



ID: 715056
Cookbook: browseurl.jbs
Time: 15:38:48
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://youtu.be/BKUwZGqpxXY 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 9
Public IPs 9
Private 9
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
Network Behavior 11
Statistics 11
Behavior 11
System Behavior 11
Analysis Process: chrome.exePID: 5892, Parent PID: 4612 11
General 11
File Activities 12
Registry Activities 12
Analysis Process: chrome.exePID: 4388, Parent PID: 5892 12
General 12
File Activities 12
Analysis Process: chrome.exePID: 5216, Parent PID: 4612 12
General 12
Registry Activities 13
Analysis Process: chrome.exePID: 6828, Parent PID: 5892 13
General 13
Analysis Process: chrome.exePID: 7116, Parent PID: 5892 13
General 13
File Activities 13
Registry Activities 14
Disassembly 14

Copyright Joe Security LLC 2022

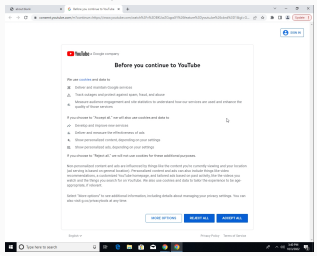
Windows Analysis Report

https://youtu.be/BKUwZGqpxXY

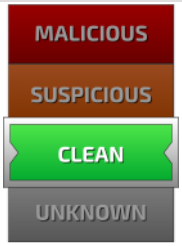
Overview

General Information

Sample URL:	http://https://youtu.be/BKUwZGqpxXY
Analysis ID:	715056
Infos:	



Detection

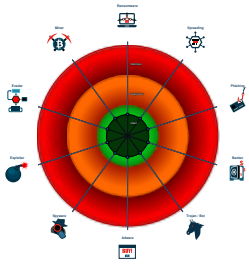


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 5892 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 4388 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=1960 --field-trial-handle=1764,i,17618918851396802 10,6239086101532742970,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 6828 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5480 --field-trial-handle=1764,i,17618918851396802 10,6239086101532742970,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 7116 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=3820 --field-trial-handle=1764,i,17618918851396802 10,6239086101532742970,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5216 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://youtu.be/BKUwZGqpxXY 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 2022

Snort Signatures

No Snort rule has matched

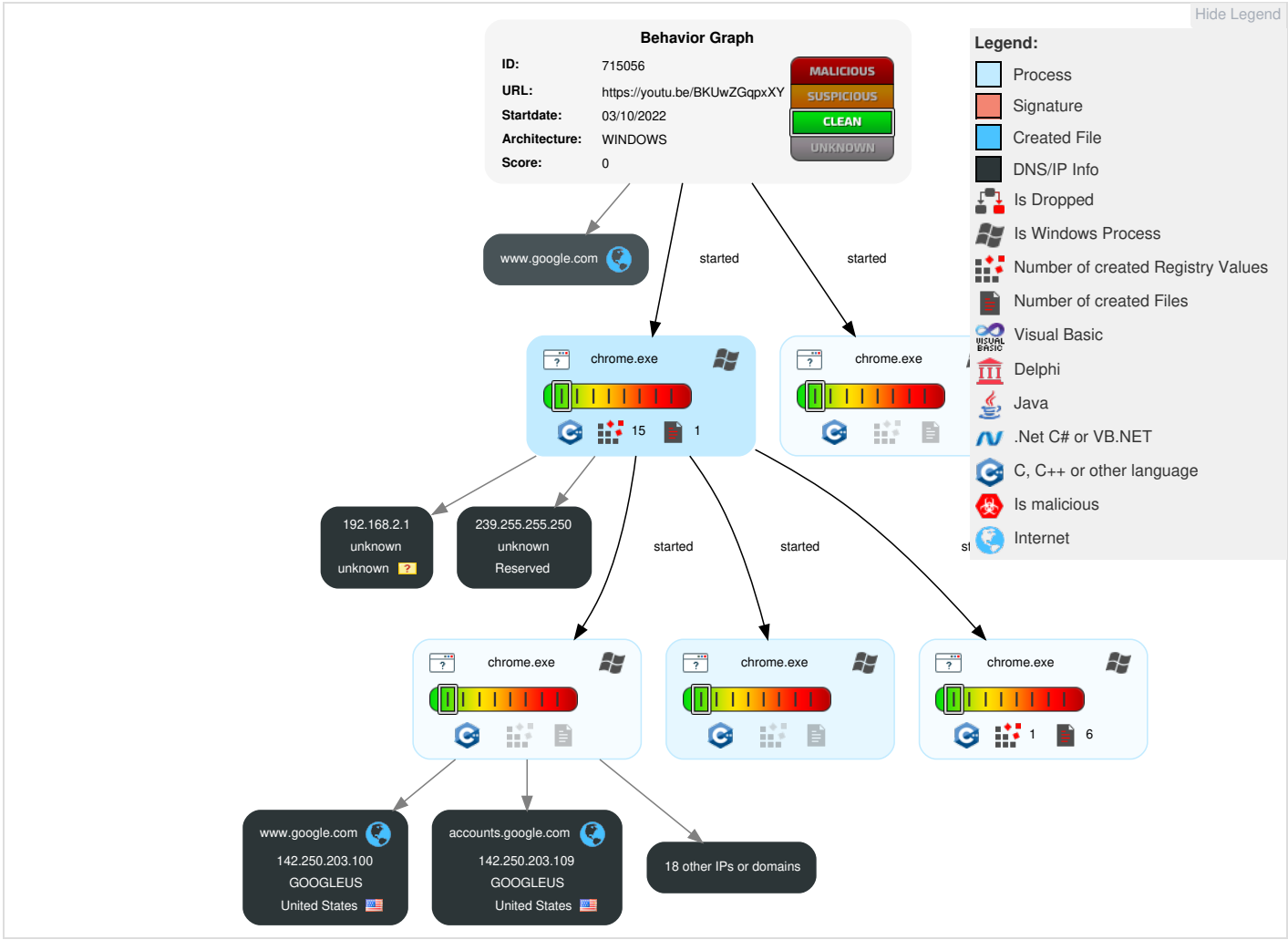
Joe Sandbox Signatures

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	4 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	5 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

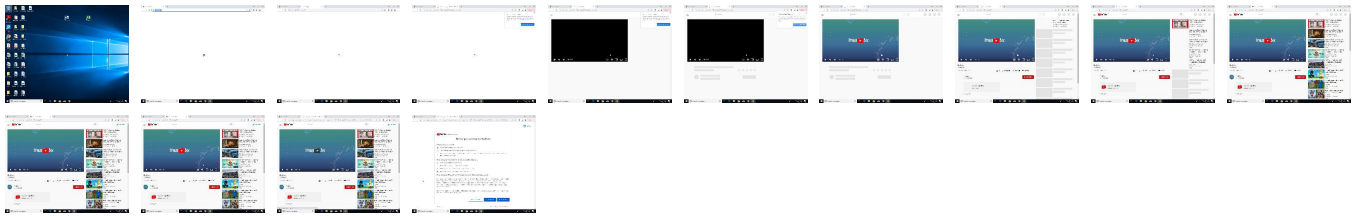
Behavior Graph

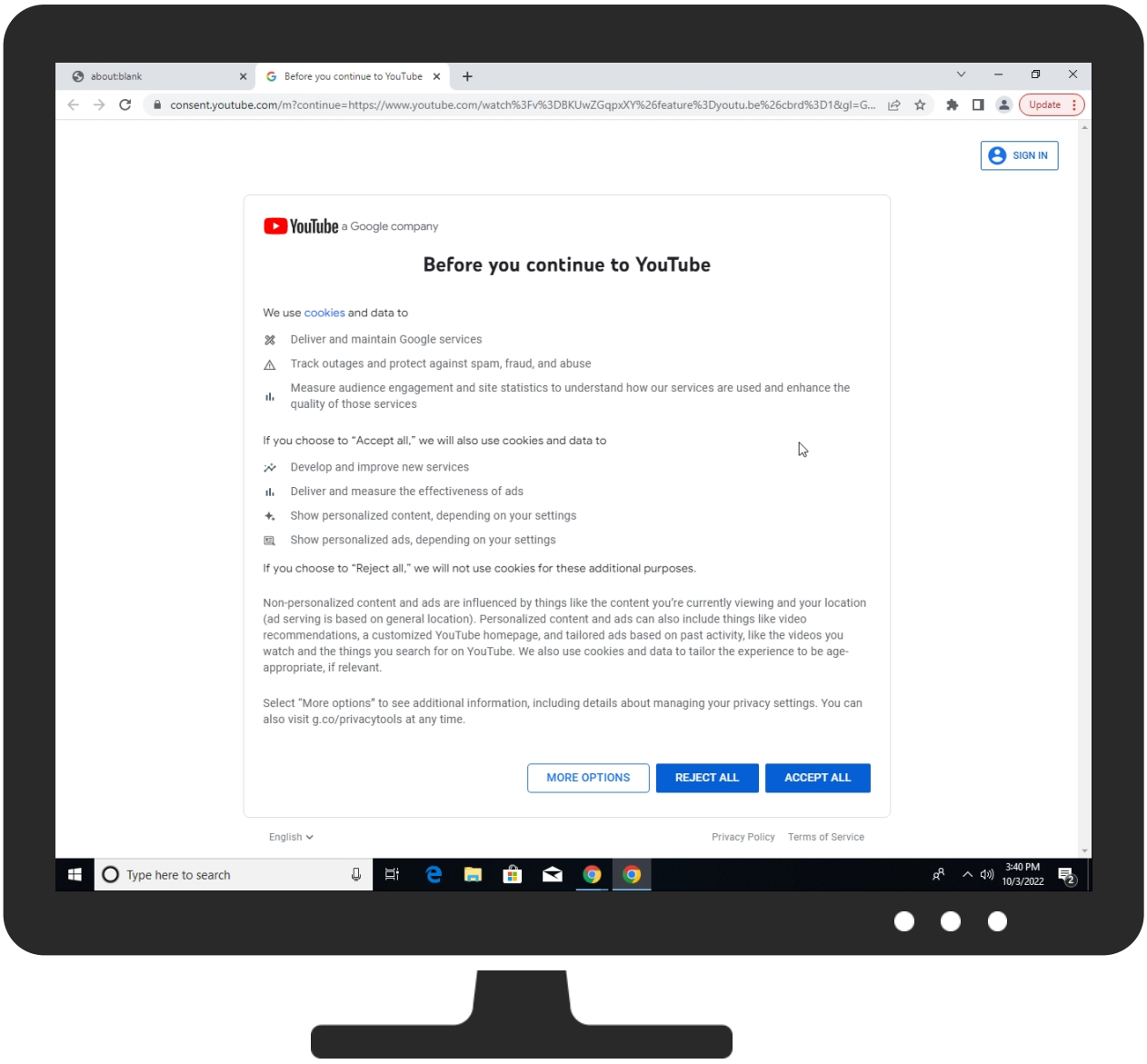


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://youtu.be/BKUwZGqpxXY	0%	Virustotal		Browse
http://https://youtu.be/BKUwZGqpxXY	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
i.ytimg.com	172.217.168.54	true	false		high
consent.youtube.com	172.217.168.46	true	false		high
rr5.sn-4g5edndr.googlevideo.com	172.217.133.234	true	false		high
youtube.com	142.250.203.110	true	false		high
youtu.be	172.217.168.14	true	false		high
youtube-ui.l.google.com	172.217.168.14	true	false		high
rr4.sn-4g5lznls.googlevideo.com	74.125.11.9	true	false		high
play.google.com	142.250.203.110	true	false		high
r3.sn-4g5ednkl.googlevideo.com	173.194.10.104	true	false		high
photos-ugc.l.googleusercontent.com	142.250.203.97	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
yt3.ggpht.com	unknown	unknown	false		high
r3---sn-4g5ednkl.googlevideo.com	unknown	unknown	false		high
rr5---sn-4g5edndr.googlevideo.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
rr4---sn-4g5lznls.googlevideo.com	unknown	unknown	false		high

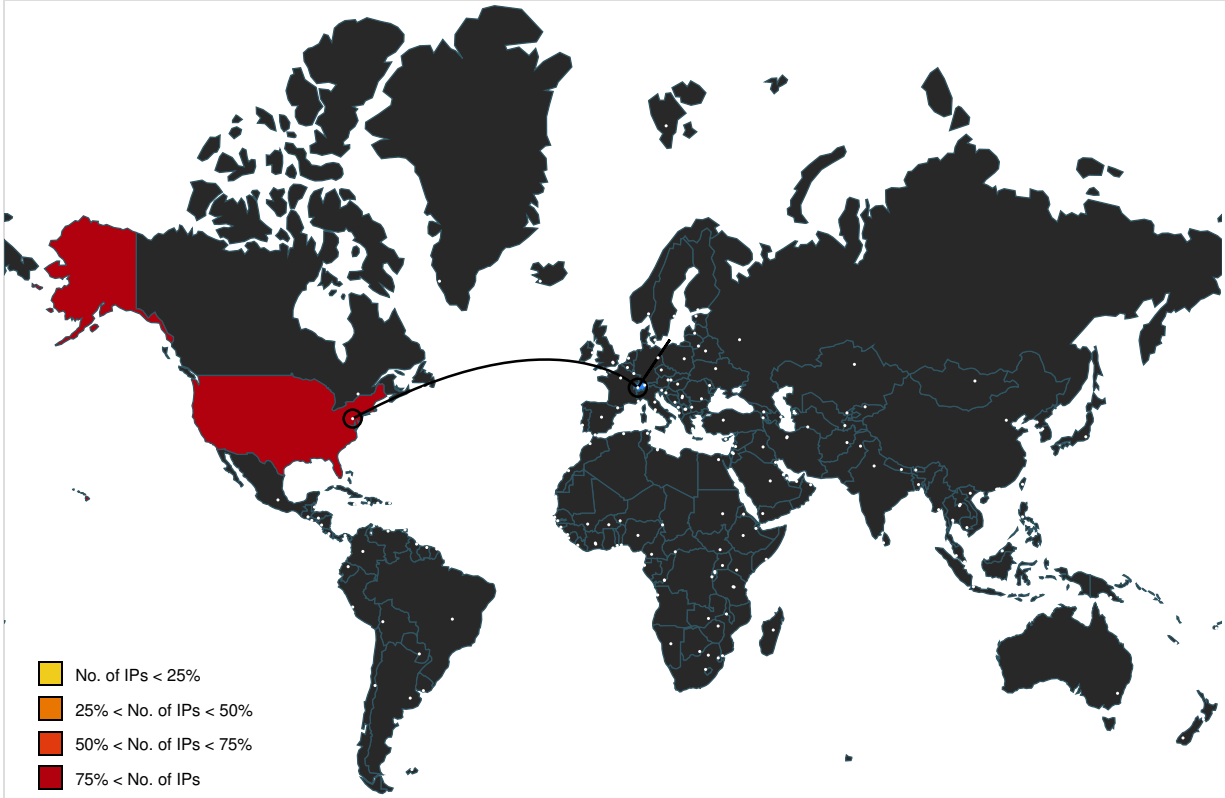
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://accounts.google.com/v3/signin/identifier?dsh=S-1022972884%3A1664804396065157&continue=https%3A%2F%2Fwww.youtube.com%2Fsignin%3Faction_handle_signin%3Dtrue%26app%3Ddesktop%26hl%3Den%26next%3D%252Fsignin_passive%26feature%3Dpassive&hl=en&passive=true&service=youtube&uilel=3&flowName=GlifWebSignIn&flowEntry=ServiceLogin&ifkv=AQDHYWra2-WDKfFJKSlBM-GWwkRYHfidvNjzEdO1dbNHFk8l-eLNXtaTgzJbseMLBelkXdkd-3ha	false		high
http://https://accounts.google.com/ServiceLogin?service=youtube&uilel=3&passive=true&continue=https%3A%2F%2Fwww.youtube.com%2Fsignin%3Faction_handle_signin%3Dtrue%26app%3Ddesktop%26hl%3Den%26next%3D%252Fsignin_passive%26feature%3Dpassive&hl=en	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/desktop_polymer.vflset/desktop_polymer.js	false		high
http://https://www.youtube.com/sw.js	false		high
http://https://www.google.com/js/th/VM1LbcxuQZ7urdjSm15-Kft2ldlldgxYJTjOL3p1Mjw.js	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/miniplayer.js	false		high
http://https://www.youtube.com/s/search/audio/open.mp3	false		high
http://https://i.ytimg.com/vi/lpinwHPBmuY/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLCQaypNHXiK5Fhvz5v12J1InO7OZQ	false		high
http://https://www.youtube.com/s/search/audio/failure.mp3	false		high
http://https://i.ytimg.com/vi/41i5AaxcwUA/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLBwMZvo67pstXVQJYZdlCXQdMQUcA	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/base.js	false		high
http://https://r3---sn-4g5ednkl.googlevideo.com/generate_204	false		high
http://https://www.youtube.com/s/player/a336babc/www-player.css	false		high
http://https://i.ytimg.com/generate_204	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/scheduler.vflset/scheduler.js	false		high
http://https://www.youtube.com/s/search/audio/no_input.mp3	false		high
http://https://www.youtube.com/watch?v=BKUwZGqpxXY&feature=youtu.be	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/network.vflset/network.js	false		high
http://https://i.ytimg.com/vi/4cRp2EffKgY/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLDK8QQXzirTRust6CkVm9JBOQQpIg	false		high
http://https://youtu.be/BKUwZGqpxXY	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/custom-elements-es5-adapter.vflset/custom-elements-es5-adapter.js	false		high
http://https://www.youtube.com/generate_204?YFasmg	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://i.ytimg.com/vi/q0i_0PiguEI/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLBfezge_INPTo5BBL3djNUhXUabUA	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/endscreen.js	false		high
http://https://consent.youtube.com/_/ConsentUi/browserinfo?f.sid=5434109171826470979&bl=boq_identityfrontenduiserver_20220925.17_p2&hl=en&gl=GB&_reqid=56430&rt=j	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/remote.js	false		high
http://https://i.ytimg.com/vi/fYofI_9azM8/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLBzUM5xSWmflJD2kMVBKafj77UbiQ	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/offline.js	false		high
http://https://i.ytimg.com/vi/DLhZh0P8LCc/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLCIrfhrD0TUqbqZdA1NUEJdPvU8Kg	false		high
http://https://www.youtube.com/youtubei/v1/log_event?alt=json&key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8	false		high
http://https://www.youtube.com/s/player/a336babc/player_ias.vflset/en_US/captions.js	false		high
http://https://i.ytimg.com/vi/JRqMJHbQBhQ/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLBG-x-fRVm8H87OabFSHQNPchwS3g	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/cssbin/www-main-desktop-watch-page-skeleton.css	false		high
http://https://i.ytimg.com/vi/BKUwZGqpxXY/maxresdefault.jpg	false		high
http://https://i.ytimg.com/vi/ywiqFEYYWyg/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLDfnpXgFE38Yy_x4VIC7ToB6_Ba5w	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/cssbin/www-onepick.css	false		high
http://https://r3---sn-4g5ednkl.googlevideo.com/generate_204?conn2	false		high
http://https://youtube.com/	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/img/favicon_32x32.png	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/spf.vflset/spf.js	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/cssbin/www-main-desktop-player-skeleton.css	false		high
http://https://www.youtube.com/s/_/ytmainappweb/_/ss/k=ytmainappweb.kevlar_base.AwIVWlJRnaA.L.B1.O/d=0/rs=AGKMywHoCmxVFz7S6CsgSo9NN0yigqc6wg	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/intersection-observer.min.vflset/intersection-observer.min.js	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/img/favicon.ico	false		high
http://https://www.google.com/favicon.ico	false		high
http://https://i.ytimg.com/vi/sMaoGmeiwmg/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLAjsfdG9gHJnDdYKGVHRCby5h0K5w	false		high
http://https://www.youtube.com/manifest.webmanifest	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/web-animations-next-lite.min.vflset/web-animations-next-lite.min.js	false		high
http://https://play.google.com/log?format=json&hasfast=true	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/webcomponents-sd.vflset/webcomponents-sd.js	false		high
http://https://consent.youtube.com/m?continue=https://www.youtube.com/watch%3Fv%3DBKUwZGqpxXY%26feature%3Dyoutu.be%26cbrd%3D1&gl=GB&m=0&pc=yt&hl=en&src=1	false		high
http://https://consent.youtube.com/m?continue=https://www.youtube.com/watch%3Fv%3DBKUwZGqpxXY%26feature%3Dyoutu.be%26cbrd%3D1&gl=GB&m=0&pc=yt&hl=en&src=1	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://i.ytimg.com/vi/FvQdL0_17bw/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLAVbEusmk0YWx_sdTTpVp--mSvDLA	false		high
http://https://www.youtube.com/s/search/audio/success.mp3	false		high
http://https://www.youtube.com/s/desktop/a3a2ae5f/jsbin/www-i18n-constants-en_US.vflset/www-i18n-constants.js	false		high
http://https://yt3.ggpht.com/ytc/AMLnZu_y_xWSIUn9il5pU5PE_M4TBJMuCcFUSU1CdV281g=s48-c-k-c0x00ffffff-no-rj	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://www.youtube.com/youtubei/v1/att/get?key=AIzaSyAO_FJ2SlqU8Q4STEHLGCilw_Y9_11qcW8&prettyPrint=false	false		high
http://https://i.ytimg.com/vi/Qe9JcVsRQvY/hqdefault.jpg?sqp=-oaymwEbCKgBEF5IVfKriqkDDggBFQAAiEIYAXABwAEG&rs=AOn4CLDIeHUhUWOVA-1cf_NsEMXERxTm1A	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
142.250.203.110	youtube.com	United States		15169	GOOGLEUS	false
74.125.11.9	rr4.sn-4g5lznls.googlevideo.com	United States		15169	GOOGLEUS	false
172.217.168.46	consent.youtube.com	United States		15169	GOOGLEUS	false
172.217.168.14	youtu.be	United States		15169	GOOGLEUS	false
142.250.203.97	photos-ugc.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.133.234	rr5.sn-4g5edndr.googlevideo.com	United States		15169	GOOGLEUS	false
172.217.168.54	i.ytimg.com	United States		15169	GOOGLEUS	false
173.194.10.104	r3.sn-4g5ednkl.googlevideo.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715056
Start date and time:	2022-10-03 15:38:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://youtu.be/BKUwZGqpxXY
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@29/0@16/13
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 216.58.209.42, 172.217.168.10, 172.217.168.42, 172.217.168.74, 142.250.203.106, 216.58.215.234
- Excluded domains from analysis (whitelisted): fonts.googleapis.com, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, fonts.gstatic.com, update.googleapis.com, clientservices.googleapis.com, www.gstatic.com, jnn-pa.googleapis.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

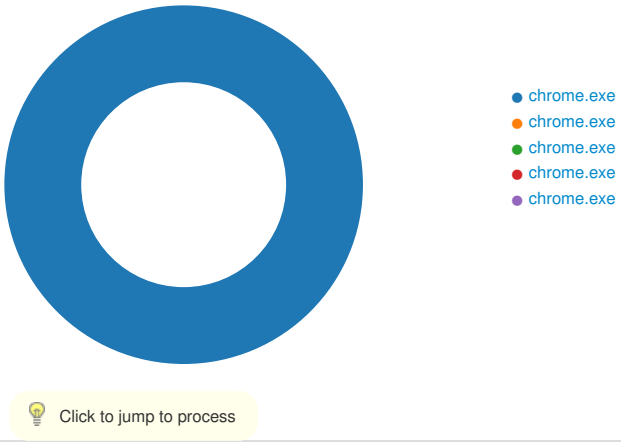
No static file info

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5892, Parent PID: 4612

General

Target ID:	0
Start time:	15:39:46

Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	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

Registry Activities

Analysis Process: chrome.exe PID: **4388**, Parent PID: **5892**

General

Target ID:	1
Start time:	15:39:47
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1960 --field-trial-handle=1764,i,1761891885139680210,6239086101532742970,131072 --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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5216**, Parent PID: **4612**

General

Target ID:	2
Start time:	15:39:48
Start date:	03/10/2022

Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "https://youtu.be/BKUwZGqpxXY
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

Registry Activities

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

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

Analysis Process: chrome.exe PID: **6828**, Parent PID: **5892**

General

Target ID:	5
Start time:	15:40:06
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --mojo-platform-channel-handle=5480 --field-trial-handle=1764,i,17618918851396802 10,6239086101532742970,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6f9750000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: **7116**, Parent PID: **5892**

General

Target ID:	6
Start time:	15:40:12
Start date:	03/10/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=3820 --field-trial-handle=1764,i,17618918851396802 10,6239086101532742970,131072 --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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly