.....y..q.m..ci..,F.w.....^h&.t...Y.]/.....H...d<*..cl.c...6N4..8Fl....h%.[&u....cd.L.|...M....."n...&.....d.'t:...c5..{~/7E.(`.`...>V7.RXS.k%..9...l....eRm...%..i...~.@.B..?."../.v.0.@.c{.(.^w.=....:t=.>.....V..}P..`...}.!u..k...p.ye...6.'.,.....Y.....

Chrome Cache Entry: 154

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3588)
Category:	downloaded
Size (bytes):	72759
Entropy (8bit):	5.590945304434519
Encrypted:	false
SSDEEP:	1536:MBfIQ3LpyvtnBF4iQ9wiLxrUhqAPIR+hbixFz7TJ1L/d:qpyvjFWqwReixF/d
MD5:	532655AD32D7392FBD756A13971EACA5
SHA1:	3762BE5AC389483AA259560DB54064A0E65B6DBD
SHA-256:	211E59D3D3DD0A6E43A866197A6214E70DA275B60EECC85CD5A8B6A7E9B46D9E
SHA-512:	30153F19CCEDE229A0A682B35C45EAA762457DC3B862FFDE85A84128BC3B849C3BF3F4D41B0FF78B6DC24490D387051F8029E2A34FE0CFF55D45370C71B5807E
Malicious:	false
Reputation:	low
URL:	http://https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=googleapis_proxy/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_0?le=scs

Preview:	gapi.loaded_0(function(_){var window=this;.var ea,ia,ja,ka,la,qa,Aa;_.ca=function(a){return function(){return _.ba[a].apply(this,arguments)}};_.ba=[];ea=function(a){var b =0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}};ia="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array. prototype||a==Object.prototype)return a;a[b]=c.value;return a};.ja=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"obj ect"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("a");};ka=ja(this);la=function(a,b) {if(b)a:{var c=ka;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ia(c,a,{configurable:! 0,writable:!0,value:b})}};.la("Symbol",function(a){if(a)return a;var b=function(f,h){this.OT=f;ia(this,"description",{configurable:!0,writable:!0,value:h})};b.p

Chrome Cache Entry: 155

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2054)
Category:	downloaded
Size (bytes):	17605
Entropy (8bit):	5.460595250881794
Encrypted:	false
SSDEEP:	384:M7C33GhGUAVg/3eHjZuOzdOoFO+5SYOelHO91EIuW:M7C33mAVSelHQoxOGk
MD5:	ACA2920A8781143ECB67C051639CC27D
SHA1:	92BB38B300E6FD4886ED96F2D920F7233EE8005A
SHA-256:	4B773EF75E8D64591D0C6187AEF5FD7F6164C7684EFE5ADD0A8547EBC143D76C
SHA-512:	0660464A43AF0A7B9BAD64554EBDC354A234FA7CDBC92F964C980F44DC951ACFF9A2FB11D7F217738FC8AE39BB1ADEEBD74DEC03F5215CE5AC124ECE6745A 292
Malicious:	false
Reputation:	low
URL:	http://https://apis.google.com/js/googleapis.proxy.js?onload=startup
Preview:	(function(){var da=function(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}},g="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ea=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");},fa=ea(this),h=function(a,b){if(b)a:{var c=fa;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&g(c,a,{configurable:!0,writable:!0,value:b})}};.h("Symbol",function(a){if(a)return a;var b=function(f,k){this.B=f;g(this,"description",{configurable:!0,writable:!0,value:k})};b.prototype.toString=function(){return this.B};var c="jscomp_symbol_"+(1E9*Math.random()>>>0)+"_",d=0,e=function(f){if(

Chrome Cache Entry: 156

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (557)
Category:	downloaded
Size (bytes):	821823
Entropy (8bit):	5.58278594848444
Encrypted:	false
SSDEEP:	6144:aYZWs5qe0zOBSEhrURBYZEDZK1+XAshjLBdzLo3FEAaU1/sWmC3KAE4tTk:XKX04XAgldAqUCdWE4tY
MD5:	263997AB57E6A25329C731505CEB732A
SHA1:	AE34B3267E5DA3698E961E08C9FB52BB014D44E4
SHA-256:	0FA16EF1CF9B1439673F06EF491C09D65C094545F2320DF2B3C51F34896D9858
SHA-512:	2D68E9E2305B9C7194A24C4A5BC15839BCD877CA11AA591970C075D628EF0DEC56D6B89ADF838C0060C4DF3D2D800559B9634EC695062AC2DDC7240A814FD9 E
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/apps-fileview/_/js/k=apps-fileview.v.en_GB.9qdjxbpljH4.O/am=AAAC/d=0/rs=AO0039tRi3xSxgh5nYQ8l2yLn0fJCJAQgg/m=sy2,b96Luc,dflQFd,HyHasc,E7aOmb,sy3,Yfyhhd,sy4,sy6,sy7,sy8,sy9,sya,syb,AtsVYc"
Preview:	try{.var Hhb=function(){A.call(this)};Q(Hhb,A);Hhb.prototype.init=function(){this.C=[]};var Ihb=new Hhb;.}catch(e){_DumpException(e)}.try{.qd("b96Luc");..rd();.}catch(e){ _DumpException(e)}.try{.qd("dflQFd");.var Jhb=new Jp;Jhb.altKey=!0;Jhb.keyCode=39;(new Jp).keyCode=13;.rd();.}catch(e){_DumpException(e)}.try{.qd("HyHasc");..rd ();.}catch(e){_DumpException(e)}.try{.qd("E7aOmb");..rd();.}catch(e){_DumpException(e)}.try{.var Khb=function(){return ea&&fa?!fa.mobile&&(ja("iPad")||ja("Android")||ja(" Silk")):ja("iPad")||ja("Android")&&!ja("Mobile")||ja("Silk")},VO=function(){return!(ea&&fa?fa.mobile:!Khb()&&(ja("iPod")||ja("iPhone")||ja("Android")||ja("IEMobile")))&&! Khb()};.}catch(e){_DumpException(e)}.try{.qd("Yfyhhd");..rd();.}catch(e){_DumpException(e)}.try{.var YO=function(a,b,c,d){null!==c&&(a.style.top=c+"px");d?(a.style.right= b+"px",a.style.left=""):(a.style.left=b+"px",a.style.right="")};.}catch(e){_DumpException(e)}.try{.var Ohb=1;(function(){for(var a=["ms","moz","webkit","o"],b=0

Chrome Cache Entry: 157

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, Exif Standard: [TIFF image data, little-endian, direntries=4, software=Google], baseline, precision 8, 64x64, components 3
Category:	dropped
Size (bytes):	3652
Entropy (8bit):	7.6849645750973625
Encrypted:	false
SSDEEP:	48:02E4knNrH7uhTnFUF7P2gqTrYUHKcdJ/eXBDQT5fL0HJN5Hs5ivlkuKRyFl:3knNTahRK7PLqT8UH3KBD45f6vDlkuZ
MD5:	2C5D279433276B451E100C464D4A10A3

SHA1:	90BBC2F1FCF5407EFE7561E9937F7D6F16C26DD7
SHA-256:	18B09260BEA886FF56F294EFF842E2DB3F3B8ED4A5562FD97C78C16F555E000B
SHA-512:	7F60B8330E20CFCB0B3471497AD14BF7AFEDDA649B621C53F00630A737ADF21360E29916EF28DD981E0674B4DF1493962B1CDB7DCBF509CB5D167F81D6CD54C
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Exif..II*.....1.....>...;.....E.....!...L..i.....n.....Google.Corbis.. Corbis. All Rights Reserved.....0220.....R98.....0100... ...._http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <r df:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org /dc/elements/1.1/" xmp:CreatorTool="Google"> <dc:rights> <rdf:Alt> <rdf:li xml:lang="x-default">. Corbis. All Rights Reserved.</rdf:li> </rdf:Alt> </dc:rights> <dc:creator> <rdf:Seq> <rdf:li>Corbis</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>..... .....@.@.....

Chrome Cache Entry: 158

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	7.862952554761723
Encrypted:	false
SSDEEP:	24:M5DhErRsW6OTfolVFt/qRyFQCB0RxgawoIqH4B36zPiX9/YhtdHft7:M5dlWGbofFBq+GR2eITl6sf9
MD5:	C66F20F2E39EB2F6A0A4CDBE0D955E5F
SHA1:	575EF086CE461E0EF83662E3ACB3C1A789EBB0A8
SHA-256:	2AB9CD0FFDDDF7BF060620AE328FE626BFA2C004739ADEDB74EC894FAF9BEE31
SHA-512:	B9C44A2113FB078D83E968DC0AF2E78995BB6DD4CA25ABFF31E9AB180849C5DE3036B69931CCA295AC64155D5B168B634E35B7699F3FE65D4A30E9058A2639BD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....IDATX.WkLSg.....65..A-f....lOk..."2..f[T...9.3q.q.....CnaKX.4.A^\D.l....m1qY....~ik+..F.i..;.A..,.<.NN.....~..B..1.f..V....7....?.R..<.r3./...d...*..A.. h....S.....W^...`...0.....?_M...L.....`M.V.muG.$.eJ+.~Y.....B.g?aF.+..M1..[.1. .?2O ...n.y.....XuQ.H. ...A.....+.....b..D..D.y.....E.....M o4....R.w..b;`...R..#.\.t.%..]..[....%X< .L.Eo5Umm?..F.Oa1...W`uU:..L<..k..C....7a..1../QD3..U.D.l.T.5H.....4...v.....=t.."D?b.Pr.~....d#.Q.R.....)9'F/B. ....U.k'...p.!..J...O4.J.)G./"9.6.)@....4.h.(B2I.fB...AD..... ..7eK.%.O$gP.v.... y.t"9.E....h[...z{.C..[....7.....4.....-....X.....tJ...a.y....o<P..."..H\Ml(Y....Y..A.,.D.$6B..`.Y..B.....y..q.m..ci..,F.w.....^h&.t...Y.]/.....H...d<*..cl.c...6N4..8FI....h%. [&u....cd.L.|...M....."n...&.....d.'t:...c5..{~/7E.(`.`...>V7.RXS.k%..9...l....eRm...%..i...~.@.B..?."../.v.0.@.c{.(.^w.=....:t=.>.....V..}P..`...}.!u..k...p.ye...6.'.,.....Y.....

Chrome Cache Entry: 159

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	831
Entropy (8bit):	7.690596689293278
Encrypted:	false
SSDEEP:	24:ars5HGJLO4eG5bQxWGUpbIW779bHBoLU489YmBZo:arssA4L6hvaZ7wv8mml
MD5:	916C9BCCCF19525AD9D3CD1514008746
SHA1:	9CCCE6978D2417927B5150FFAAC22F907FF27B6E
SHA-256:	358E814139D3ED8469B36935A071BE6696CCAD7DD9BDBFDB80C052B068AE2A50
SHA-512:	B73C1A81997ABE12DBA4AE1FA38F070079448C3798E7161C9262CCBA6EE6A91E8A243F0E4888C8AEF33CE1CF83818FC44C85AE454A522A079D08121CD8628D0
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/images/branding/product/1x/drive_2020q4_32dp.png
Preview:	.PNG.....IHDR... ... .szz.....IDATx.b .....+.....m..dW.@..tm.Y.....m.....m.m..L.|.....{..b...t.....=H..qt..V..X..<jQc...p...fdU.\2.....9T...Jz!9...L.)&.....n....`~.T.\.\.$.....q Q.....LFOx.....^&,"bB..Lh9$_.6<...A...Q.T&y.,'...p...W`.2.?X(.o.4.J?.2...@.4...*..X..c.....[UZJ...MN.].z..f..DFe.J.....:lr...0X.....).....^*..!....u..c..R4.GH....Y....E....Q.....+!..)... e".....,.Ge.r.T..!.r..(.|.9f..}.....(...s..N...[..~.%6QF..g..r.....CN.e"(..uY.h._1.H.e....r.k..%^S.c..<..0.s.j..,D.....]..y.2(..OC.o\.3.."....cw...:;.btq.....w=.....R-[].4..]...?.....o..K../cC. <O...y..O.....{.-'Ln9..M.*6t.(.....o.K.$....bz.X._d.....Z].U.....t....Bf.Zl.^vA._..g.{l....V...{....=.jua..[...k.....j....Y\...!..+.m..X..t(....."..Mz.26l....7X.C...-...Z.lvl.....y}x.....7.m .VV....IEND.B`.

Chrome Cache Entry: 160

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	831
Entropy (8bit):	7.690596689293278
Encrypted:	false
SSDEEP:	24:ars5HGJLO4eG5bQxWGUpbIW779bHBoLU489YmBZo:arssA4L6hvaZ7wv8mml

MD5:	916C9BCCCF19525AD9D3CD1514008746
SHA1:	9CCCE6978D2417927B5150FFAAC22F907FF27B6E
SHA-256:	358E814139D3ED8469B36935A071BE6696CCAD7DD9BDBFDB80C052B068AE2A50
SHA-512:	B73C1A81997ABE12DBA4AE1FA38F070079448C3798E7161C9262CCBA6EE6A91E8A243F0E4888C8AEF33CE1CF83818FC44C85AE454A522A079D08121CD8628D 0
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ... .szz.....IDATx.b .....+.....m..dW.@..tm.Y.....m.....m.m..L.|.....{..b...t.....=H..qt..V..X..<jQc...p...fdU.\2.....9T...Jz!9...L.)&.....n....`~.T.\.\.$.....q Q.....LFOx.....^&,"bB..Lh9$_.6<...A...Q.T&y.,'...p...W`.2.?X(.o.4.J?.2...@.4...*..X..c.....[UZJ...MN.].z..f..DFe.J.....:lr...0X.....).....^*..!....u..c..R4.GH....Y....E....Q.....+!..)... e".....,.Ge.r.T..!..r..(.|.9f...}.....(...s..N...[..~.%6QF..g..r.....CN.e"(..uY.h._1.H.e....r.k..%^S.c..<..0.s.j..,D.....]..y.2(..OC.o\.3.."....cw...:;.btq.....w=.....R-[].4..]...?.....o..K../cC. <O...y..O.....{.-'Ln9..M.*6t.(.....o.K.$....bz.X._d.....Z].U.....t....Bf.Zl.^vA._..g.{l....V...{....=.jua..[...k.....j....Y\...!..+.m..X..t(.....".Mz.26l....7X.C...-...Z.lvl.....y}x.....7.m .VV....IEND.B`.

Chrome Cache Entry: 161	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 162	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 163	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	113532
Entropy (8bit):	5.839678678501525
Encrypted:	false
SSDEEP:	3072:+PdSJxbML3MNcsq1xCLqrQcS8xriAX7E1fbaRrcjSkoi5WYDQ/JHzb4:qHCLqEcS8xOAX7E1f2BPC
MD5:	A81225ED4531630A28B0358ABB240AE0
SHA1:	ED8006477D268D4BD40DD5CBE8ECCD58ADDE4F70
SHA-256:	2A41DA0D6A970C6E9DF2A3C8F6B5A2A71B1F047125858EA4D58276041CA7CD54
SHA-512:	587E82E3C7DC1F161434174165F5FA3E8106ADB26CBAD37CF76AD6BFFEAFCB9B8FE57B00481F5F7C1EE73F6AA978AA32F3BCD7AA1FAEDB68E66DABD1D119 F793
Malicious:	false

Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYPE svg PUBLIC '-//W3C//DTD SVG 1.1//EN' 'http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd'>.<svg width ="31px" height="3834px" preserveAspectRatio="none" version="1.1" viewBox="0 0 31 3834" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xl ink">. <g transform="translate(0,1632)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5H7V9h4V5h2v4h4v2h-4v4h-2v-4z"/>. </g>. <g transform="translate(0,2602)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5 H7V9h4V5h2v4h4v2h-4v4z" fill="#fff"/>. </g>. <g transform="translate(0,1816)" fill="#fff">. <path d="m17.705 10.14-3.405-6.1401h-4.6l-6.1 11 2.1 4h8.1027c0.4644 0.8028 1.1094 1.488 1.8795 2h-9.9822c-0.7 0-1.4-0.4-1.8-1.1l-2.1-4c-0.3-0.6-0.3-1.3 0-1.9l6.2-11c0.3-0.6 1-1 1.7-1h4.6c0.7 0 1.4 0.4 1.8 1l3.9307 7.0882c-0.3348-0.058-0.6792-0.0882-1.0307-0.0882-0.4446 0-0.878 0.

Chrome Cache Entry: 164

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E5 B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=8kxzoqhhzdfm
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 165

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E5 B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=oq13xo2n6gkx
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 166

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2323)
Category:	downloaded
Size (bytes):	98314
Entropy (8bit):	5.462295124848516
Encrypted:	false
SSDEEP:	1536:OSZlhz0kRLmyopk+AzYHW3kON2Khc25B0ThcLF2xyAnlJEt/F:qz0bpeD08ZP5iThcLAnl0
MD5:	E1F9EA0662C81137CEF4F0F54A2447DE
SHA1:	78DF8762DBAEEE7A48A3025B16F944E18B1BF743
SHA-256:	DBC814581D65726954572A4AC59433E4B30E3A2B434EE1EB975A62D61A287580
SHA-512:	E07054D7C4AB1734A3A561F9D45F6B0DA157BD7110BA55623D778A25DDD8BF31043BEABA0719DA78CA64666864CBC4AA0DB17EB9EA68FE3CF94841A0100D8 DF
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js

Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var m,aa=function(a){var b=0;return function(){return b<a.length?{done:!1, value:a[b++]}:{done:!0}}},ba="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a},ca=function(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");.},da=ca(this),r=function(a,b){if(b)a:{var c=da;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];if(!(e in c))break a;c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ba(c,a,{configurable:!0,writable:!0,value:b})}};r("Symbol",function(a){if(a)return a;var b=function(f,g){this.oc=f;ba(this,"description",{configurable:!0,writable:!0,value:g})};b.prototype.toString=function

Chrome Cache Entry: 167

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:HKmn:qmn
MD5:	EC331136E75314D2030EE013B6069921
SHA1:	6B7428B8B15616A67F767D42964AF94FCBE2A803
SHA-256:	A7358DF6B7B60280F2A0D7CD5B70A9F1DFA4FCE5C31FB1A24FB2F109AF7EE977
SHA-512:	30C9B411C937F7D3DE9E59D8BE1CDE4F262B05C6AC2EC2D2C1956E705FE255D84DE17913826A0378B7FD4E51E075EE72A6BF16B870BF78B83D4F1D4507A4428
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTA0LjAuNTExMi44MRIQCaU0dxS7vz-SEgUNBu27_w==?alt=proto
Preview:	CgkKBw0G7bv/GgA=

Chrome Cache Entry: 168

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E5B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 169

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E5B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=9zfweupfmegm
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 170	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3 B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 171	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	382
Entropy (8bit):	5.363005447378165
Encrypted:	false
SSDEEP:	6:hxuJLzLMb038GIdLqo37fVBeQDXY2F6YkAbvOm/esHeOldL2V4Nhdx434QL:hYA0Id579hLFBkAb2m/esHOdCV4Nbx4j
MD5:	5CE4A9AEB22947B188CF1902E116801C
SHA1:	42013E8BD4F56968729AD2FE0DFE66806B22A14B
SHA-256:	1E20DFA5C0E411BBE6BA8E82388F1AEC7679BA56DC3E9AA02DEC04453C591C60
SHA-512:	5BE23E8F48CFF1AB89141943932ED05376098ED27F737071A742EFD2A963E63E2864AC60B3FEBA0D7624C291FD901CDACB8488D02EDBAF33B422C33171B395D 6
Malicious:	false
Reputation:	low
URL:	http://https://content.googleapis.com/static/proxy.html?usegapi=1&jsh=m%3B%2F_%2Fscs%2Fabc-static%2F_%2Fjs%2Fk%3Dgapi.gapi.en.UjJbvPIecP0.O%2Fd%3D1%2Frs%3DAHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA%2Fm%3D__features__
Preview:	<!DOCTYPE html>.<html>.<head>.<title></title>.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<script nonce="Gf5CizWbZtBk7s8gvnL55Q">. window ['startup'] = function() {. googleapis.server.init();. };.</script>.<script src="https://apis.google.com/js/googleapis.proxy.js?onload=startup" async defer nonce="Gf5 CizWbZtBk7s8gvnL55Q"></script>.</head>.<body>.</body>.</html>.

Chrome Cache Entry: 172	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	209
Entropy (8bit):	6.668570364625647
Encrypted:	false
SSDEEP:	6:6v/lhP+Bw51z9YaD6kDNsPl2PLIUdyDXwn/jp:6v/7IwrnPDNe2PLIUdyDXwn/N
MD5:	E718A1B337A3197CBC7ED8C8F560FB5D
SHA1:	703765677CFEA246D06C2481E0BB495EC3D095F3
SHA-256:	933453961F18E84204C8A3A13FBF771DF892E18DFD0C820C4437D99CC0EDED60
SHA-512:	8328FCF407EA2510F910FE3C729615061CE44AA049FA7CA7278FEA81AF533607541CB15700C01DB2BD5070DB8816B6CF8A5E2AFAE2CACCF9E83B4AA3B25671 5
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/doclist/images/mediatype/icon_2_archive_x16.png
Preview:	.PNG.....IHDR.....a....IDATx.....1..].@#\.../R..@'.@....@.f.....bY.....W9g...>.....4..=.U...`.....z...w.....bY..P...n2=....%...L..\@%P....!...U.m....e..-.~9.....IEND.B`.

Chrome Cache Entry: 173	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped

Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3B57E
Malicious:	false
Reputation:	low
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 174

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, Exif Standard: [TIFF image data, little-endian, direntries=4, software=Google], baseline, precision 8, 64x64, components 3
Category:	downloaded
Size (bytes):	3652
Entropy (8bit):	7.6849645750973625
Encrypted:	false
SSDEEP:	48:02E4knNrH7uhTnFUF7P2gqTrYUHKcdJ/eXBDQT5fL0HJN5Hs5ivlkuKRyFl:3knNTahRK7PLqT8UH3KBD45f6vDlkuZ
MD5:	2C5D279433276B451E100C464D4A10A3
SHA1:	90BBC2F1FCF5407EFE7561E9937F7D6F16C26DD7
SHA-256:	18B09260BEA886FF56F294EFF842E2DB3F3B8ED4A5562FD97C78C16F555E000B
SHA-512:	7F60B8330E20CFCB0B3471497AD14BF7AFEDDA649B621C53F00630A737ADF21360E29916EF28DD981E0674B4DF1493962B1CDB7DCBF509CB5D167F81D6CD54C
Malicious:	false
Reputation:	low
URL:	http://https://lh3.googleusercontent.com/a-/AD_cMMSAfLQ3pvUn0ke3ZHFy0ZF-iRjAux4sy-U_uwY3=s64
Preview:	......JFIF.....Exif..II*.....1.....>...;.....E.....!...L...i.....n.....Google.Corbis.. Corbis. All Rights Reserved.....0220.....R98.....0100.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="XMP Core 5.5.0"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:dc="http://purl.org/dc/elements/1.1/" xmp:CreatorTool="Google"> <dc:rights> <rdf:Alt> <rdf:li xml:lang="x-default">. Corbis. All Rights Reserved.</rdf:li> </rdf:Alt> </dc:rights> <dc:creator> <rdf:Seq> <rdf:li>Corbis</rdf:li> </rdf:Seq> </dc:creator> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="w"?>.....@.@.....

Chrome Cache Entry: 175

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	downloaded
Size (bytes):	1383873
Entropy (8bit):	5.695036599807018
Encrypted:	false
SSDEEP:	6144:4mHNB7N5dBZ7KPOoNM/gi7DDfFKM7+rcBGhOiOG75EeiXJZkaYses49h0qftn/NO:Rz7NrBZ7KPOoNpPRTubwdxhtJsCa
MD5:	D26439F1E1919DF94CE75E14A995FF50
SHA1:	FAB1EA89D7B86A0BA286D284A36EA1E640A83754
SHA-256:	75C73FD64CF4A810E929F4B320E21489AD2FEECC051721FD291BC692A0FBEF42
SHA-512:	CBD4623EFE55B45A5AEF831D8650953AE1F394D29E5B692AB28696A180BF59A46679C72B33EB96381970560F188F7BBF9361E82EA05F4C0C1EB62C376ACA2D25
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/_/apps-fileview/_/ss/k=apps-fileview.v.dn51dlpkwdA.L.W.O/am=AAAC/d=0/rs=AO0039sCPWxySfx_IVRyiRbtjaAT2bMwRw
Preview:	@keyframes shimmer{0%{background-position:100% 50%}to{background-position:0 50%}}@keyframes fadeInAnimation{0%{opacity:0}to{opacity:1}}.ja0jmf{-webkit-align-content:center;align-content:center;-webkit-animation-fill-mode:forwards;animation-fill-mode:forwards;-webkit-animation-iteration-count:1;animation-iteration-count:1;-webkit-animation:fadeInAnimation ease 200ms;animation:fadeInAnimation ease 200ms;background-color:var(--dt-surface,#fff);display:-webkit-box;display:-webkit-flex;display:flex;-webkit-flex-direction:column;flex-direction:column;height:100%;position:absolute;top:0;width:100%;z-index:3000}.F6wkof{-webkit-animation:shimmer 2.2s ease infinite;animation:shimmer 2.2s ease infinite;background:0 0/300% 300% linear-gradient(-61deg,var(--dt-inverse-on-surface,#dadce0) 40%,var(--dt-surface-variant,#f1f3f4) 50%,var(--dt-inverse-on-surface,#dadce0) 60%);background-color:var(--dt-inverse-on-surface,#dadce0)}@media (forced-colors:active){.F6wkof{border:1px solid var(--dt-outline,#808

Chrome Cache Entry: 176

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2120)
Category:	downloaded
Size (bytes):	112653
Entropy (8bit):	5.469717500832877
Encrypted:	false
SSDEEP:	1536:If0ZLXjdUu6R8+1sWzUpPKhA5KOu5qLdLjVQ9Q4yT8RDiABZDG19qbIHKkyIWwq:ZZDZU2PofcJjkfBVZy19qRtwq
MD5:	159AE9BD9515B2DF7F0E21D6BB54EA44
SHA1:	07144BFFA06DC8C6DAC584A2C5290A5915014D96
SHA-256:	64E08184323782F2DD3302720587969454FB602810BC9F6436DC305A5A0C1A01
SHA-512:	19DAFCB556468F94BB610663ECFD2EC2DE3BB8CFEE8492A8AC522A498084996AC9BD3BE5624DB9FBAAEE09D806D50F5EBABA6D19D89753513A25154EDD432F09
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/og/_/js/k=og.qtm.en_US.-QJ0wzngI5w.2019.O/rt=j/m=qabr,q_dnp,qapid/exm=qaaw,qadd,qaid,qein,qhaw,qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/rs=AA2YrTvWsOfJ2hY7SYcWL595KdVibQGLUQ"
Preview:	this.gbar_=this.gbar_||{};(function(_){var window=this;.try{._.ee=function(a){return _.hb(a)&&1==a.nodeType};_.fe=function(a,b){if("textContent"in a)a.textContent=b;else if(3==a.nodeType)a.data=String(b);else if(a.firstChild&&3==a.firstChild.nodeType){for(;a.lastChild!=a.firstChild;)a.removeChild(a.lastChild);a.firstChild.data=String(b)}else _.ce(a),a.appendChild(_.de(a).createTextNode(String(b)))};var ge;_.he=function(a,b){b?a.setAttribute("role",b):a.removeAttribute("role")};_.ie=function(a,b,c){Array.isArray(c)&&(c=c.join(" "));var d="aria-"+b;""===c||void 0==c?(ge||(ge={atomic:!1,autocomplete:"none",dropeffect:"none",haspopup:!1,live:"off",multiline:!1,multiselectable:!1,orientation:"vertical",readonly:!1,relevant:"additions text",required:!1,sort:"none",busy:!1,disabled:!1,hidden:!1,invalid:"false"}),c=ge,b in c?a.setAttribute(d,c[b]):a.removeAttribute(d)):a.setAttribute(d,c)};var je,ke,le;je=function(a){return"string"==typeof a.className?a.className:a.getAttribute&&a.getAttribute

Chrome Cache Entry: 177

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	113532
Entropy (8bit):	5.839678678501525
Encrypted:	false
SSDEEP:	3072:+PdSJxbML3MNcsq1xCLqrQcS8xriAX7E1fbaRrcjSkoi5WYDQ/JHzb4:qHCLqEcS8xOAX7E1f2BPC
MD5:	A81225ED4531630A28B0358ABB240AE0
SHA1:	ED8006477D268D4BD40DD5CBE8ECCD58ADDE4F70
SHA-256:	2A41DA0D6A970C6E9DF2A3C8F6B5A2A71B1F047125858EA4D58276041CA7CD54
SHA-512:	587E82E3C7DC1F161434174165F5FA3E8106ADB26CBAD37CF76AD6BFFEAFCB9B8FE57B00481F5F7C1EE73F6AA978AA32F3BCD7AA1FAEDB68E66DABD1D119F793
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/viewer/v3/v-sprite50.svg
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYPE svg PUBLIC '-//W3C//DTD SVG 1.1//EN' 'http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd'>.<svg width="31px" height="3834px" preserveAspectRatio="none" version="1.1" viewBox="0 0 31 3834" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">. <g transform="translate(0,1632)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5H7V9h4V5h2v4h4v2h-4v4h-2v-4z"/>. </g>. <g transform="translate(0,2602)">. <path d="M20 2H4c-1.1 0-2 .9-2 2v18l4-4h14c1.1 0 2-.9 2-2V4c0-1.1-.9-2-2-2zm0 14H4V4h16v12zm-9-5H7V9h4V5h2v4h4v2h-4v4h-2v-4z" fill="#fff"/>. </g>. <g transform="translate(0,1816)" fill="#fff">. <path d="m17.705 10.14-3.405-6.1401h-4.6l-6.1 11 2.1 4h8.1027c0.4644 0.8028 1.1094 1.488 1.8795 2h-9.9822c-0.7 0-1.4-0.4-1.8-1.1l-2.1-4c-0.3-0.6-0.3-1.3 0-1.9l6.2-11c0.3-0.6 1-1 1.7-1h4.6c0.7 0 1.4 0.4 1.8 1l3.9307 7.0882c-0.3348-0.058-0.6792-0.0882-1.0307-0.0882-0.4446 0-0.878 0.

Chrome Cache Entry: 178

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (922)
Category:	downloaded
Size (bytes):	14513
Entropy (8bit):	5.655669776943351
Encrypted:	false
SSDEEP:	192:gPol1YenqxpaAQo8kZtGdfZbxR20EQSsbWGhus+Tl47t/PUPpH2Aw:gPneqpanoM7tEQSyxuFTll9UP0
MD5:	1075BEE3AF8C635D6CE12AACF119CD7A
SHA1:	3544C9F817BAB99B86A8D2096465FFC880AF110D
SHA-256:	0A0F978E59131CC6646687047CA7ECA7E4343B3EEF91F99DD9CF2B8C68136DB0
SHA-512:	9363056EB05A5436BC57A634B28923B90DE6C7080D83BE521145A9B53E2EB593C42E53FD83DCCD4F790AC296D62347E94EF8DA23EB60E2B9C998865364E0BCB3
Malicious:	false
Reputation:	low
URL:	"https://www.gstatic.com/_/apps-fileview/_/js/k=apps-fileview.v.en_GB.9qdjxbpIjH4.O/am=AAAC/d=0/rs=AO0039tRi3xSxgh5nYQ8l2yLn0fJCJAQgg/m=sy5,sye,syd,syf,T807ad,J9ssyb"

Preview:	try{.var Lhb=function(){aJ.apply(this,arguments)};Q(Lhb,aJ);Lhb.prototype.enqueue=function(a,b){this.insert(a,b)};var WO=function(a,b){a%=b;return 0>a*b?a+b:a}, Mhb=/[\x00\x09-\x0d \x22\x26\x27\x2d\/\x3c-\x3e`\x85\xa0\u2028\u2029]/g,Nhb=/[\x00\x09-\x0d \x22\x27\x2d\/\x3c-\x3e`\x85\xa0\u2028\u2029]/g,XO=function(a){return Ou(a,Gu)?String(tta(a.getContent())).replace(Nhb,Qu):String(a).replace(Mhb,Qu)};.}catch(e){_DumpException(e)}.try{.var h_b=function(a,b){this.C=a instanceof Xp?a:new Xp(a,b)};R(h_b,RC);h_b.prototype.kc=function(a,b,c,d){var e=Ke(a);var f=e.body;e=e.documentElement;e=new Xp(f.scrollLeft||e.scrollLeft,f.scrollTop||e.scrollTop);f =this.C.x+e.x;e=this.C.y+e.y;var g=kFa(a);f-=g.x;e-=g.y;TC(new Xp(f,e),a,b,c,null,null,d)};var o1=function(a,b){h_b.call(this,a,b)};R(o1,h_b);o1.prototype.F=0;o1.prototyp e.D=function(a){this.F=a};.o1.prototype.kc=function(a,b,c,d){var e=dra(a);e=lt(e);var f=lq(Od(a).C);f=new Xp(this.C.x+f.scrollLeft,this.C.y+f.scrollTop);var g=b,k=TC(f,a, g,c,e,10,d

Chrome Cache Entry: 179

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3 B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=siwecesfducc
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 180

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	209
Entropy (8bit):	6.668570364625647
Encrypted:	false
SSDEEP:	6:6v/lhP+Bw51z9YaD6kDNsPl2PLIUdyDXwn/jp:6v/7lwrnPDNe2PLIUdyDXwn/N
MD5:	E718A1B337A3197CBC7ED8C8F560FB5D
SHA1:	703765677CFEA246D06C2481E0BB495EC3D095F3
SHA-256:	933453961F18E84204C8A3A13FBF771DF892E18DFD0C820C4437D99CC0EDED60
SHA-512:	8328FCF407EA2510F910FE3C729615061CE44AA049FA7CA7278FEA81AF533607541CB15700C01DB2BD5070DB8816B6CF8A5E2AFAE2CACCF9E83B4AA3B25671 5
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx.....1..].@#\.../R..@'.@....@.f.....bY.....W9g...>.....4..=.U...`.....z...w.....bY..P...n2=....%...L..\@%P....!...U.m....e..-.~9.....IEND.B`.

Chrome Cache Entry: 181

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 15344, version 1.0
Category:	downloaded
Size (bytes):	15344
Entropy (8bit):	7.984625225844861
Encrypted:	false
SSDEEP:	384:ctE5KIuhGO+DSdXwye6i9Xm81v4vMHCbppV0pr3Ll9/w:cqrVO++tw/9ClCFbQLlxw
MD5:	5D4AEB4E5F5EF754E307D7FFAEF688BD
SHA1:	06DB651CDF354C64A7383EA9C77024EF4FB4CEF8
SHA-256:	3E253B66056519AA065B00A453BAC37AC5ED8F3E6FE7B542E93A9DCDCC11D0BC
SHA-512:	7EB7C301DF79D35A6A521FAE9D3DCCC0A695D3480B4D34C7D262DD0C67ABEC8437ED40E2920625E98AAEAFBA1D908DEC69C3B07494EC7C29307DE49E91C2 EF48
Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2

Preview:	wOF2.....;.....H..;.....d..@..J.`..L.T..<.....x.....^...x.6.$..6. ..t. ..I.h\|.I....A....b6.....(.....@e.]...*:..-.0..r.)..hS..h...N.).D.....b.].....^..t?.m{...."84...9.....c...?..r3o.. ..}....S]....zbO.../z..{.....~cc....I...#.G.D....#*e.A..b...b`a5P.4.....M....v4..fI#X.z,.,...=avy..F.a.\9.P\|.[....r.Q@M.I.._.9..V..Q..]....[{u..L@...]..K.....]C....I$.Z.Z...Zs.4..... x..... ..F.?.7N..].|.wb\....Z{1L#..t....0.dM...$JV...{..oX...i....6.v.~.....)\|.TtAP&).KQ.]y.....'...:.d..+..d..."C.h..p.2.M..e,.*UP..@.q..7..D.@...,.....B.n. r&.....F!....\...;R.?-.i...,7..cb../I...E g...!X.)5.Aj7...Ok..l7.j.A@B`".}.w.m..R.9..T..X.X.d....S..`XI..1... .$C.H.,.\. ..A(.AZ.....`Wr.0]y..-..K.1.....1.tBs..n.0...9.F[b.3x...*$....T..PM.Z-.N.rS?I.<8eR'.3..27..? ;..OLf*.Rj.@.o.W.....j~ATA....vX.N:.3dM.r.)Q.B...4i.f..K.I..s....e.U.2...k..a.GO.}..../.'..%$..ed.*.'..qP....M..j...../.z&.=...q<....-..?.A.%..K..

Chrome Cache Entry: 182	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1674)
Category:	downloaded
Size (bytes):	210900
Entropy (8bit):	5.522942323555225
Encrypted:	false
SSDEEP:	3072:4mz6pMfQVG7P0oFFLnqOqXTAOGQ2UbLcsqYrIixFvMkg0mFNZX7aPeBm7o:p6zMXmOvSbLcslLF4d7aPeBm7o
MD5:	E9B65543C045B9466E1BFA601C7F1130
SHA1:	4C203FB4144EF28C5AFA642CC5EA3743736E4419
SHA-256:	770AE555CE9A43F97B5BB89731D7B36B04EDB8C1EE24FF2754A230C2AC83B04A
SHA-512:	CB34D915A6507B7653E8C7CF0478691CDB76BA815A3AFE26871C9E2C7A4A8DC9F62C2D64F4C559E7B496F1A407030A963723EE574D6C36D78A7D1626476EBA(B
Malicious:	false
Reputation:	low
URL:	"https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.UjJbvPIecP0.O/m=client/exm=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo_flbzE3yQmWQ7n7N3yCQZtJt8-oA/cb=gapi.loaded_1"
Preview:	gapi.loaded_1(function(_){var window=this;_.Dg=(window.gapi||{}).load;_.Xn=_.He(_.Se,"rw",_.Ie());.var Yn=function(a,b){(a=_.Xn[a])&&a.state<b&&(a.state=b)};var Zn=function(a){a=(a=_.Xn[a])?a.oid:void 0;if(a){var b=_.Ee.getElementById(a);b&&b.parentNode.removeChild(b);delete _.Xn[a];Zn(a)}};_.$n=function(a){a=a.container;"string"===typeof a&&(a=document.getElementById(a));return a};_.ao=function(a){var b=a.clientWidth;return"position:absolute;top:-10000px;width:"+(b?b+"px":a.style.width||"300px")+";margin:0px;border-style:none;"};_.bo=function(a,b){var c={},d=a.jc(),e=b&&b.width,f=b&&b.height,h=b&&b.verticalAlign;h&&(c.verticalAlign=h);e||(e=d.width||a.width);f||(f=d.height||a.height);d.width=c.width=e;d.height=c.height=f;d=a.getIframeEl();e=a.getId();Yn(e,2);a:{e=a.getSiteEl();c=c||{};if(_.Se.oa){var k=d.id;if(k){f=(f=_.Xn[k])?f.state:void 0;if(1===f||4===f)break a;Zn(k)}}(f=e.nextSibling)&&f.getAttribute&&f.getAttribute("data-gapistub")&&(e.parentNode.removeChild(f),e.style.cssTex

Chrome Cache Entry: 183	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.16293190511019
Encrypted:	false
SSDEEP:	3:CUmExltxlHh/:Jb/
MD5:	FC94FB0C3ED8A8F909DBC7630A0987FF
SHA1:	56D45F8A17F5078A20AF9962C992CA4678450765
SHA-256:	2DFE28CBDB83F01C940DE6A88AB86200154FD772D568035AC568664E52068363
SHA-512:	C87BF81FD70CF6434CA3A6C05AD6E9BD3F1D96F77DDDAD8D45EE043B126B2CB07A5CF23B4137B9D8462CD8A9ADF2B463AB6DE2B38C93DB72D2D511CA60E3 B57E
Malicious:	false
Reputation:	low
URL:	http://https://ssl.gstatic.com/docs/common/cleardot.gif?zx=2u0s1p2so5ze
Preview:	GIF89a.....!.....,.....D..;

Chrome Cache Entry: 184	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 29728, version 1.0
Category:	downloaded
Size (bytes):	29728
Entropy (8bit):	**7.992172668524615**
Encrypted:	**true**
SSDEEP:	768:TH6A20dJY6b2NtZVnUZsaH4e730cMYpO/amBAs:TH6D0zYOav6sIz30HYG7As
MD5:	F8D4CD97E53436F3C20D32BC3DD18695
SHA1:	B412CB15B2B545181E6F3075E9847E6F1F5802E8
SHA-256:	45A61A04904FC2115C440A349A65DC93D2965B0B24DC5A8172BD8B792BDBF103
SHA-512:	169197AF2B468514C86C2F9434B4E62A814EEC67B32FED51BA25484A15D69C8569DA63E2776EB14C3587868731BB2482A375DAEFCD6EE8BAD82CD2BCB9B78B 5E

Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/googlesans/v46/4UasrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iqcsih3SAyH6cAwhX9RPjIUvQ.woff2
Preview:	wOF2......t ....../d..s..........................&...4.."?HVAR...`?STAT..'..../<.....I..W..2.0..".6.$..N. ..>..1..[8.q.m..._w...)_....{..D.....{.6...L....?+.!......SO..).=S..]H.G....J...[.^:.w.G.6l.. ..e....ne$.F...>.DF,.p..?s...@/..K!dBL....{.$.j.2.....S2.n.0!........CO.f...r..nR....E......P{XY..H../<?.c.Y...o...f....X..B1.L~..4....]....Z$.f......1...(...c-u....7..r..'..UU.JV....$\|@.w3G ....Hj.a.}.Li\|......At..h{@..._.......\|..PyR..P......(......%...i.i.r....].......5.L..e..3G66.>.O....G..e..%B..4..^.N...).. ...._..N.t..#.%]..c/..~.<.Eq....@3,iH...,......X..d.xa....(. ..>.>.....c.1... .$..p...r. ...YF...UT'.h..p...iw.`.[6s..|.E..L......Z..$.yz4.H.W5.n.]..=....;3.#...:....&......)......u..u`...dY.d.L..<......L~..r.n;.8....].l.x@....FS.........p,........2.....8.C...if...L.o....S...]..S..AiD... ..x...!..n..<Y.....~...L......'..s..5q.h.....*.W.....0ml.n..J`..0..p.$..sN..9....6......$:.D&.UHq9.......^...><_....yXX.....K.3o..&.#..F..j..Sl..

Chrome Cache Entry: 185

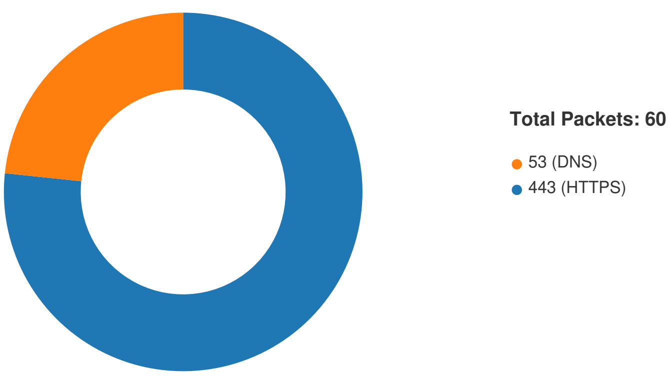
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	JSON data
Category:	downloaded
Size (bytes):	1379
Entropy (8bit):	4.46945576240193
Encrypted:	false
SSDEEP:	24:Gv7F9ihRTY1hAMWZHWnJ8rD50JzNa4Ia+vLW:GDFwRTY1hTWZHWJsN2tI6
MD5:	F187568CA87D2DC7FE4414BEC8272A9B
SHA1:	5FF9EBBB0997BD75FF13C8B71F24957D14EF85E5
SHA-256:	B86471EA6F82CB14E357EF23B457E253B2018B32157B0BCC8A47DBF9CBF681B0
SHA-512:	DC59E58C3C7A3DFAA00A5B1942B74EAE4241007BD5E88F2FA381D18D0916DF66D88C4B0A1EF61E072EC56EF8499B96574AFA94B9EE44B34DCFFA9C04778C1(4F
Malicious:	false
Reputation:	low
URL:	http://https://blobcomments-pa.clients6.google.com/v1/metadata? docId=1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph&revisionId=0B8SUfFm0WuGdeHdlT1RRWHMrVldGUHljTXNRM05EMmdxZmpvPQ&userLocale=en-GB&timeZoneId=Etc%2FGMT%2B7&documentResourceKey.resourceKey&forceImportEnabled=true&key=AIzaSyCMp6sr4oTC18AWkE2Ii4UBZHTHEpGZWZM&%24unique=gc797
Preview:	{. "serializedDocosKeyData": "[null,null,0,null,null,null,null,1,[\"Anonymous\",null,\"//ssl.gstatic.com/docs/common/blue_silhouette96-0.png\",\"ANONYMOUS_105250506097979753968\",1,null,1,null,1],1,\"AAHRpnXtS-4ITJxCxA3jvVz1cTHDJXcY0agz0jbM4MGLHE9m0pnYQ2rJKZdPKs_boQ6ST5EHt6VBNoQiRZZo6QTE0RAmpVQ5djQ\",null,null,null,null,null,1,null,null,1,null,null,null,null,1,0,null,null,null,0,null,null,0,null,null,null,null,1,0,null,null,null,null,[\"tf\",60000,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,0,0,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,0,0,null,null,null,1,null,null,null,null,null,null,0,null,null,\"\",null,0,null,null,null,null,0],[[5704745,5707899,5711538,5712270,5712639,5712647,5714051,5732271,5737800,5744348,5747066,5747106,5748810,5759562,5779500,5780225,5781970,5782900,48966262,49365955,49372463,49375342,49376021,49378909,

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:52:17.817081928 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:17.817167997 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.817317963 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:17.817409039 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:17.817461014 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:17.817568064 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:17.817940950 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:17.817984104 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.818413973 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:17.818465948 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:17.911799908 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:17.913811922 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:17.913855076 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:17.915894985 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:17.915971994 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:17.925100088 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.926182032 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:17.926264048 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.927247047 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.927382946 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:17.928548098 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:17.928652048 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.214133978 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.214572906 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.214643955 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.214972019 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.215132952 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.215152025 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.215281963 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.252743959 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.252851963 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.252871990 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.253019094 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.253084898 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.253606081 CEST	49709	443	192.168.2.6	216.58.215.238
May 26, 2023 11:52:18.253638029 CEST	443	49709	216.58.215.238	192.168.2.6
May 26, 2023 11:52:18.260288000 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.266479969 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.266510010 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.295067072 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.295207024 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.295254946 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.295407057 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:18.295475960 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.328648090 CEST	49710	443	192.168.2.6	172.217.168.45
May 26, 2023 11:52:18.328706026 CEST	443	49710	172.217.168.45	192.168.2.6
May 26, 2023 11:52:19.432224989 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.432301998 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.432404041 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.432882071 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.432924032 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.433784962 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.433852911 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.433934927 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.434542894 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.434583902 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.496968985 CEST	443	49712	172.217.168.14	192.168.2.6

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:52:19.497133017 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.497395039 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.497459888 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.497546911 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.497606993 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.498070002 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.498178959 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.498322010 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.498429060 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.499126911 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.499233007 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.499385118 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.499453068 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.509076118 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.509421110 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.509430885 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.509545088 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.510083914 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.510127068 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.549348116 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.549388885 CEST	443	49713	172.217.168.14	192.168.2.6
May 26, 2023 11:52:19.589385986 CEST	49713	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:19.635334015 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.206237078 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.206473112 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.206558943 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.206630945 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.206825972 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.206908941 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.206924915 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.206944942 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.207003117 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.207571983 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.208590031 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.208647013 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.208692074 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.208719015 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.208776951 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.209647894 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.210673094 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.210728884 CEST	443	49712	172.217.168.14	192.168.2.6
May 26, 2023 11:52:20.210756063 CEST	49712	443	192.168.2.6	172.217.168.14
May 26, 2023 11:52:20.210772038 CEST	443	49712	172.217.168.14	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:52:17.776421070 CEST	62910	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:17.777230024 CEST	63863	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:17.799540997 CEST	53	62910	8.8.8.8	192.168.2.6
May 26, 2023 11:52:17.805440903 CEST	53	63863	8.8.8.8	192.168.2.6
May 26, 2023 11:52:19.328315020 CEST	54903	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:19.370168924 CEST	53	54903	8.8.8.8	192.168.2.6
May 26, 2023 11:52:20.704629898 CEST	53943	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:20.732867956 CEST	53	53943	8.8.8.8	192.168.2.6
May 26, 2023 11:52:20.965207100 CEST	56086	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:20.980113029 CEST	53	56086	8.8.8.8	192.168.2.6
May 26, 2023 11:52:21.499419928 CEST	62520	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:21.532278061 CEST	53	62520	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 26, 2023 11:52:21.662101984 CEST	55629	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:21.685375929 CEST	53	55629	8.8.8.8	192.168.2.6
May 26, 2023 11:52:21.696335077 CEST	52079	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:21.719547987 CEST	53	52079	8.8.8.8	192.168.2.6
May 26, 2023 11:52:45.333854914 CEST	55956	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:45.353858948 CEST	53	55956	8.8.8.8	192.168.2.6
May 26, 2023 11:52:46.886775017 CEST	61089	53	192.168.2.6	8.8.8.8
May 26, 2023 11:52:46.906850100 CEST	53	61089	8.8.8.8	192.168.2.6
May 26, 2023 11:53:21.308495998 CEST	51362	53	192.168.2.6	8.8.8.8
May 26, 2023 11:53:21.336286068 CEST	53	51362	8.8.8.8	192.168.2.6
May 26, 2023 11:53:21.727843046 CEST	59965	53	192.168.2.6	8.8.8.8
May 26, 2023 11:53:21.742500067 CEST	53	59965	8.8.8.8	192.168.2.6
May 26, 2023 11:54:21.787348986 CEST	57054	53	192.168.2.6	8.8.8.8
May 26, 2023 11:54:21.802145958 CEST	53	57054	8.8.8.8	192.168.2.6
May 26, 2023 11:54:21.805433035 CEST	64638	53	192.168.2.6	8.8.8.8
May 26, 2023 11:54:21.828772068 CEST	53	64638	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 26, 2023 11:52:17.776421070 CEST	192.168.2.6	8.8.8.8	0x9d3d	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:17.777230024 CEST	192.168.2.6	8.8.8.8	0x6f0d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:19.328315020 CEST	192.168.2.6	8.8.8.8	0x8d9a	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:20.704629898 CEST	192.168.2.6	8.8.8.8	0x9098	Standard query (0)	apis.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:20.965207100 CEST	192.168.2.6	8.8.8.8	0x682d	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.499419928 CEST	192.168.2.6	8.8.8.8	0xd61f	Standard query (0)	blobcomments-pa.clients6.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.662101984 CEST	192.168.2.6	8.8.8.8	0x1ffd	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.696335077 CEST	192.168.2.6	8.8.8.8	0x35c8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:45.333854914 CEST	192.168.2.6	8.8.8.8	0x1d04	Standard query (0)	lh3.googleusercontent.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:46.886775017 CEST	192.168.2.6	8.8.8.8	0x13bd	Standard query (0)	peoplestackwebexperiments-pa.clients6.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:53:21.308495998 CEST	192.168.2.6	8.8.8.8	0xc7a8	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:53:21.727843046 CEST	192.168.2.6	8.8.8.8	0x8935	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:54:21.787348986 CEST	192.168.2.6	8.8.8.8	0x7dbc	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 26, 2023 11:54:21.805433035 CEST	192.168.2.6	8.8.8.8	0x165a	Standard query (0)	www.google.com	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
May 26, 2023 11:52:17.799540997 CEST	8.8.8.8	192.168.2.6	0x9d3d	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:52:17.799540997 CEST	8.8.8.8	192.168.2.6	0x9d3d	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:17.805440903 CEST	8.8.8.8	192.168.2.6	0x6f0d	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false

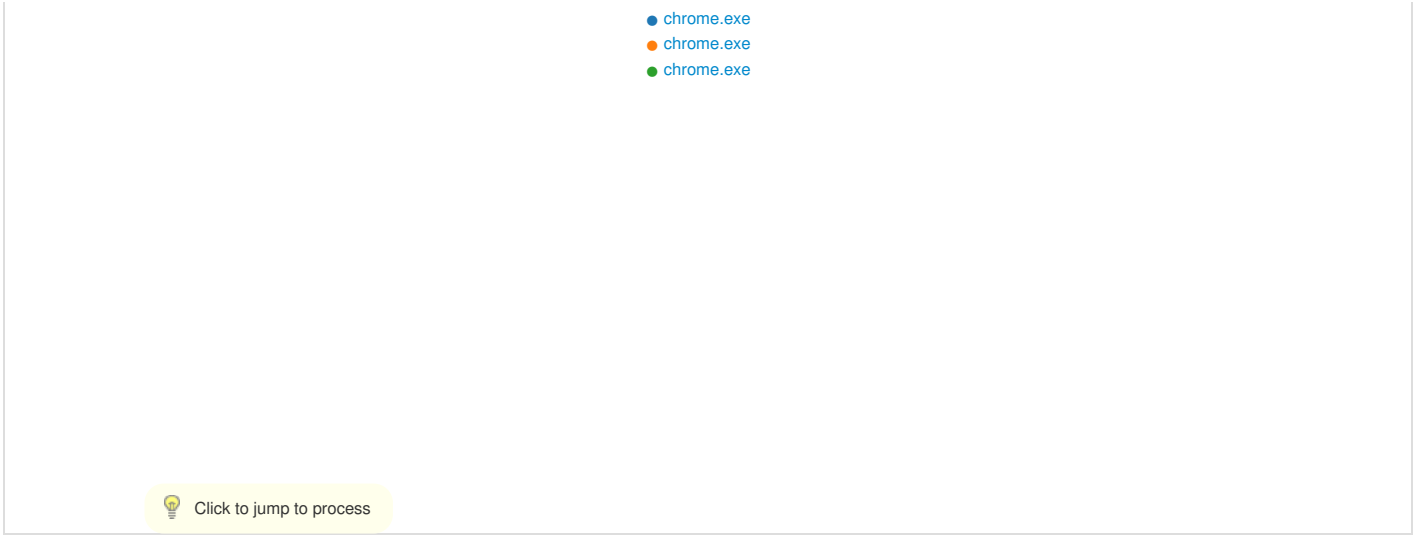
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 26, 2023 11:52:19.370168924 CEST	8.8.8.8	192.168.2.6	0x8d9a	No error (0)	drive.google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:20.732867956 CEST	8.8.8.8	192.168.2.6	0x9098	No error (0)	apis.google.com	plus.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:52:20.732867956 CEST	8.8.8.8	192.168.2.6	0x9098	No error (0)	plus.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:20.980113029 CEST	8.8.8.8	192.168.2.6	0x682d	No error (0)	play.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.532278061 CEST	8.8.8.8	192.168.2.6	0xd61f	No error (0)	blobcomments-pa.clients6.google.com		142.250.203.106	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.685375929 CEST	8.8.8.8	192.168.2.6	0x1ffd	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:21.719547987 CEST	8.8.8.8	192.168.2.6	0x35c8	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:45.353858948 CEST	8.8.8.8	192.168.2.6	0x1d04	No error (0)	lh3.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
May 26, 2023 11:52:45.353858948 CEST	8.8.8.8	192.168.2.6	0x1d04	No error (0)	googlehosted.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)	false
May 26, 2023 11:52:46.906850100 CEST	8.8.8.8	192.168.2.6	0x13bd	No error (0)	peoplestackwebexperiments-pa.clients6.google.com		216.58.215.234	A (IP address)	IN (0x0001)	false
May 26, 2023 11:53:21.336286068 CEST	8.8.8.8	192.168.2.6	0xc7a8	No error (0)	play.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
May 26, 2023 11:53:21.742500067 CEST	8.8.8.8	192.168.2.6	0x8935	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:54:21.802145958 CEST	8.8.8.8	192.168.2.6	0x7dbc	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false
May 26, 2023 11:54:21.828772068 CEST	8.8.8.8	192.168.2.6	0x165a	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- drive.google.com
- https:
  - apis.google.com
  - play.google.com
  - lh3.googleusercontent.com

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5288, Parent PID: 2372

General

Target ID:	0
Start time:	11:52:15
Start date:	26/05/2023
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:	0x7ff6f9750000
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

Analysis Process: chrome.exe PID: 5780, Parent PID: 5288

General

Target ID:	1
Start time:	11:52:16
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Copyright Joe Security LLC 2023

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1944 --field-trial-handle=1720,i,4096288064433636703,17727572675558076264,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
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

Analysis Process: chrome.exe PID: **5508**, Parent PID: **2372**

General

Target ID:	2
Start time:	11:52:18
Start date:	26/05/2023
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://drive.google.com/file/d/1Aau7Aza1Kdf_IYLUiT_3CLuLEAY5qdph/view?usp=drive_web
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly