ID: 1400707
Cookbook: browseurl.jbs
Time: 08:38:57
Date: 29/02/2024
Version: 40.0.0 Tourmaline

Table of Contents

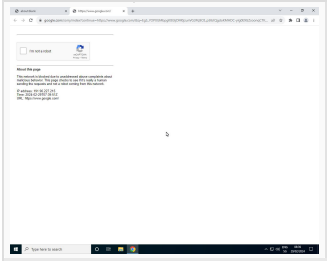
Windows Analysis Report

http://link.jschoenconsultingco.com/

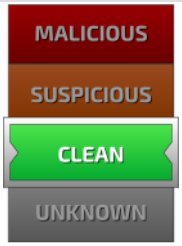
Overview

General Information

Sample URL:	http://link.jschoenconsultingco.com/
Analysis ID:	1400707
Infos:	



Detection

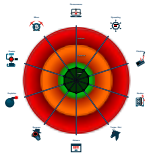


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 1376 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
  - chrome.exe (PID: 5572 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=2228 --field-trial-handle=2168,i,5198871792002701054,9817953159442565843,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8 MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- chrome.exe (PID: 6500 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "http://link.jschoenconsultingco.com/ MD5: 45DE480806D1B5D462A7DDE4DCEFC4E4)
- 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

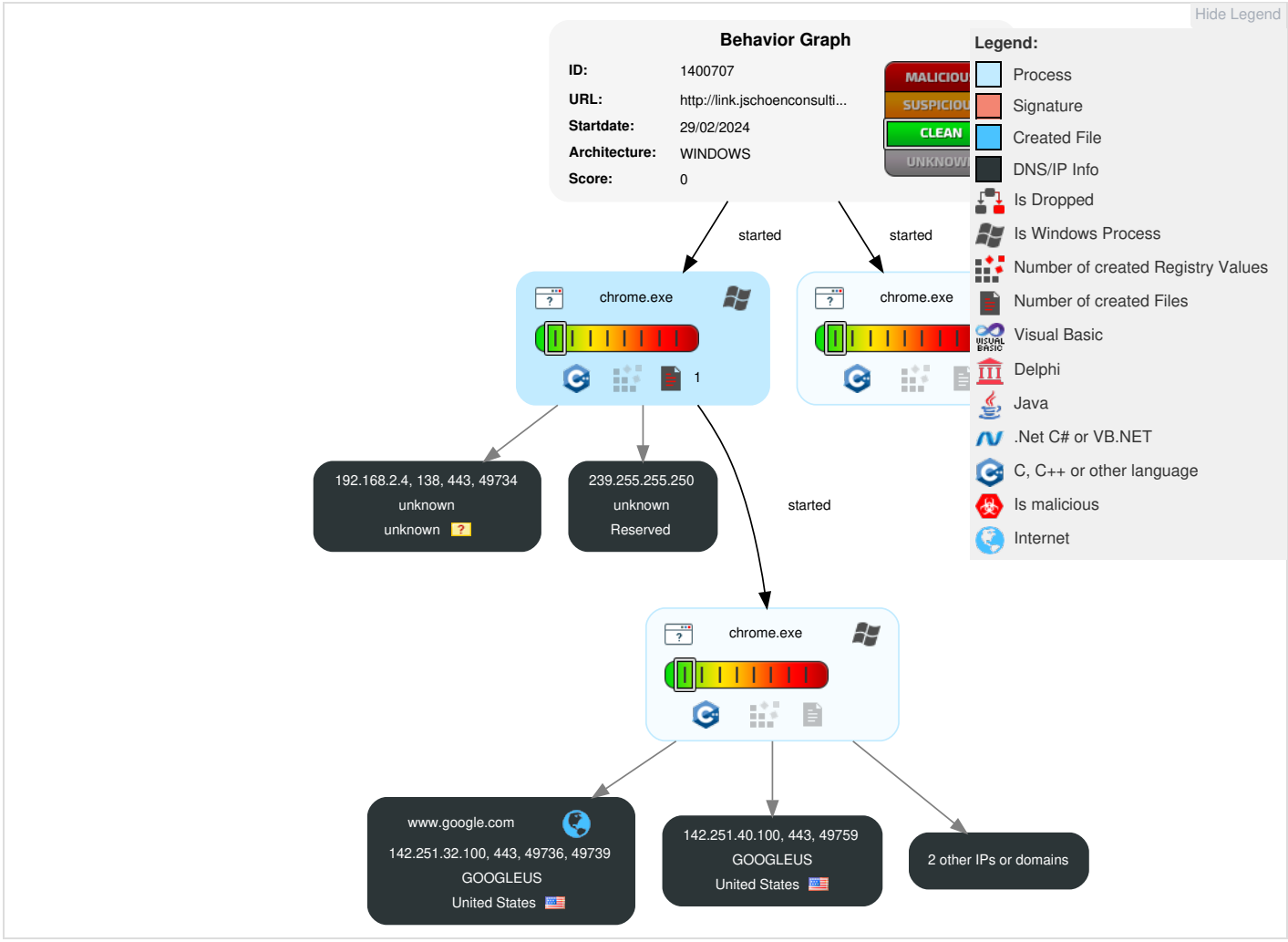
Joe Sandbox Signatures

There are no malicious signatures

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	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	2 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	3 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	1 Ingress Tool Transfer	Traffic Duplication	Data Destruction

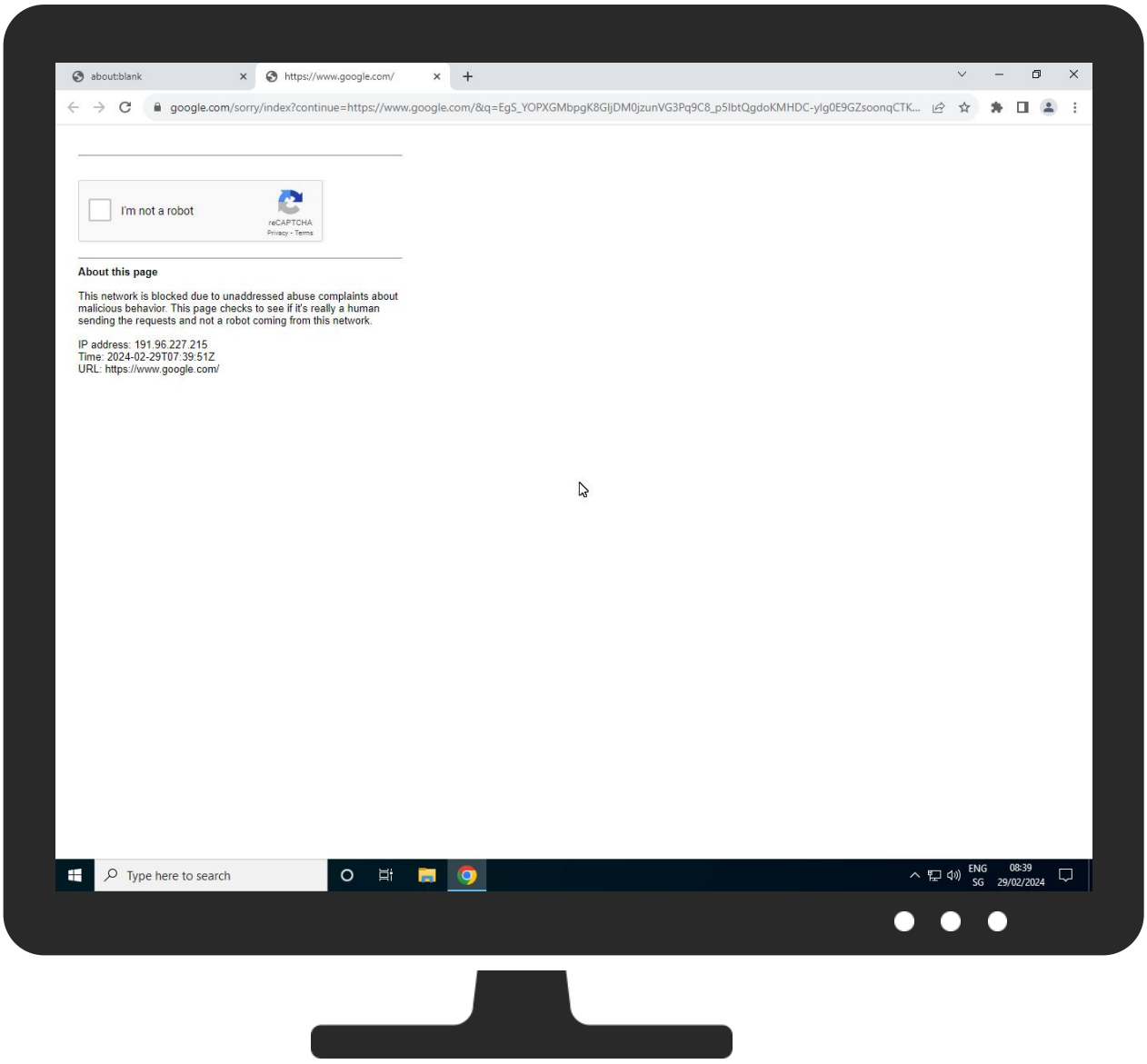
Behavior Graph



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://link.jschoenconsultingco.com/	0%	Avira URL Cloud	safe	
http://link.jschoenconsultingco.com/	1%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
link.jschoenconsultingco.com	1%	Virustotal		Browse
fp2e7a.wpc.phicdn.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://recaptcha.net	0%	URL Reputation	safe	
http://https://recaptcha.net	0%	URL Reputation	safe	
http://https://www.gstatic.c..?/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__.	0%	URL Reputation	safe	
about:blank	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.google.com	142.251.32.100	true	false		high
custom.autoklose.com	35.222.146.56	true	false		high
fp2e7a.wpc.phicdn.net	192.229.211.108	true	false	• 0%, Virustotal, Browse	unknown
link.jschoenconsultingco.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

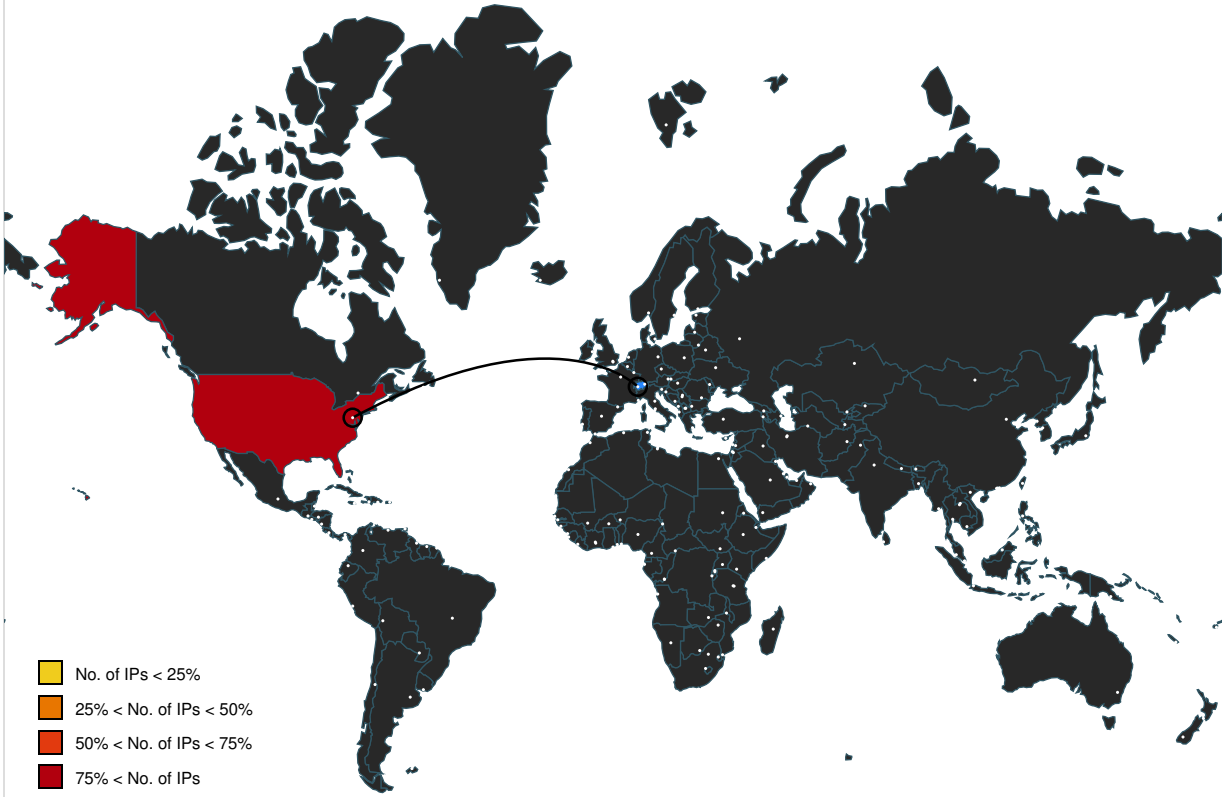
Name	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/recaptcha/api.js	false		high
http://https://www.google.com/js/bg/722MIWu_TMZiQau3mAaarHtCk2pd6rTYw5oNsH4wR_g.js	false		high
http://https://www.google.com/recaptcha/api2/bframe?hl=en&v=1kRDYC3bfA-o6-tsWzIBvp7k&k=6LfwuyUTAAAAAOAmoS0fdqijC2PbbdH4kjq62Y1b	false		high
about:blank	false	• Avira URL Cloud: safe	low
http://https://www.google.com/	false		high
http://link.jschoenconsultingco.com/	false		unknown
http://https://www.google.com/sorry/index?continue=https://www.google.com/&q=EgS_YOPXGMbpgK8GIjDM0jzunVG3Pq9C8_p5lbtQgdoKMHDC-yIg0E9GZsoonqCTKFjaHWbLvRCdKXGn0-4yAXJKGVNPUlJZX0FCVVNJVkVfTkVUX01FU1NBR0VaAUM	false		high
http://https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LfwuyUTAAAAAOAmoS0fdqijC2PbbdH4kjq62Y1b&co=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbTo0NDM.&hl=en&v=1kRDYC3bfA-o6-tsWzIBvp7k&size=normal&s=SJMv6d_Y3rtpRU1dZxBWoLycSG3oTNhRUgLWbZXALt-npqYKQ-ZbbZwf7zIhBct_gKIax55iTMFgrLqb3Kp0Ul25oxXgX_0tu2jWCkwg-yzJxFxTPF3fFBFr63ny_eeasrd2REhhMop-kacaKeULBBP4el3cmpv4c70Hhpl7Eky3z8R2OlGcOwKq3jaY5KHEicYv7Frh5xJSYHcVdbYW8Voup6KOqgkxcljh3Uods9K5LCrFAhhGYDH43c6z9mnkxwQLqH-W5v9w7Ws8e2LDjVfiIZBXiMI&cb=vfor8c80z1l5	false		high
http://https://www.google.com/favicon.ico	false		high
http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=1kRDYC3bfA-o6-tsWzIBvp7k	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://play.google.com/log?format=json&hasfast=true	chromecache_55.2.dr	false		high
http://https://developers.google.com/recaptcha/docs/faq#are-there-any-qps-or-daily-limits-on-my-use-of-reca	chromecache_55.2.dr	false		high
http://https://developers.google.com/recaptcha/docs/faq#localhost_support	chromecache_55.2.dr	false		high
http://https://support.google.com/recaptcha/#6175971	chromecache_55.2.dr	false		high
http://https://support.google.com/recaptcha#6262736	chromecache_55.2.dr	false		high
http://https://cloud.google.com/recaptcha-enterprise/billing-information	chromecache_55.2.dr	false		high
http://https://recaptcha.net	chromecache_55.2.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.google.com/log?format=json&hasfast=true	chromecache_55.2.dr	false		high
http://https://www.google.com/recaptcha/api2/	chromecache_55.2.dr, chromecache_53.2.dr	false		high
http://https://support.google.com/recaptcha/?hl=en#6223828	chromecache_55.2.dr	false		high
http://https://cloud.google.com/contact	chromecache_55.2.dr	false		high
http://https://support.google.com/recaptcha	chromecache_55.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.gstatic.c..?/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__.	chromecache_55.2.dr	false	• URL Reputation: safe	low
http://https://developers.google.com/recaptcha/docs/faq#my-computer-or-network-may-be-sending-automated-que	chromecache_55.2.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.251.40.100	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.251.32.100	www.google.com	United States		15169	GOOGLEUS	false
35.222.146.56	custom.autoklose.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.4

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1400707
Start date and time:	2024-02-29 08:38:57 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 3m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://link.jschoenconsultingco.com/
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01

Number of analysed new started processes analysed:	8
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@17/20@6/5
EGA Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.251.40.195, 142.251.40.142, 172.253.63.84, 34.104.35.123, 142.250.80.35, 142.250.65.170, 142.251.40.202, 142.250.65.234, 142.251.35.170, 142.250.81.234, 142.250.72.106, 142.250.176.202, 142.250.80.42, 142.251.32.106, 142.251.41.10, 142.250.80.10, 142.250.80.74, 142.250.65.202, 142.251.40.234, 142.250.64.106, 142.250.80.106, 142.250.80.67, 13.85.23.86, 72.21.81.240, 192.229.211.108, 13.85.23.206, 20.166.126.56, 142.250.176.195
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, clientservices.googleapis.com, wu.azureedge.net, clients2.google.com, ocsp.digicert.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, ocsp.edge.digicert.com, glb.cws.prod.dcat.dsp.trafficmanager.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, www.gstatic.com, glb.sls.prod.dcat.dsp.trafficmanager.net, fs.microsoft.com, accounts.google.com, content-autofill.googleapis.com, fonts.gstatic.com, wu.ec.azureedge.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, fe3cr.delivery.mp.microsoft.com, fe3.delivery.mp.microsoft.com, edgedl.me.gvt1.com, clients.l.google.com
- HTTPS proxy raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile 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

Chrome Cache Entry: 48

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (17256), with no line terminators
Category:	downloaded
Size (bytes):	17256
Entropy (8bit):	5.53116771237722
Encrypted:	false
SSDEEP:	384:9NZkA7rPe5uwZBDXiKp56VhgQXdl5GpZbAvWzyUj:SAHZwl6rMpZUu5
MD5:	1D6072146DC8D80DC70FF94257474E51
SHA1:	42CBA58A012A23743FF4A338C390A56DFD49C4FD
SHA-256:	EF6D8C216BBF4CC66241ABB798069AAC7B42936A5DEAB4D8C39A0DB07E3047F8
SHA-512:	93D8618477D8B7AB37CE9127225CD278CC554645B32806106224641AB23A4898231D1C099C263BA69364CFAB76B8398E13CFE68C7AB5C0CA379F861F7310DCF
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/js/bg/722MIWu_TMZiQau3mAaarHtCk2pd6rTYw5oNsH4wR_g.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var W=this||self,N=function(t,h){if(!(t=(h=W.trustedTypes,null),h)||!h.createPolicy)return t;try{t=h.createPolicy("bg",{createHTML:u,createScript:u,createScriptURL:u})}catch(l){W.console&&W.console.error(l.message)}return t},u=function(t){return t};(0,eval)(function(t,h){return(h=N())&&1===t.eval(h.createScript("1"))?function(l){return h.createScript(l)}:function(l){return""+l}}(W)(Array(7824*Math.random()|0).join("\n")+'(function(){var G=function(t,h,W){t[f(W,h,t),t6]=2796},je=function(t,h,W,u){X(h,(u=p((W=p(h),h)),u),F(t,E(h,W)))},A={passive:true,capture:true},h6=function(t,h){(h.push(t[0]<<24|t[1]<<16|t[2]<<8|t[3]),h.push(t[4]<<24|t[5]<<16|t[6]<<8|t[7]),h).push(t[8]<<24|t[9]<<16|t[10]<<8|t[11])},lZ=function(t,h){return h=0,function(){return h<t.length?{done:false,value:t[h++]}:{done:true}}},b=function(t,h){h.o=((h.o?h.o+"~":"E:")+t.message+":"+t.stack).slice(0,2048)},WH=function(t,h

Chrome Cache Entry: 49

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wlJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wlJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/favicon.ico
Preview:	..... .h...&... ....(..... ....0.....v.].X.:.X.:.r.Y.....q.X.S.4.S.4.S.4.S.4.S.4...X.....0.....q.W.S.4.X.:.....J...A...g.....K.H.V.8.....F..B.....B.....B..B..B..B..B...u.....B..B..B..B..B...{.....5.....k.....7R..8F.....2.....Vb..5C..;I.....R^.....0.....Xc..5C..5C..5C..5C..5C..5C..lv.....]i..<J..:G..Zf.....

Chrome Cache Entry: 50

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (56398), with no line terminators
Category:	downloaded
Size (bytes):	56398
Entropy (8bit):	5.907604034780877
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKYlebyB5lxRx54PHSGdXXwW7MFWwXVuE2:4UcW6v+0B5chXwW49z2
MD5:	EB4BC511F79F7A1573B45F5775B3A99B
SHA1:	D910FB51AD7316AA54F055079374574698E74B35
SHA-256:	7859A62E04B0ACB06516EB12454DE6673883ECFAEAED6C254659BCA7CD59C050
SHA-512:	EC9BDF1C91B6262B183FD23F640EAC22016D1F42DB631380676ED34B962E01BADDA91F9CBDFA189B42FE3182A992F1B95A7353AF41E41B2D6E1DAB17E87637A0
Malicious:	false
Reputation:	low

URL:	http://https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit-border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-index:1}.recaptcha-checkbox-borderAnimation{background-image:url(
Preview:	Cut (see below)

Chrome Cache Entry: 51	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.954234440752388
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKPMwmIknZSSZgWaee:PLKdXNQKss6gL
MD5:	7E005BC0107FE8DD6255D4253228EF02
SHA1:	718501672A9B00AFFE1D688D7B3F2F6202E3E96E
SHA-256:	80663B7D03F283B27D8D833CA725A43D5CD3D5B5A7DD6487970DCA9469F9C139
SHA-512:	3F17B8CCEF75B49E01343A33D14744D589C87EC2A574B529E7EC65ED921C47D6D4A6F768CA4229B4A0B9E87D6624D76E0B4241AD214014305A9AA8E76643315
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=1kRDYC3bfA-o6-tsWzIBvp7k
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js');

Chrome Cache Entry: 52	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	5430
Entropy (8bit):	3.6534652184263736
Encrypted:	false
SSDEEP:	48:wIJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wIJct+A47v+rcqlBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA5620880159634213E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B370 2563
Malicious:	false
Reputation:	low
Preview:	.... .h...&... ....(....... ....0...v.].X.:.X.:.r.Y................ ....q.X.S.4.S.4.S.4.S.4.S.4.S.4...X....................0........q.W.S.4.X.:.................J...A...g.........................K.H.V.8.........................F..B..................,......................... ..............B..B..B..B..B..B...u...B..B..B..B..B...{.................5.......k...7R..8F............ ....2........Vb..5C..;I..................R^.....................0................Xc..5C..5C..5C..5C..5C..5C..lv..]i..<J..:G..Zf.............................. ....

Chrome Cache Entry: 53	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1222), with no line terminators
Category:	downloaded
Size (bytes):	1222
Entropy (8bit):	5.821461377873524
Encrypted:	false
SSDEEP:	24:2jkm94/zKPccAv+KVCLTLv138EgFB5vtTGJTlWtZ1v8IgsLqo40RWUnYN:VKEctKonR3evtTA871v8IhLrwUnG
MD5:	AF236E134BD0FB0FB4945E14343C4F72
SHA1:	4293C60ACE63C1685AB3218E8705E8338A3E1E0F
SHA-256:	9ED2048AF008ABE9739E5658331FA63F436F359C2085099E7636F191BC5D1A9D
SHA-512:	657F76AC4B5DED234C45C03DCB0F2B5B261848C1437A4C5FD6A7592285CFB67D743F7194DFB8D058FE79F26D1455747B83F4F15D543622512CD974052B010E2
Malicious:	false
Reputation:	low
URL:	http://https://www.google.com/recaptcha/api.js

Preview:	/* PLEASE DO NOT COPY AND PASTE THIS CODE. */(function(){var w=window,C='___grecaptcha_cfg',cfg=w[C]=w[C]||{},N='grecaptcha';var gr=w[N]=w[N]||{};gr.ready=gr.ready||function(f){(cfg['fns']=cfg['fns']||[]).push(f);};w['__recaptcha_api']='https://www.google.com/recaptcha/api2/';(cfg['render']=cfg['render']||[]).push('onload');w['__google_recaptcha_client']=true;var d=document,po=d.createElement('script');po.type='text/javascript';po.async=true;var m=d.createElement('meta');m.httpEquiv='origin-trial';m.content='Az520Inasey3TAyqLyojQa8MnmCALSEU29yQFW8dePZ7xQTvSt73pHazLFTK5f7SyLUJSo2uKLesEtEa9aUYcgMAAACPeyJvcmlnaW4iOiJodHRwczovL2dvb2dsZS5jb206NDQzIiwiZmVhdHVyZSI6IkRpc2FibGVUaGlyZFBhcnR5U3RvcmFnZVBhcnRpdGlvbmluZyIsImV4cGlyeSI6MTcyNTQwNzk5OSwiaXNTdWJkb21haW4iOnRydWUsImlzVGhpcmRQYXJ0eSI6dHJ1ZX0=';d.head.prepend(m);po.src='https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js';po.crossOrigin='anonymous';po.integrity='sha384-mOWLSQycXikmw9Z/tMAEHluYe0wwJfLBh1efKEgK

Chrome Cache Entry: 54	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D9
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PIP8..;.C.1iL#6...*.Z..!.....3.po.o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\..._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"lc.LB.....jG.uD..B....Tm....T.).).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....|...)..KS4....I.....W...@....S.s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....I.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

Chrome Cache Entry: 55	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (568)
Category:	downloaded
Size (bytes):	503430
Entropy (8bit):	5.708119764112345
Encrypted:	false
SSDEEP:	6144:HEYt9e4UlnQyfZLsIB74RSHywNGte2fp0YROQVZT+DSUAZqH/:Hi9fpj140SwQz0YRO+ZSj/
MD5:	3E528C5BD4E8985F914F84BC5F86DF5F
SHA1:	34104EA645A6789DD9CB58C264E20ED6855EA1DE
SHA-256:	E51E616D124133B0FB24968469097A4D311B972F78455143D940703EA0639BA6
SHA-512:	C59A1D40F649446F33FF0FF3FA9A8E997D3CFF10F968D35226BA08BB91C9013AE937460CF2DAB0888848ABE1B693D4377FBD6904E3E03360B15035A8C3E9BC9
Malicious:	false
Reputation:	low
URL:	http://https://www.gstatic.com/recaptcha/releases/1kRDYC3bfA-o6-tsWzIBvp7k/recaptcha__en.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2005, 2007 Bob Ippolito. All Rights Reserved.. Copyright The Closure Library Authors.. SPDX-License-Identifier: MIT.*/./*. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var C=function(){return[function(f,q,S,Z,P,X,U){return(f|((X=[1,6,4],(f+X[1]&X[2])<X[0]&&3<=((f^17)&7))&&(this.X=S,this.N=q),X[1]))>>3||(P=0,P=void 0===P?0:P,U=l[16](14,q,L[13](26,Z,S),P)),U},function(f,q,S,Z,P,X,U,b,k,E,J,K,B,n,F,c){if(1<=(f|(F=(f-7>>3||(c=q instanceof qd&&q.constructor===qd?q.N:"type_error:SafeUrl"),["T","call",0]),72))==f&&(c=u[22](26,function(r,g,m){m=["could not contact reCAPTCHA.",15,(g=[2,3,6],"recaptcha::2fa")];switch(r.N){case 1:if(!U.C)throw Error(m[0]);if(!U.X)return r.return(l[19](72,.g[0]));if("string"!==typeof X||X.length!=g[2])return r.return(l[19](32,P));return u[10]((r.C=g[0],m[1]),P,U.C,r);case P:C[2

Chrome Cache Entry: 56	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A

SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D9
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PIP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\..._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"lc.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....\|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+....(...S..\h....@.....I.$..%.2....I.....a.\.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

Chrome Cache Entry: 57

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:	7EB7C301DF79D35A6A521FAE9D3DCCC0A695D3480B4D34C7D262DD0C67ABEC8437ED40E2920625E98AAEAFBA1D908DEC69C3B07494EC7C29307DE49E91C2EF48
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.$..6. ..t. ..I.h\|.I....A....b6.....(.....@e.]...*:..-.0..r.)..hS..h...N.).D.....b.].....^..t?.m{...."84...9.....c...?..r3o.. ..}...S]....zbO.../z..{.....~cc....I...#.G.D....#*e.A..b...b`a5P.4.....M....v4..fI#X.z,.,..=avy..F.a.\9.P\|.[....r.Q@M.I.._.9..V..Q..].....[{u..L@...]..K.....]C....l$.Z.Z...Zs.4..... x..... ..F.?.7N..]..|.wb\....Z{1L#..t....0.dM...$JV...{..oX...i....6.v.~.....)\|.TtAP&).KQ.]y.....'...:.d..+..d..."C.h..p.2.M..e,.*UP..@.q..7..D.@...,.....B.n. r&.....F!.....\...;R.?-.i...,7..cb../I...Eg...!X.)5.Aj7...Ok..l7.j.A@B`".}.w.m..R.9..T.X.X.d....S..`Xl..1... .$C.H.,.\. ..A(.AZ.....`Wr.0]y..-..K.1.....1.tBs..n.0...9.F[b.3x...*$....T..PM.Z-.N.rS?I.<8eR'.3..27..?;..OLf*.Rj.@.o.W.....j~ATA....vX.N:.3dM.r.)Q.B...4i.f..K.l..s....e.U.2...k..a.GO.}..../.'..%$..ed.*.'..qP....M..j...../.z&.=...q<....-..?.A.%..K..

Chrome Cache Entry: 58

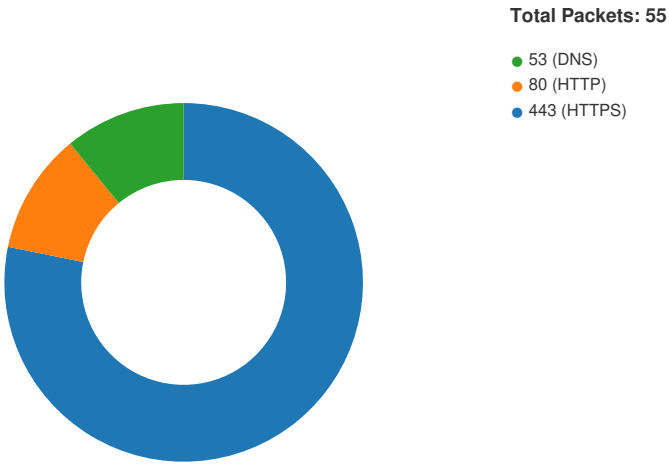
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	16
Entropy (8bit):	3.75
Encrypted:	false
SSDEEP:	3:H0hCkY:UUkY
MD5:	AFB69DF47958EB78B4E941270772BD6A
SHA1:	D9FE9A625E906FF25C1F165E7872B1D9C731E78E
SHA-256:	874809FB1235F80831B706B9E9B903D80BD5662D036B7712CC76F8C684118878
SHA-512:	FD92B98859FFCCFD12AD57830887259F03C7396DA6569C0629B64604CD964E0DF15D695F1A770D2E7F8DF238140F0E6DA7E7D176B54E31C3BB75DDE9B9127C4
Malicious:	false
Reputation:	low
URL:	http://https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTE3LjAuNTkzOC4xMzISEAk8dqZYMe7mkRIFDVNaR8U=?alt=proto
Preview:	CgkKBw1TWkfFGgA=

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 29, 2024 08:39:39.597486973 CET	49678	443	192.168.2.4	104.46.162.224
Feb 29, 2024 08:39:41.238322020 CET	49675	443	192.168.2.4	173.222.162.32
Feb 29, 2024 08:39:49.868393898 CET	49734	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:49.869128942 CET	49735	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:49.984452009 CET	80	49734	35.222.146.56	192.168.2.4
Feb 29, 2024 08:39:49.984539986 CET	49734	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:49.984733105 CET	49734	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:49.985043049 CET	80	49735	35.222.146.56	192.168.2.4
Feb 29, 2024 08:39:49.985121965 CET	49735	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:50.099013090 CET	80	49734	35.222.146.56	192.168.2.4
Feb 29, 2024 08:39:50.114965916 CET	80	49734	35.222.146.56	192.168.2.4
Feb 29, 2024 08:39:50.115014076 CET	80	49734	35.222.146.56	192.168.2.4
Feb 29, 2024 08:39:50.115082026 CET	49734	80	192.168.2.4	35.222.146.56
Feb 29, 2024 08:39:50.210946083 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.210973978 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.211040974 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.211654902 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.211678982 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.402690887 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.403157949 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.403177023 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.404174089 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.404257059 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.405375957 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.405447960 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.405575037 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.405581951 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.457973003 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.847434044 CET	49675	443	192.168.2.4	173.222.162.32
Feb 29, 2024 08:39:50.932271004 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.932338953 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.932351112 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.932379961 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.932430029 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.937838078 CET	49736	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.937851906 CET	443	49736	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.948515892 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.948559046 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:50.948649883 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.949753046 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:50.949779034 CET	443	49739	142.251.32.100	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 29, 2024 08:39:51.136454105 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.154604912 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.154628038 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.155019999 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.156188965 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.156251907 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.156572104 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.197907925 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.322866917 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.322899103 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.322935104 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.322952032 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.322987080 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.323014021 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.323034048 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.323079109 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.324949026 CET	49739	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.324980974 CET	443	49739	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.481379986 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.481410980 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.481486082 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.482445002 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.482460976 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.668884039 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.669203043 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.669222116 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.669508934 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.670991898 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.671047926 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.671535015 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.717912912 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.872546911 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.872649908 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:51.872708082 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.877928019 CET	49740	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:51.877945900 CET	443	49740	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.070045948 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.070092916 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.070163012 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.071258068 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.071280003 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.201839924 CET	49743	443	192.168.2.4	23.51.58.94
Feb 29, 2024 08:39:53.201958895 CET	443	49743	23.51.58.94	192.168.2.4
Feb 29, 2024 08:39:53.202047110 CET	49743	443	192.168.2.4	23.51.58.94
Feb 29, 2024 08:39:53.206763029 CET	49743	443	192.168.2.4	23.51.58.94
Feb 29, 2024 08:39:53.206796885 CET	443	49743	23.51.58.94	192.168.2.4
Feb 29, 2024 08:39:53.258352041 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.292864084 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.292891026 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.293277979 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.294183969 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.294250965 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.294660091 CET	49742	443	192.168.2.4	142.251.32.100
Feb 29, 2024 08:39:53.294688940 CET	443	49742	142.251.32.100	192.168.2.4
Feb 29, 2024 08:39:53.405193090 CET	443	49743	23.51.58.94	192.168.2.4
Feb 29, 2024 08:39:53.405316114 CET	49743	443	192.168.2.4	23.51.58.94
Feb 29, 2024 08:39:53.410325050 CET	49743	443	192.168.2.4	23.51.58.94
Feb 29, 2024 08:39:53.410367966 CET	443	49743	23.51.58.94	192.168.2.4
Feb 29, 2024 08:39:53.410792112 CET	443	49743	23.51.58.94	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 29, 2024 08:39:47.975641966 CET	53	53040	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:48.019260883 CET	53	64680	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:48.709408045 CET	53	55362	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:49.486093044 CET	60367	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:49.486399889 CET	59878	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:49.751461029 CET	53	59878	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:49.867130041 CET	53	60367	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:50.119218111 CET	65514	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:50.119573116 CET	53608	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:50.208758116 CET	53	65514	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:50.209983110 CET	53	53608	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:52.002919912 CET	53	63059	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:53.220463037 CET	53	60230	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:54.547789097 CET	53	57960	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:55.828419924 CET	53	61408	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:56.748756886 CET	65186	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:56.749463081 CET	57539	53	192.168.2.4	1.1.1.1
Feb 29, 2024 08:39:56.836888075 CET	53	65186	1.1.1.1	192.168.2.4
Feb 29, 2024 08:39:56.837611914 CET	53	57539	1.1.1.1	192.168.2.4
Feb 29, 2024 08:40:06.000442982 CET	53	57342	1.1.1.1	192.168.2.4
Feb 29, 2024 08:40:10.138386011 CET	138	138	192.168.2.4	192.168.2.255
Feb 29, 2024 08:40:25.049850941 CET	53	63585	1.1.1.1	192.168.2.4
Feb 29, 2024 08:40:47.460072041 CET	53	50806	1.1.1.1	192.168.2.4
Feb 29, 2024 08:40:48.142477989 CET	53	53592	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 29, 2024 08:39:49.486093044 CET	192.168.2.4	1.1.1.1	0xfc0c	Standard query (0)	link.jschoenconsultingco.com	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:49.486399889 CET	192.168.2.4	1.1.1.1	0xcfec	Standard query (0)	link.jschoenconsultingco.com	65	IN (0x0001)	false
Feb 29, 2024 08:39:50.119218111 CET	192.168.2.4	1.1.1.1	0x36ce	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:50.119573116 CET	192.168.2.4	1.1.1.1	0xe78d	Standard query (0)	www.google.com	65	IN (0x0001)	false
Feb 29, 2024 08:39:56.748756886 CET	192.168.2.4	1.1.1.1	0x556b	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:56.749463081 CET	192.168.2.4	1.1.1.1	0xce9f	Standard query (0)	www.google.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 29, 2024 08:39:49.751461029 CET	1.1.1.1	192.168.2.4	0xcfec	No error (0)	link.jschoenconsultingco.com	custom.autoklose.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:39:49.867130041 CET	1.1.1.1	192.168.2.4	0xfc0c	No error (0)	link.jschoenconsultingco.com	custom.autoklose.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:39:49.867130041 CET	1.1.1.1	192.168.2.4	0xfc0c	No error (0)	custom.autoklose.com		35.222.146.56	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:50.208758116 CET	1.1.1.1	192.168.2.4	0x36ce	No error (0)	www.google.com		142.251.32.100	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:50.209983110 CET	1.1.1.1	192.168.2.4	0xe78d	No error (0)	www.google.com			65	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 29, 2024 08:39:56.836888075 CET	1.1.1.1	192.168.2.4	0x556b	No error (0)	www.google.com		142.251.40.100	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:39:56.837611914 CET	1.1.1.1	192.168.2.4	0xce9f	No error (0)	www.google.com			65	IN (0x0001)	false
Feb 29, 2024 08:40:04.545690060 CET	1.1.1.1	192.168.2.4	0xd162	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:40:04.545690060 CET	1.1.1.1	192.168.2.4	0xd162	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:40:17.607615948 CET	1.1.1.1	192.168.2.4	0x3d01	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:40:17.607615948 CET	1.1.1.1	192.168.2.4	0x3d01	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:40:40.140090942 CET	1.1.1.1	192.168.2.4	0x651a	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:40:40.140090942 CET	1.1.1.1	192.168.2.4	0x651a	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false
Feb 29, 2024 08:41:00.520751953 CET	1.1.1.1	192.168.2.4	0x5fdd	No error (0)	fp2e7a.wpc.2be4.phicdn.net	fp2e7a.wpc.phicdn.net		CNAME (Canonical name)	IN (0x0001)	false
Feb 29, 2024 08:41:00.520751953 CET	1.1.1.1	192.168.2.4	0x5fdd	No error (0)	fp2e7a.wpc.phicdn.net		192.229.211.108	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.google.com
- https:
- fs.microsoft.com
- link.jschoenconsultingco.com

Statistics

Behavior

All data are 0.

System Behavior

Analysis Process: chrome.exe PID: 1376, Parent PID: 5848

General

Target ID:	0
Start time:	08:39:43
Start date:	29/02/2024
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:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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

Analysis Process: chrome.exe PID: **5572**, Parent PID: **1376**

General

Target ID:	2
Start time:	08:39:46
Start date:	29/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2228 --field-trial-handle=2168,i,5198871792002701054,9817953159442565843,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes
MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	false

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: **6500**, Parent PID: **5848**

General

Target ID:	3
Start time:	08:39:48
Start date:	29/02/2024
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "http://link.jschoenconsultingco.com/
Imagebase:	0x7ff76e190000
File size:	3'242'272 bytes

MD5 hash:	45DE480806D1B5D462A7DDE4DCEFC4E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

Disassembly

No disassembly