ID: 1438321
Sample Name: JrE5qsYZD8.exe
Cookbook: default.jbs
Time: 15:50:06
Date: 08/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

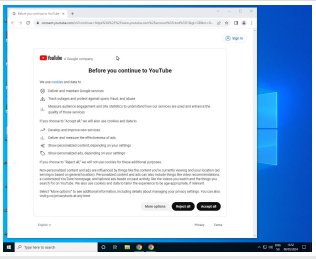
Windows Analysis Report

JrE5qsYZD8.exe

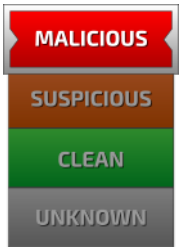
Overview

General Information

Sample name:	JrE5qsYZD8.exerenamed because original name is a hash value
Original sample name:	5f4a7d44b849b..
Analysis ID:	1438321
MD5:	3143cd8f56bf5…
SHA1:	33b83cd5d719…
SHA256:	5f4a7d44b849b..
Tags:	exe
Infos:	



Detection

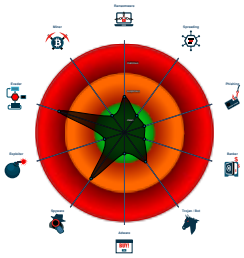


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Binary is likely a compiled AutoIt sc…
- Found API chain indicative of debug…
- Found API chain indicative of sandb…
- Machine Learning detection for sam…
- Contains functionality for read data …
- Contains functionality to block mous…
- Contains functionality to check if a d…
- Contains functionality to check if a w…
- Contains functionality to communica…
- Contains functionality to dynamicall…

Classification



Process Tree

- **System is w10x64**
- JrE5qsYZD8.exe (PID: 5020 cmdline: "C:\Users\user\Desktop\JrE5qsYZD8.exe" MD5: 3143CD8F56BF599B3CFDDAF9152D445D)
  - chrome.exe (PID: 3236 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.youtube.com/account MD5: 5BBFA6CBDF4C254EB368D534F9E23C92)
    - chrome.exe (PID: 5788 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=2044 --field-trial-handle=1992,i,15798156456821883579,10995336834318236159,262144 /prefetch:8 MD5: 5BBFA6CBDF4C254EB368D534F9E23C92)
- **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

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Binary is likely a compiled AutoIt script file

Malware Analysis System Evasion

Found API chain indicative of sandbox detection

Anti Debugging

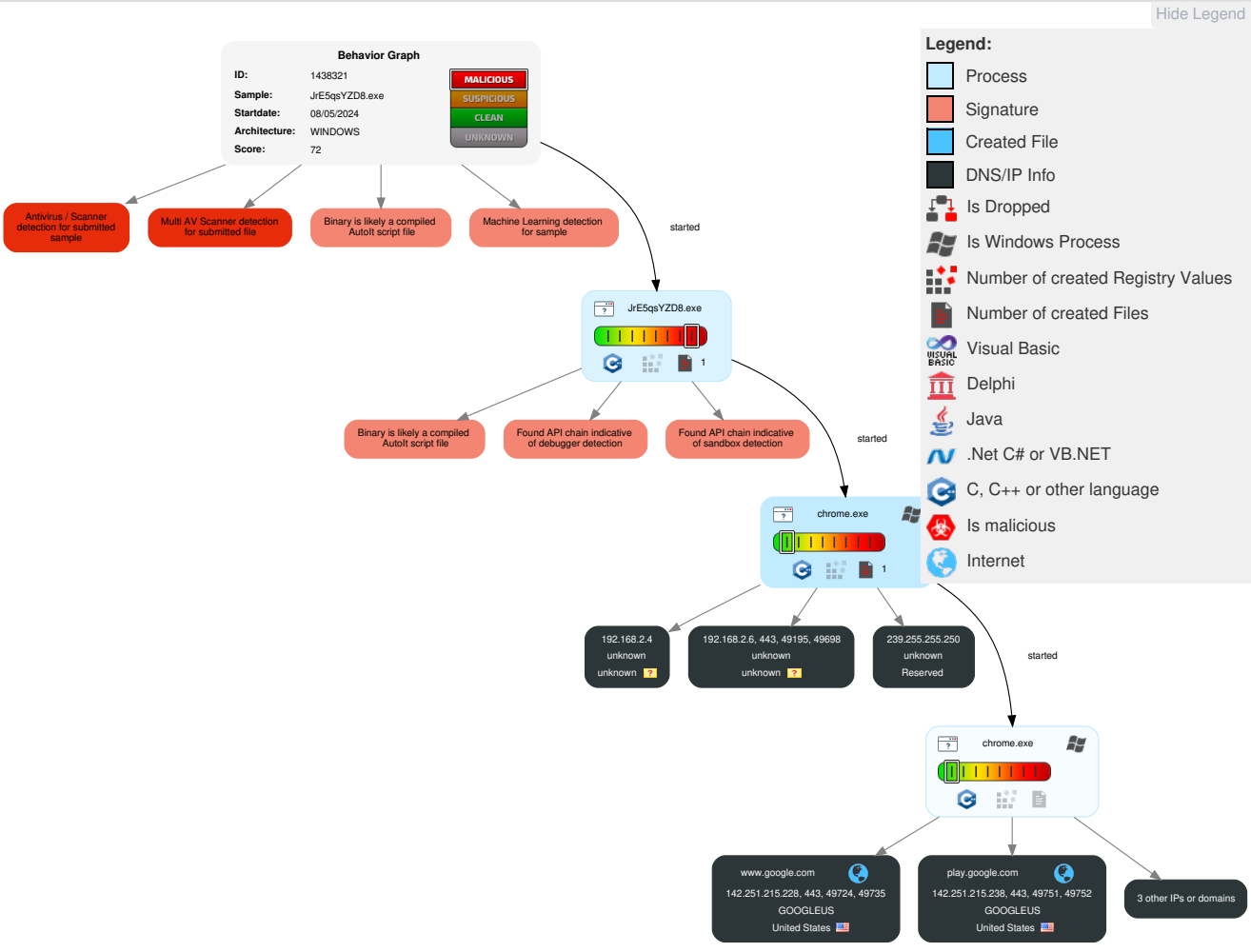
Found API chain indicative of debugger detection

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	2 Valid Accounts	1 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	3 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	1 System Shutdown/Reboot
Credentials	Domains	Default Accounts	Scheduled Task/Job	2 Valid Accounts	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	3 1 Input Capture	1 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	2 Valid Accounts	2 Obfuscated Files or Information	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	3 Clipboard Data	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	2 1 Access Token Manipulation	1 DLL Side-Loading	NTDS	1 5 System Information Discovery	Distributed Component Object Model	Input Capture	4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	1 2 Process Injection	2 Valid Accounts	LSA Secrets	2 2 1 Security Software Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	2 1 Access Token Manipulation	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 2 Process Injection	Proc Filesystem	1 1 Application Window Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	HTML Smuggling	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

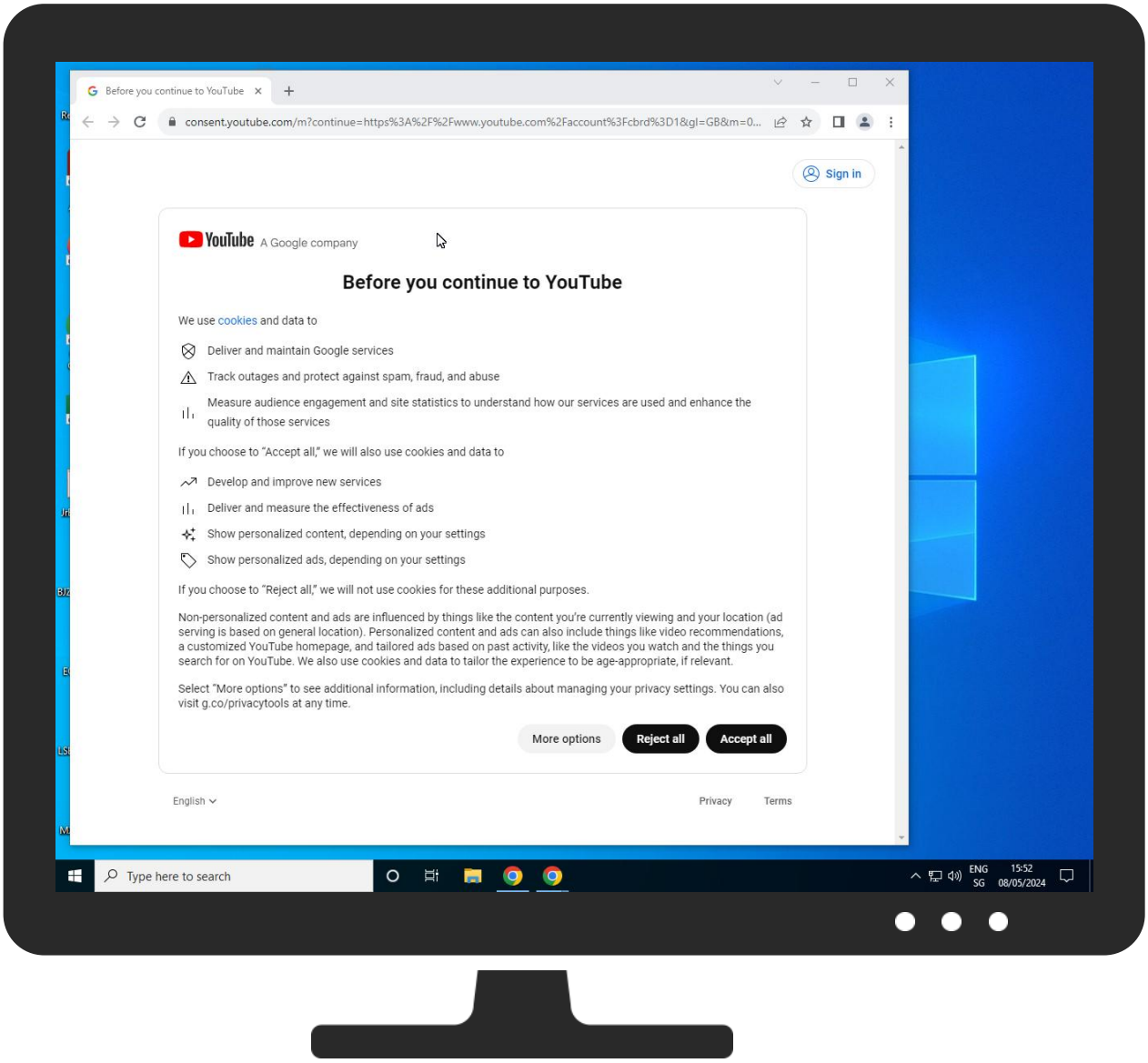
Behavior Graph



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
JrE5qsYZD8.exe	53%	ReversingLabs	Win32.Trojan.AutoitInject	
JrE5qsYZD8.exe	100%	Avira	TR/AutoIt.zstul	
JrE5qsYZD8.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://localhost.proxy.googlers.com/inapp/	0%	URL Reputation	safe	
http://https://asx-frontend-autopush.corp.google.co.uk/inapp/	0%	URL Reputation	safe	
http://https://asx-frontend-autopush.corp.google.co.uk/tools/feedback/	0%	URL Reputation	safe	
http://https://localhost.proxy.googlers.com/inapp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
youtube-ui.l.google.com	142.250.69.206	true	false		high
play.google.com	142.251.215.238	true	false		high
consent.youtube.com	142.251.33.78	true	false		high
www.google.com	142.251.215.228	true	false		high
www.youtube.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://consent.youtube.com/_/ConsentUi/browserinfo?f.sid=-9033751170818193612&bl=boq_identityfrontenduiserver_20240505.08_p1&hl=en&gl=GB&_reqid=157061&rt=j	false		high
http://https://consent.youtube.com/m?continue=https%3A%2F%2Fwww.youtube.com%2Faccount%3Fcbrd%3D1&gl=GB&m=0&pc=yt&cm=2&hl=en&src=1	false		high
http://https://consent.youtube.com/_/ConsentUi/browserinfo?f.sid=-9033751170818193612&bl=boq_identityfrontenduiserver_20240505.08_p1&hl=en&gl=GB&_reqid=57061&rt=j	false		high
http://https://play.google.com/log?format=json&hasfast=true&authuser=0	false		high
http://https://www.google.com/favicon.ico	false		high

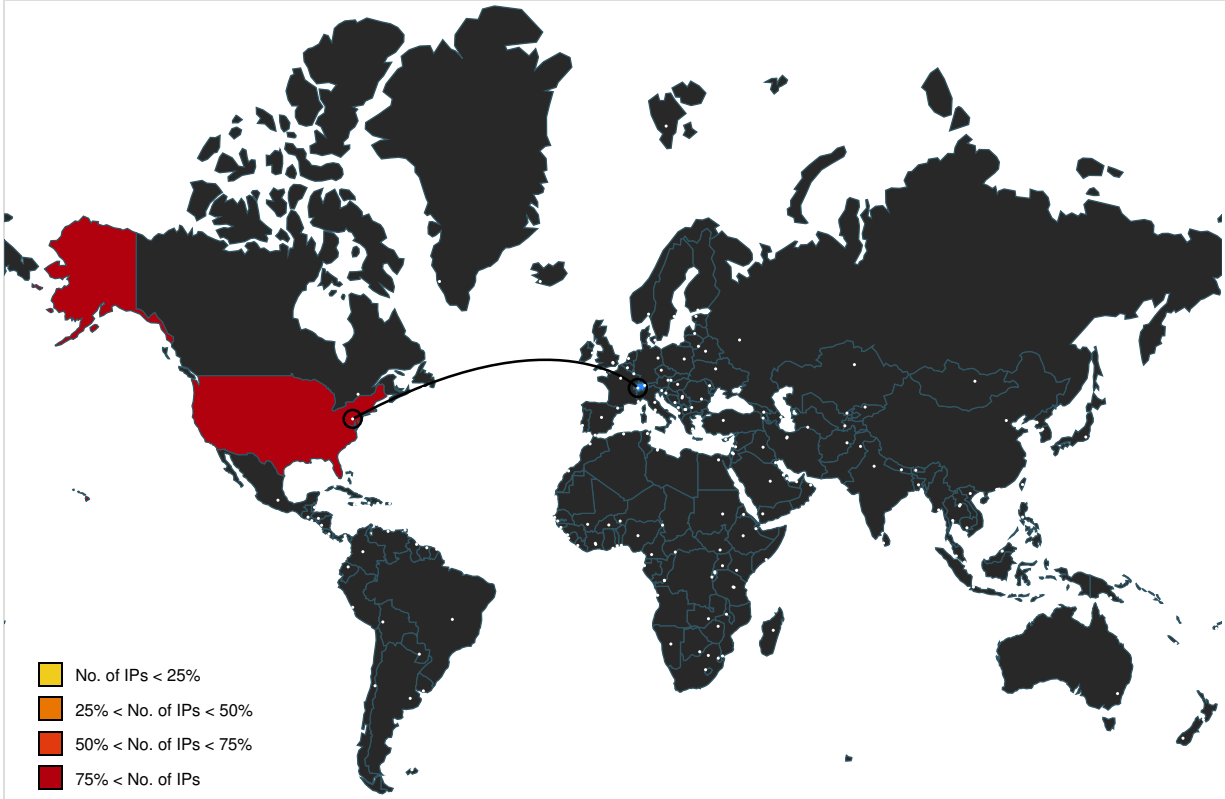
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://localhost.corp.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://feedback.googleusercontent.com/resources/annotator.css	chromecache_83.4.dr	false		high
http://https://apis.google.com/js/client.js	chromecache_83.4.dr	false		high
http://https://feedback2-test.corp.googleusercontent.com/tools/feedback/%	chromecache_83.4.dr	false		high
http://https://support.google.com	chromecache_94.4.dr	false		high
http://https://play.google.com	chromecache_94.4.dr	false		high
http://localhost.proxy.googlers.com/inapp/	chromecache_83.4.dr	false	• URL Reputation: safe	unknown
http://https://stagingqual-feedback-pa-googleapis.sandbox.google.com	chromecache_83.4.dr	false		high
http://https://support.google.com/inapp/%	chromecache_83.4.dr	false		high
http://https://asx-help-frontend-autopush.corp.youtube.com/inapp/	chromecache_83.4.dr	false		high
http://https://www.youtube.com/accountd	JrE5qsYZD8.exe, 00000000.00000003.2312661987.00000000038DA000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2312997328.00000000038ED000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2312157038.00000000038D5000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2312611297.00000000038D6000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000002.2314882594.00000000038F4000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://help.youtube.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://asx-frontend-staging.corp.google.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://support.google.com/	chromecache_83.4.dr	false		high
http://https://www.google.com	chromecache_94.4.dr	false		high
http://https://scone-pa.clients6.google.com	chromecache_83.4.dr	false		high
http://https://support.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://asx-frontend-autopush.corp.google.co.uk/inapp/	chromecache_83.4.dr	false	• URL Reputation: safe	unknown
http://https://asx-frontend-autopush.corp.google.co.uk/tools/feedback/	chromecache_83.4.dr	false	• URL Reputation: safe	unknown
http://https://asx-frontend-autopush.corp.google.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://asx-frontend-autopush.corp.youtube.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://feedback2-test.corp.google.com/inapp/%	chromecache_83.4.dr	false		high
http://https://www.google.com/tools/feedback	chromecache_83.4.dr	false		high
http://https://sandbox.google.com/inapp/%	chromecache_83.4.dr	false		high
http://https://apis.google.com/js/api.js	chromecache_85.4.dr	false		high
http://https://feedback2-test.corp.googleusercontent.com/inapp/%	chromecache_83.4.dr	false		high
http://https://localhost.proxy.googlers.com/inapp/	chromecache_83.4.dr	false	• URL Reputation: safe	unknown
http://https://www.google.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://www.google.cn/tools/feedback/	chromecache_83.4.dr	false		high
http://https://asx-frontend-autopush.corp.google.de/inapp/	chromecache_83.4.dr	false		high
http://https://www.google.cn/tools/feedback/%	chromecache_83.4.dr	false		high
http://https://feedback2-test.corp.google.com/tools/feedback/%	chromecache_83.4.dr	false		high
http://https://www.google.com/tools/feedback/help_panel_binary.js	chromecache_83.4.dr	false		high
http://https://www.youtube.com/account	JrE5qsYZD8.exe, 00000000.00000002.2314882594.00000000038F4000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2308250823.0000000003845000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2313520255.0000000003874000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000003.2309857328.000000000386D000.00000004.00000020.00020000.00000000.sdmp, JrE5qsYZD8.exe, 00000000.00000002.2314771847.00000000038D7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://uberproxy-pen-redirect.corp.google.com/uberproxy/pen?url=	chromecache_85.4.dr	false		high
http://https://asx-frontend-autopush.corp.google.de/tools/feedback/	chromecache_83.4.dr	false		high
http://https://sandbox.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://test-scone-pa-googleapis.sandbox.google.com	chromecache_83.4.dr	false		high
http://https://asx-help-frontend-autopush.corp.youtube.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://play.google.com/log?format=json&hasfast=true	chromecache_88.4.dr	false		high
http://https://asx-frontend-autopush.corp.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://feedback.googleusercontent.com/resources/render_frame2.html	chromecache_83.4.dr	false		high
http://https://sandbox.google.com/tools/feedback/%	chromecache_83.4.dr	false		high
http://https://sandbox.google.com/tools/feedback/	chromecache_83.4.dr	false		high
http://https://localhost.corp.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://asx-frontend-autopush.corp.youtube.com/inapp/	chromecache_83.4.dr	false		high
http://https://feedback-pa.clients6.google.com	chromecache_83.4.dr	false		high
http://https://asx-frontend-staging.corp.google.com/inapp/	chromecache_83.4.dr	false		high
http://https://www.google.com/tools/feedback/%	chromecache_83.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://fonts.google.com/license/googlerestricted	chromecache_101.4.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.251.33.78	consent.youtube.com	United States		15169	GOOGLEUS	false
142.251.215.228	www.google.com	United States		15169	GOOGLEUS	false
142.251.215.238	play.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.4
192.168.2.6

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1438321
Start date and time:	2024-05-08 15:50:06 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
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
Sample name:	JrE5qsYZD8.exerenamed because original name is a hash value
Original Sample Name:	5f4a7d44b849b744b38f11fbb131743324c84705ec16ae7a1f0789f4f35e49c2.exe
Detection:	MAL
Classification:	mal72.evad.winEXE@33/48@12/6
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.69.206, 74.125.142.84, 142.250.217.99, 34.104.35.123, 142.251.211.227, 142.251.211.234, 142.250.69.202, 142.251.33.106, 142.251.33.74, 142.250.217.74, 142.250.217.106, 142.251.215.234, 172.217.14.234, 199.232.214.172, 192.229.211.108, 142.250.217.67, 142.251.211.238
- Excluded domains from analysis (whitelisted): clients1.google.com, fonts.googleapis.com, fs.microsoft.com, accounts.google.com, slscr.update.microsoft.com, fonts.gstatic.com, ctldl.windowsupdate.com, clientservices.googleapis.com, fe3cr.delivery.mp.microsoft.com, clients2.google.com, ocsp.digicert.com, edgedl.me.gvt1.com, update.googleapis.com, clients.l.google.com, www.gstatic.com, optimizationguide-pa.googleapis.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 exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: JrE5qsYZD8.exe

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: 100

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 24 x 24, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	128
Entropy (8bit):	5.9358359421205895
Encrypted:	false
SSDEEP:	3:yionv//thPlT/Xti9kyUViilmtzG9agqtlsg1p:6v/lhPX2kP+ty/O2up
MD5:	AE90CD36AD79C9F93FB53A960BC6D171
SHA1:	893F232DAF35C28F17D17822795F7E180B34FC11
SHA-256:	EEA4C83B7BA7B9C7E2E0843E8D7F4593760CBC14281C92666327701118 22B8F9
SHA-512:	4165C36E9F9BBB4487CDCFEE48FCBE738A0AF6DF928AC8ACBB69C4801E2F915A7CA97196B110FDF58B8BB78497F3D5D11A834AAAB6BE645E8DB24C66DA192F53
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://www.gstatic.com/images/icons/material/system/1x/check_black_24dp.png
Preview:	.PNG.....IHDR.....J~.s...GIDATx.c..F..i...04...?C..S...!...C...."HqL.XK$.r.Z....PN...r..`(.....-.....IEND.B`.

Chrome Cache Entry: 101

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (1116)
Category:	downloaded
Size (bytes):	65972
Entropy (8bit):	5.509981930150997
Encrypted:	false
SSDEEP:	768:HPK1YrrBBvEXETV8oNXupV7RnHa5+KuXZ0Qzr1XL4Uw3YfC/sDwydk8JDpPL7nbG:N+V3Zz9BQowEN6XViYkQ2byr
MD5:	388E5EAC053059DD6E4303D080A52143
SHA1:	F39B58B6062078A79FE8C33F00A07CBD08B83DAD
SHA-256:	467F435EC60DD102FD227B26EEE269C37D2DDAD9F84480DBC6B89086379A8ABD
SHA-512:	F6FB03E176A3A827A58E6636CB446AE906EE8E858E84BE72174BA345008FBA26D51D667F69C02BE79F771CFBA6904CBD0F646BBF0C09AC222A58C867C5DDCE60
Malicious:	false
Reputation:	low
URL:	http://https://fonts.googleapis.com/css?family=YouTube+Sans:700&display=swap
Preview:	/*. * See: https://fonts.google.com/license/googlerestricted. */./* [2] */.@font-face {. font-family: 'YouTube Sans';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/youtubesans/v30/Qw3hZQNGEDjaO2m6tqlqX5E-AVS5_rSejo46_PCTRspJ0OosolrBEJL3HMXfxQASluL2m_dA4FGABPaUsmg3nQVU1JcNWPLEgrh9odK7.2.woff2) format('woff2');. unicode-range: U+d723-d728, U+d72a-d733, U+d735-d748, U+d74a-d74f, U+d752-d753, U+d755-d757, U+d75a-d75f, U+d762-d764, U+d766-d768, U+d76a-d76b, U+d76d-d76f, U+d771-d787, U+d789-d78b, U+d78d-d78f, U+d791-d797, U+d79a, U+d79c, U+d79e-d7a3, U+f900-f909, U+f90b-f92e;.}./* [3] */.@font-face {. font-family: 'YouTube Sans';. font-style: normal;. font-weight: 700;. font-display: swap;. src: url(https://fonts.gstatic.com/s/youtubesans/v30/Qw3hZQNGEDjaO2m6tqlqX5E-AVS5_rSejo46_PCTRspJ0OosolrBEJL3HMXfxQASluL2m_dA4FGABPaUsmg3nQVU1JcNWPLEgrh9odK7.3.woff2) format('woff2');. unicode-range: U+d679-d68b, U+d68e-d69e, U+d6a0, U+d6a2-

Chrome Cache Entry: 102

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	800
Entropy (8bit):	4.463585747493267
Encrypted:	false
SSDEEP:	24:t4jU/va2dO0VjIIXRl0SBv+t1qOv3V2N5cOa:t/i24w9Blr1+tNv3cDa
MD5:	CB63876A89F2E55871EAE56F05488045
SHA1:	011F6EDB7A4E8D0FA3854B30EC6A11077F90F470
SHA-256:	7EAF8A916EF14FD599542E95061275C804C46A957B15A5B9CF05AE0E6CB03C97
SHA-512:	4C49F3081D6D83E54223E65BBABB0C8015546EF71903D150175611000417A12A47F5FE80FD8E96704C06A9F1D6508EEACCD8A34F9789626649C259D085A34C4B
Malicious:	false
Reputation:	low
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/shield_24px.svg

Preview:	<svg xmlns="http://www.w3.org/2000/svg" enable-background="new 0 0 24 24" height="24" viewBox="0 0 24 24" width="24"><path d="M12,2L4,5.67v5.49c0,1.47 ,0.3,2.9,0.81,4.22c0.17,0.44,0.37,0.86,0.6,1.28c0.16,0.3,0.34,0.6,0.52,0.88 c1.42,2.17,3.52,3.82,5.95,4.44L12,22l0.12-0.03c2.43-0.61,4.53-2.26,5.95-4.43c0.19-0. 29,0.36-0.58,0.52-0.88 c0.22-0.41,0.43-0.84,0.6-1.28C19.7,14.05,20,12.62,20,11.15V5.67L12,2z M12,3.1l6.11,2.8L12,11.15L5.89,5.9L12,3.1z M5.75,15.01 C5.25,13.75, 5,12.45,5,11.15v-4.7l6.23,5.35l-4.98,4.28C6.05,15.71,5.88,15.36,5.75,15.01z M17.23,16.99 C15.91,19,14.06,20.41,12,20.97C9.94,20.41,8.09,19,6.77,16.99c0-0.01-0.01-0. 0.01-0.01-0.02l5.24-4.5l5.24,4.5 C17.23,16.98,17.23,16.98,17.23,16.99z M19,11.15c0,1.3-0.25,2.6-0.75,3.86c-0.14,0.35-0.3,0.7-0.5,1.08l-4.98-4.28L19,6.45V11.15z"/> </svg>

Chrome Cache Entry: 103

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 52280, version 1.0
Category:	downloaded
Size (bytes):	52280
Entropy (8bit):	**7.995413196679271**
Encrypted:	**true**
SSDEEP:	1536:1rvqtK8DZilXxwJ8mMwAZy7phqsFLdG3B4d:xytBZits8bw4wzbFxG3B4d
MD5:	F61F0D4D0F968D5BBA39A84C76277E1A
SHA1:	AA3693EA140ECA418B4B2A30F6A68F6F43B4BEB2
SHA-256:	57147F08949ABABE7DEEF611435AE418475A693E3823769A25C2A39B6EAD9CCC
SHA-512:	6C3BD90F709BCF9151C9ED9FFEA55C4F6883E7FDA2A4E26BF018C83FE1CFBE4F4AA0DB080D6D024070D53B2257472C399C8AC44EEFD38B9445640EFA85D5C 87
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://fonts.gstatic.com/s/googlesans/v58/4UaRrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iq2vgCI.woff2
Preview:	wOF2.....8.....^...$..4?HVAR..?MVAR9.`?STAT.*',..J/.....`..(..Z.0..R.6.$.... .....K..[..q..c..T.....>.P.j.`.w..#...%.....N."....$..3.0.6..... .L.rX/r[j.y.\|*(. 4.%#.....2.v.m..-..%.....;-.Y.{..&..O=#l@...k..7g..ZI...#.Z./+T..r7...M..3).Z%.x....s..sL..[A!.5*1w'/.8V..2Z..%.X.h.o.).]..9..Q`.$.....7..kZ.~O.....d..g.n.d.Rw+&....Cz..uy#..fz, (.J....v.%..`..9.....h...?O..:...c%.....6s....xl..#...5..._.....1.>.)"U.4 W....?%.....6//!$...!.n9C@n.....!""^.....W..Z<.7.x.."UT.T....E..."R>.R..t.....H d..e_.K../.+8.Q.P.ZQ....;...U ....]....._.e*.....71.?.7.ORv.?...I...G\|.P...\|:...I.X..2.,.L.....d.g.]}W#uW]QnuP-s.;.-Y.....].....C..j_.M0...y.....J.....NY..@A...,....-.F.....'..w./j5g.vUS...U..0.&...y7.LP.....%..... Y.....Y..D. e.A..G.?.$.....6...eaK.n5.m...N...,...+BCl..L> .E9~.b[.w.x....6<...}.e...%V....O.....*.?...a..#[eE.4..p..$...].....%.....o._.....N.._~..El....b..A.0.r8.....|..D.d..

Chrome Cache Entry: 80

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	180
Entropy (8bit):	4.850122490909282
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5sAR+hHiATcvXjXRHRcBHoNcHo6ggNqGfImRLNpBzxZFRFXnNXqf:tI9mc4slhohC/vmI4oVdGfzXpjXks8
MD5:	572FC8D2BB8E7D64716824F2490E9500
SHA1:	196420553BDE9EB1879623ABC51629FDE8D9E468
SHA-256:	47CCDD35EFA1997EB1596ABCD551155E7D1046B29820B35A90681A007B9E22C6
SHA-512:	9881DABC52E125847F217F4611FB5213B1B249ED01BD1FDED52A4843EB7CE7B4F9C6AEA27ECE47476DACD7FA7D8E04AB9080EDCE03B216D22BFDD2456ACD 56A7
Malicious:	false
Reputation:	moderate, very likely benign file
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/alert_triangle_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" height="24" viewBox="0 0 24 24" width="24"><path d="M13 18h-2v-2h2v2zm0-8h-2v5h2v-5zm-1-4.11L20.2 19H3.8L12 5. 89M12 4 2 20h20L12 4z"/></svg>

Chrome Cache Entry: 81

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
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: 82

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (952)
Category:	downloaded
Size (bytes):	3344
Entropy (8bit):	5.517076721226713
Encrypted:	false
SSDEEP:	96:e2bfI42YFX4TDM5IzNtdke9fgSiduhGcn:nbfIYeRB4SFhrn
MD5:	5B4C24EDFAB3EFF1E6D9B2FA6E2DCE2E
SHA1:	FE8EDCC5775BEDA655561A2C422AD29610BDB3A6
SHA-256:	3488D47695DDD45A27A18923FA64CC8DEF97AA49B449E7095483A087AE454817
SHA-512:	AE0B37B0F2E5EA5C5BB7940123AB84FDA8C03C422D37F6756FE50872CADFD18ABE0C1593D0E6AEB64F931404895822DA2243AE8DAC290F33FE9C9D0901C5F5 6F
Malicious:	false
URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/ck=boq-identity.ConsentUi.KIDMQ00cEM4.L.B1.O/am=GCzQWQ/d=1/exm=A7fCU,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,Mlhmy,MpJwZc,Ndreoc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OgOVNe,OmgaI,PHUIyb,PrPYRd,QlhFr,RMhBfe,RqjULd,SdcwHb,SpsfSb,U0aPgd,UMu52b,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WpP9Yc,XVMNvd,YTxL4,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,bm51tf,byfTOb,e5qFLc,fKUV3e,fkuQ3,gychg,hc6Ubd,kWgXee,lsjVmc,lwddkf,m9oV,n73qwf,ovKuLd,pjICDe,pw70Gc,s39S4,soHxf,vjKJJ,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,y5vRwf,yDVVkb,ywOR5c,zbML3c,zr1jrb/excm=_b,_tp,mainview/ed=1/wt=2/ujg=1/rs=AOaEmlFxmyZssOHbs21nbssPRY2wW9cOTg/ee=BcQPH:lOY4De;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QlhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;vNjB7d:YTxL4;wR5FRb:O1Gjze;xqZiqf:BBI74;yxTchf:KUM7Z;zxnPse:GkRiKb/m=Wt6vjf,hhhU8,FCpbqb,WhJNk"
Preview:	"use strict";this.default_ConsentUi=this.default_ConsentUi||{};(function(_){var window=this;.try{._.p("Wt6vjf");.var Mz=function(a){this.Pa=_.w(a,0,Mz.Wb)};_.D(Mz,_.z);Mz.prototype.Ta=function(){return _.Kc(_.xl(this,1))};Mz.prototype.Kb=function(a){return _.Ql(this,1,a)};Mz.Wb="f.bo";var Nz=function(){_.Lo.call(this)};_.D(Nz,_.Lo);Nz.prototype.Pb=function(){this.Ax=!1;Oz(this);_.Lo.prototype.Pb.call(this)};Nz.prototype.j=function(){Pz(this);if(this.Zn)return Qz(this),!1;if(!this.ez)return Rz(this),!0;this.dispatchEvent("p");if(!this.iu)return Rz(this),!0;this.Os?(this.dispatchEvent("r"),Rz(this)):Qz(this);return!1};.var Sz=function(a){var b=new _.lu(a.vF);null!=a.ov&&_.Qu(b,"authuser",a.ov);return b},Qz=function(a){a.Zn=!0;var b=Sz(a),c="rt=r&f_uid="+encodeURIComponent(String(a.iu));_.Aq(b,(0,_.$g)(a.l,a),"POST",c)};.Nz.prototype.l=function(a){a=a.target;Pz(this);if(_.Gq(a)){this.Kr=0;if(this.Os)this.Zn=!1,this.dispatchEvent("r");else if(this.ez)this.dispatchEvent("s");else{try{var b=

Chrome Cache Entry: 83

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (3383)
Category:	downloaded
Size (bytes):	108457
Entropy (8bit):	5.48559468980492
Encrypted:	false
SSDEEP:	1536:dQed4sDzUVRhLgvIDTxF9/a4+ECrOd/FeSWiSyz2NUAMSceu4GseEP2q:pV8JpTxv9erMmi72NUAMIGs3
MD5:	936C777790659F304D0D75DD37C349C5
SHA1:	C02A937CC205D9D9332B92E05C69836CEAFEE53A
SHA-256:	1252984607640507F1E1AED2558E401937EE530BB81FB2237619B15F953052B1
SHA-512:	7B93634962EA45C2AC645A9CC8BC959846DD453CDA1CC8113CFECD5B29E88F78AC8C16DCD0C29B21F2ECC2F17F17363CDE7D82D04844D5BE50F8E0131B12301
Malicious:	false
URL:	**http**://https://www.gstatic.com/feedback/js/help/prod/service/lazy.min.js
Preview:	(function(){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(g,f){this.uc=g;ba(this,"description",{configurable:!0,writable:!0,value:f})};b.prototype.toString=function(){return this.uc};var c="jscomp_symbol_"+(1E9*Math.random()>>>0)+"_",d=0,e=function

Chrome Cache Entry: 84

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (793)
Category:	downloaded
Size (bytes):	1424
Entropy (8bit):	5.304404758229372
Encrypted:	false
SSDEEP:	24:kZfGs71TY1xYkT3N/C/jF3Gfk+rYa2O3Plpv3xF5GWlo/mAGbOpEGboZPWSOerkw:efGs9Y3xbKjFOjr6dpfx1/fGbOpEGb0V

MD5:	ECA5506E3D24C3BE972304BDA6277A91
SHA1:	3497276607014AEFA50B703628FE33BB3A6894EB
SHA-256:	EFF4C7C3FFC3593C5ECDB47B1F08732EABDDB963F4060240A11F5DED6C839566
SHA-512:	826E991F921BA6FB0B722E68E2712D950D5016FBFAFBAEB0BB3ADABE2F39386C3D235C48AF801F0D223C4CBDA007181B45E7C86FFEE97CB1E6000671736813B1
Malicious:	false
URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/ck=boq-identity.ConsentUi.KIDMQ00cEM4.L.B1.O/am=GCzQWQ/d=1/exm=A7fCU,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,Mlhmy,MpJwZc,Ndreoc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OgOVNe,OmgaI,PHUIyb,PrPYRd,QlhFr,RMhBfe,RqjULd,SdcwHb,SpsfSb,U0aPgd,UMu52b,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WpP9Yc,XVMNvd,YTxL4,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,fkuQ3,gychg,hc6Ubd,kWgXee,lsjVmc,lwddkf,m9oV,n73qwf,ovKuLd,pjICDe,pw70Gc,s39S4,soHxf,vjKJJ,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,y5vRwf,yDVVkb,ywOR5c,zbML3c,zr1jrb/excm=_b,_tp,mainview/ed=1/wt=2/ujg=1/rs=AOaEmlFxmyZssOHbs21nbssPRY2wW9cOTg/ee=BcQPH:lOY4De;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;vNjB7d:YTxL4;wR5FRb:O1Gjze;xqZiqf:BBI74;yxTchf:KUM7Z;zxnPse:GkRiKb/m=bm51tf"
Preview:	"use strict";this.default_ConsentUi=this.default_ConsentUi||{};(function(_){var window=this;.try{._.p("bm51tf");.var wla=!!(_.Nh[0]>>17&1);var xla=function(a,b,c,d,e){this.o=a;this.oa=b;this.ha=c;this.ka=d;this.ta=e;this.j=0;this.l=IK(this)},yla=function(a){var b={};_.Ea(a.Ww(),function(e){b[e]=!0});var c=a.Jw(),d=a.Pw();return new xla(a.Ow(),1E3*c.j(),a.uw(),1E3*d.j(),b)},lK=function(a){return Math.random()*Math.min(a.oa*Math.pow(a.ha,a.j),a.ka)},JK=function(a,b){return a.j>=a.o?!1:null!=b?!!a.ta[b]:!0};var KK=function(a){_.K.call(this,a.Ea);this.Nb=null;this.o=a.service.Vy;this.ha=a.service.metadata;a=a.service.fQ;this.l=a.o.bind(a)};_.D(KK,_.K);KK.Ha=_.K.Ha;KK.ya=function(){return{service:{Vy:_.GK,metadata:_.CK,fQ:_.uK}}};KK.prototype.j=function(a,b){if(1!=this.ha.getType(a.qc()))return _.yp(a);var c=this.o.j;(c=c?yla(c):null)&&JK(c)?(b=LK(this,a,b,c),a=new _.xp(a,b,2)):a=_.yp(a);return a};.var LK=function(a,b,c,d){return c.then(function(e){return e},function(e){if(wla)if(e instance

Chrome Cache Entry: 85

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2305)
Category:	downloaded
Size (bytes):	187674
Entropy (8bit):	5.451308564341929
Encrypted:	false
SSDEEP:	3072:XiWdIKPnOdDm9XUJ1F573MiB+5Wg5HypS95sa4KcES:cE0Dm9UTD4595syS
MD5:	061103852F74D4419CBDA2FDC0358167
SHA1:	2BA505F844EDCE317CECC548FF17851B26767147
SHA-256:	38F7F18A3F91AA8BE9A0F15CDBC6681C7C0EC278A43BD4CA569DA04625F2405E
SHA-512:	A7D19821730AC6E1A445440720C7998E188D41984B9EB7F2CFA28FE252A00BCB0DCD095F9D8AA950BCC2D7BA4C275D523B69D9ABB6C78F38A70AA19D61370701
Malicious:	false
URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/am=GCzQWQ/d=1/excm=_b,_tp,mainview/ed=1/dg=0/wt=2/ujg=1/rs=AOaEmlHauA6tRftuUHa8-1ykvk9qVAF4wQ/m=_b,_tp"
Preview:	"use strict";this.default_ConsentUi=this.default_ConsentUi||{};(function(_){var window=this;.try{._._F_toggles_initialize=function(a){("undefined"!==typeof globalThis?globalThis:"undefined"!==typeof self?self:this)._F_toggles=a||[]};(0,_._F_toggles_initialize)([0x19d02c18, 0x1,]);./*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/./*.. SPDX-License-Identifier: Apache-2.0.*/./*. SPDX-License-Identifier: Apache-2.0.*/./*.. Copyright 2024 Google, Inc. SPDX-License-Identifier: MIT.*/.var ja,aaa,la,caa,Ra,Ta,Ua,Wa,Xa,Ya,ab,daa,eaa,gb,ub,zb,Ub,Wb,$b,haa,dc,gc,jaa,oc,qc,rc,xc,Gc,Ic,Bc,Vc,Wc,Xc,maa,kd,naa,nd,md,pd,qd,td,zd,Kd,Od,od,qaa,Zd,saa,taa,Xd,fe,Yd,ye,we,ze,Ae,Ee,He,yaa,zaa,Aaa,Baa,Caa,Daa,Eaa,Faa,uf,yf,Laa,Jaa,Sf,Xf,Oaa,Paa,Zf,mg,Taa,Uaa,Vaa,tg,xg,Waa,Xaa,Yaa,Zaa,$aa,aba,Og,bba,cba,dba,eba,fba,hba,iba,aa,lh,mh,jba,oh,ph,sh,kba,xh,yh,zh,nba,oba,Eh,Fh,pba,qba;_.ba=function(a){return function(){return aa[a].apply(this,arguments)}};_.ca=function(a,b){retur

Chrome Cache Entry: 86

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	383
Entropy (8bit):	4.904593745442369
Encrypted:	false
SSDEEP:	6:tI9mc4slhLJ9hC/vm+QqDChQLcOvQggs70qwSLHvBQSgiBwWj0tijO2o/YocE:t47N9U/vmnqDCGLq/Y0qwSLPsgAtdg1E
MD5:	F4C48C4C1B76585510EC7F53A790737E
SHA1:	F8F55EB42F869C66738ED6CA906EAD4692613B23
SHA-256:	531547B215670051B02E037060CCEA39488BFBF684BBE5827661780E9A1F2F4A
SHA-512:	FBF7D7025AF21AFE01F5934BFD69DCAFB0B950B7D203CECAD81D693E5F7A6EA1CB7D9A52B34327A975BE65BBC97F2EFB513A2235E9BA9F3CED7445C4C74B0BEB
Malicious:	false
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/price_tag_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" enable-background="new 0 0 24 24" height="24" viewBox="0 0 24 24" width="24"><g><path d="M5.02,6.75C4.88,5.93,5.44,5.16,6.25,5.02s1.59,0.41,1.73,1.23c0.14,0.82-0.41,1.59-1.23,1.73 C5.93,8.12,5.16,7.56,5.02,6.75z M3.99,4L4,11.08l9.36,9.36l7.07-7.07l-9.36-9.36L3.99,4 M2.99,3l8.49,0.01l10.36,10.36l-8.49,8.49 L3,11.49L2.99,3L2.99,3z"/></g></svg>

Chrome Cache Entry: 87

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	119
Entropy (8bit):	5.611053133968996
Encrypted:	false
SSDEEP:	3:yionv//thPljll8llb9xtbcO65pqcsfnV5jZAvxYljp:6v/lhPW/zt49qP/2vijp
MD5:	9908E75487306A3B0CECCA499BF2D053
SHA1:	EA6EC8B14254E8C2742FA1730E003930C3D731EB
SHA-256:	42F8AC5554252E21B00B0833E00471C4F99C7DA83457C7992F68D49142B45A60
SHA-512:	B60FDE6D157ED8904DBAFB670C9CE03A359F2912B55B8E3803AD2D0CF94AA30B93D25FDE87ABEDDF0D5F3D1A5A98994917D95ED24A0A4D1DBAC698840791C ABE
Malicious:	false
URL:	http://https://www.gstatic.com/images/icons/material/system/1x/keyboard_arrow_down_white_18dp.png
Preview:	.PNG.....IHDR.....V.W...>IDATx.c..`....?.t9L...I`>... .R.K...i.....0.!d..n.%.-...j.....^..>.H....IEND.B`.

Chrome Cache Entry: 88

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2973)
Category:	downloaded
Size (bytes):	40516
Entropy (8bit):	5.556205286196323
Encrypted:	false
SSDEEP:	768:l3tUvJ8tQzAWsGJQe/6nPKISPJFucFlaV82NAYsMBOQe++W:l3cJNfW
MD5:	EB480EE499CB3D95B613C735D2F3A255
SHA1:	0EC8075DFF42D531FAED3794B18594C26CC64BD7
SHA-256:	D8BB539608F7892076D7CC81983C8C134ADE2ADCABB5D9FC9DBB7D5E3F51FA0C
SHA-512:	EB3442ADB31F49C34D504DFC5C28DA1A7C4268BB531FC3750677342CDB4F1F121237BFC7B652A448CB86BE2936D83E93A36C414BC2BF74FAD7625F385F3EAA F
Malicious:	false
URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/ck=boq-identity.ConsentUi.KIDMQ00cEM4.L.B1.O/am=GCzQWQ/d=1/exm=A7fCU,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,Mlhmy,MpJwZc,Ndreoc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OgOVNe,OmgaI,PHUIyb,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UMu52b,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WpP9Yc,XVMNvd,YTxL4,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,fkuQ3,gychg,hc6Ubd,kWgXee,lsjVmc,lwddkf,m9oV,n73qwf,ovKuLd,pjlCDe,pw70Gc,s39S4,soHxf,vjKJJ,w9hDv,wg1P6b,ws9Tlc,xQtZb,xUdipf,y5vRwf,yDVVkb,ywOR5c,zbML3c,zr1jrb/excm=_b,_tp,mainview/ed=1/wt=2/ujg=1/rs=AOaEmlFxmyZssOHbs21nbssPRY2wW9cOTg/ee=BcQPH:lOY4De;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;vNjB7d:YTxL4;wR5FRb:O1Gjze;xqZiqf:BBI74;yxTchf:KUM7Z;zxnPse:GkRiKb/m=RqjULd"
Preview:	"use strict";this.default_ConsentUi=this.default_ConsentUi||{};(function(_){var window=this;.try{.var Kz;_.Jz=function(a){this.j=a||{cookie:""}};_.h=_.Jz.prototype;_.h.isEnabled=function(){if(!_.da.navigator.cookieEnabled)return!1;if(this.j.cookie)return!0;this.set("TESTCOOKIESENABLED","1",{Ox:60});if("1"!==this.get("TESTCOOKIESENABLED"))return!1;this.remove("TESTCOOKIESENABLED");return!0};_.h.set=function(a,b,c){var d=!1;if("object"===typeof c){var e=c.R2;d=c.pU||!1;var f=c.domain||void 0;var g=c.path||void 0;var k=c.Ox}if(/[;=\s]/.test(a))throw Error("Kb`"+a);if(/[;\r\n]/.test(b))throw Error("Lb`"+b);void 0===k&&(k=-1);c=f?";domain="+f:"";g=g?";path="+g:"";d=d?";secure":"";k=0>k?"":0==k?";expires="+(new Date(1970,1,1)).toUTCString():";expires="+(new Date(Date.now()+1E3*k)).toUTCString();this.j.cookie=a+"="+b+c+g+k+d+(null!=e?";samesite="+e:"")};_.h.get=function(a,b){for(var c=a+"=",d=(this.j.cookie||"").split(";"),e=0,f;e<d.length;e++){f=(0,_.Li)(d[e]);if(0==f.lastIndexOf(c,0))retu

Chrome Cache Entry: 89

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (987)
Category:	downloaded
Size (bytes):	104412
Entropy (8bit):	5.606951048163228
Encrypted:	false
SSDEEP:	1536:BLAbSNYLi786mq3TA3vw8uNAeQDziB8ZDFVYclZrMg8uiG6PqBa:xaSwi2qj0w8uNAdDziBCYcHrMgWF
MD5:	1279C5C5B80DFA58FEC27708B9658965
SHA1:	823E74E967E37FDE523DDD84E6E2CC91D1F259E4
SHA-256:	AEC28A9AFC19E06AA4F9FC4EDC277E769CA3CE5397C33E957C1D157E96218CF9
SHA-512:	0DBA6C75F59FAEF25BDDB30474768380590C7683A4A1950AEC3DBEDE3A27234A07C9B93BC79DC698B8D5E7A6E781E1A750C6BC261248462F0179183D9F4E8F B
Malicious:	false

URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/ck=boq-identity.ConsentUi.KIDMQ00cEM4.L.B1.O/am=GCzQWQ/d=1/exm=A7fCU,BBI74,BVgquf,COQbmf,EEDORb,EFQ78c,GkRiKb,IZT63,JNoxi,KG2eXe,KUM7Z,L1AAkb,LEikZe,MdUzUe,Mlhmy,MpJwZc,NwH0H,O1Gjze,O6y8ed,OTA3Ae,OgOVNe,OmgaI,PrPYRd,QIhFr,RMhBfe,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,VwDzFe,WpP9Yc,XVMNvd,YTxL4,Z5uLle,ZfAoz,ZwDk9d,_b,_tp,aW3pY,aurFic,byfTOb,e5qFLc,fKUV3e,gychg,hc6Ubd,kWgXee,lsjVmc,lwddkf,m9oV,n73qwf,ovKuLd,pjlCDe,pw70Gc,s39S4,vjKJJ,w9hDv,ws9Tlc,xQtZb,xUdipf,y5vRwf,yDVVkb,zbML3c,zr1jrb/excm=_b,_tp,mainview/ed=1/wt=2/ujg=1/rs=AOaEmlFxmyZssOHbs21nbssPRY2wW9cOTg/ee=BcQPH:lOY4De;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;vNjB7d:YTxL4;wR5FRb:O1Gjze;xqZiqf:BBI74;yxTchf:KUM7Z;zxnPse:GkRiKb/m=fkuQ3,soHxf,UMu52b,Ndreoc,wg1P6b,ywOR5c,PHUIyb"
Preview:	"use strict";this.default_ConsentUi=this.default_ConsentUi||{};(function(_){var window=this;.try{._.sja=_.A("fkuQ3",[_.rp,_.Bp,_.Rp]);._.N9=function(a){for(var b=_.Kb.apply(1,arguments),c=[a[0]],d=0;d<b.length;d++)c.push(String(b[d])),c.push(a[d+1]);return new _.vb(c.join(""))};._.O9=function(a){if(!a)return null;a=_.Il(a,3);return null===a||void 0===a?null:new _.vb(a)};._.b$=function(){return"Applying your settings in the background, please wait..."};._.p("fkuQ3");.var w$=function(a){_.M.call(this,a.Ea);this.Yg=a.controller.Yg;this.l=a.controllers.Lx;this.o=a.controllers.qz;this.ze=a.service.ze;this.wb=a.Ya.wb;this.j=a.model.component};_.D(w$,_.M);w$.ya=function(){return{Ya:{wb:_.Dz},controller:{Yg:"lgk6W"},controllers:{Lx:"b3VHJd",qz:"tWT92d"},service:{ze:_.YL},model:{component:_.uB}}};_.h=w$.prototype;_.h.uL=function(){var a=_.UD(_.aE(_.vB(this.j,_.$D)));a=_.O9(a);_.SL(a,"_self");x$(this);return!0};._.h.lW=function(){var a=_.Bl(_.aE(_.vB(this.j,_.$D)),_.wD,1);a=_.O9(a);_.SL(a,"_self"

Chrome Cache Entry: 90

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 18 x 18, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	150
Entropy (8bit):	6.110666861076598
Encrypted:	false
SSDEEP:	3:yionv//thPljll8ll4PLTzhlNREvpvEr/d1heHhdiY9jImj5ESRqq1p:6v/lhPW/4PL7f1eniY9jZEoq0p
MD5:	2DE4479846949DF96020AFFD09DAD6F1
SHA1:	90037C9421C2804CCD320A15976B9CF95E292540
SHA-256:	B2AA4A5ECE0F86DEB2A8FA99BB7F621534025D6F2B6B4E6409B3E71390630CBD
SHA-512:	2EF0477E0BB345E923BC6FEC1931FEC59466F9AD7D39AA37183C8C7F7DB9990EC5B27962D0C54557434C37016163469CF07FE81526B07D422EE8B8BBAEB7948
Malicious:	false
URL:	http://https://www.gstatic.com/images/icons/material/system/1x/keyboard_arrow_down_gm_grey_18dp.png
Preview:	.PNG.....IHDR.....V.W...]IDATx.c..`.844..%..ht..,....l...O..O.....b.....a....,.....0dC.b.0u$.F.!....B.a`C.!.....7}YO[N....IEND.B`.

Chrome Cache Entry: 91

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	148
Entropy (8bit):	5.00574543839908
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5sAR+hHiATcvXjXRHRcBHoNcHaPURR+NFXUwtQoZi:tl9mc4slhohC/vmI4JONW9oZi
MD5:	96D89B10E689D53A3913CF02217751FC
SHA1:	9C76C9797B889A3F7F8964F19828CDFA4E5EAB5A
SHA-256:	28E65C268DBCAB8733E7205BAB86EFC9A758A0D8F2156EDC85D5F810B66007AB
SHA-512:	53889496661D32E3966EBE0421F83CA3CD67C7D32D66CCA22B1F76DE497CDA13E64E16D4FCA68C54EECC302A8E3CC96BCA7FE1BBB0257139E81880C9604EDC74
Malicious:	false
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/bar_graph_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" height="24" viewBox="0 0 24 24" width="24"><path d="M18 13v6h-1v-6h1zm-7-8v14h1V5h-1zM5 9v10h1V9H5z"/></svg>

Chrome Cache Entry: 92

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PNG image data, 24 x 24, 8-bit gray+alpha, non-interlaced
Category:	downloaded
Size (bytes):	137
Entropy (8bit):	5.82162437229304
Encrypted:	false
SSDEEP:	3:yionv//thPlT/Xt1sC9gzFtSVRwoGL4f+hjhaRcPgGjlppp1p:6v/lhPX1d3ViL42lgc5lzp
MD5:	DEA808DFDEDCD3348F3740B2AA9D7011
SHA1:	EC24359379D281E3306C04E929E71FFA3782B618
SHA-256:	968AE4BBCD17CC6A64E4F4E058044A00E3D7F4CE1B1BE6DE9ED3CEE073998334
SHA-512:	4D8C449FA28772125BF21B5EDEE5BAD8A3795A0AD93AEC615C9BDC7DC6D75380AEEA9C0F3B627ABBC74F7154D7901D365664362A925BC19167F809345CDAB9A
Malicious:	false

URL:	http://https://www.gstatic.com/images/icons/material/system/1x/check_white_24dp.png
Preview:	.PNG.....IHDR.....J~.s...PIDAT8.c`.....].G...4....0t..g....8.....J...A.c.7..D..v..(....BR.....#...L.p...x.....IEND.B`.

Chrome Cache Entry: 93	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	203
Entropy (8bit):	5.006827557301702
Encrypted:	false
SSDEEP:	3:tIsqDmJS4RKb5hL6Fb0zVjXRH8+hHiATcvXjXRHRcBHoNcHMFqRJfnwi/LRFzhRv:tI9mc4slhLJ9hC/vmI4Sq7/lZli
MD5:	A8506F49FCB14BE331F65ED4632FF4B1
SHA1:	47113B70522415B856D972BFCFD315AE1D53A45C
SHA-256:	DAB0610E31203CBB462F983D23D0DF56B66F093C13023D6D7FD279A82C3DD2EC
SHA-512:	C4B5C0F43CD6CE5F6DF71190BFE9DB161DC53A3794A33E473C72690E7C4FEA0FCFFCA7D381D7C3468F031115225593C1A8C2C1DF76FB1D7A5C36482E3DBDCB7
Malicious:	false
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/rating_up_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" enable-background="new 0 0 24 24" height="24" viewBox="0 0 24 24" width="24"><path d="M22 6v7h-1V7.6l-8.5 7.6-4-4-5.6 5.6-.7-.7 6.4-6.4 4 4L20.2 7H15V6h7z"/></svg>

Chrome Cache Entry: 94	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines (2353)
Category:	downloaded
Size (bytes):	252270
Entropy (8bit):	5.466158286742454
Encrypted:	false
SSDEEP:	1536:Z+vWG16sQn4L27Mn1MxcoZnU/V5XO1M6v4IScam0NSv9LoRf2r/bJwvHP5qOXcdH:Muq3o4XGu49b3TaFUmcOhK5d
MD5:	9F1412DBD38E538849BFE8D5CE1591DB
SHA1:	3F22540E585CD348CAC3C77EDED7054FF7A24818
SHA-256:	38B841D742281280DC506253B624FE6C7DC50C004C93B671BB3E1FA5094222C7
SHA-512:	2D31681CEA68ED4E45F62DFE2758EC59D489BC455996FD16D7720680DDB281F17926082F3A3437E2011A648490DF8DC2FAD3CF69ED9E26C371A0E75BA49872A
Malicious:	false
URL:	"https://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.ConsentUi.en.ZngcaDHPHhY.es5.O/ck=boq-identity.ConsentUi.KIDMQ00cEM4.L.B1.O/am=GCzQWQ/d=1/exm=_b,_tp/excm=_b,_tp,mainview/ed=1/wt=2/ujg=1/rs=AOaEmlFxmyZssOHbs21nbssPRY2wW9cOTg/ee=BcQPH:lOY4De;EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;vNjB7d:YTxL4;wR5FRb:O1Gjze;xqZiqf:BBI74;yxTchf:KUM7Z;zxnPse:GkRiKb/m=ws9Tlc,n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze,byfTOb,lsjVmc,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,m9oV,vjKJJ,y5vRwf,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwH0H,OmgaI,XVMNvd,L1AAkb,KUM7Z,Mlhmy,WpP9Yc,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,xQtZb,JNoxi,kWgXee,BVgquf,QIhFr,ovKuLd,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,BBI74,VwDzFe,MdUzUe,A7fCU,zbML3c,zr1jrb,YTxL4,Uas9Hd,OgOVNe,pjlCDe"
Preview:	"use strict";_F_installCss(".EDId0c{position:relative}.nhh4lc{position:absolute;left:0;right:0;top:0;z-index:1;pointer-events:none}.nhh4lc[data-state=snapping],.nhh4lc[data-state=cancelled]{transition:transform 200ms}.MGUFnf{display:block;width:28px;height:28px;padding:15px;margin:0 auto;transform:scale(0.7);background-color:#fafafa;border:1px solid #e0e0e0;border-radius:50%;box-shadow:0 2px 2px 0 rgba(0,0,0,.2);transition:opacity 400ms}.nhh4lc[data-state=resting] .MGUFnf,.nhh4lc[data-state=cooldown] .MGUFnf{transform:scale(0);transition:transform 150ms}.nhh4lc .LLCa0e{stroke-width:3.6px;transform:translateZ(1px)}.nhh4lc[data-past-threshold=false] .LLCa0e{opacity:.3}.rOhAxb{fill:#4285f4;stroke:#4285f4}.A6UUqe{display:none;stroke-width:3px;width:28px;height:28px}.tbcVO{width:28px;height:28px}.bQ7oke{position:absolute;width:0;height:0;overflow:hidden}.A6UUqe.qs41qe{animation-name:quantumWizSpinnerRotate;animation-duration:1568.63ms;animation-iteration-count:infinite;animation-timing-func

Chrome Cache Entry: 95	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 15436, version 1.0
Category:	downloaded
Size (bytes):	15436
Entropy (8bit):	7.986311903040136
Encrypted:	false
SSDEEP:	384:uJ/qNyGt74AcZEG+69hFFHDJ1CggakKt0y:+q/kAc+ohFx9YgB2y
MD5:	037D830416495DEF72B7881024C14B7B
SHA1:	619389190B3CAFAFB5DB94113990350ACC8A0278
SHA-256:	1D5B7C64458F4AF91DCFEE0354BE47ADDE1F739B5ADED03A7AB6068A1BB6CA97
SHA-512:	C8D2808945A9BF2E6AD36C7749313467FF390F195448C326C4D4D7A4A635A11E2DDF4D0779BE2DB274F1D1D9D022B1F837294F1E12C9F87E3EAC8A95CFD8872
Malicious:	false

URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
Preview:	wOF2.....<L.....|..;.....d..z..J.`..L.H..<.....e..^...x.6.$..6. ..~. ..).7{...K.. .k~....".v(...[...RE.$..K..C,'..{BK.C&.....'L!...DZ.....+6.r...K..._...<..0..].V.....e.r(RN. 43k;g`...?<?.....b..c.`.. .6..p...5.$zd.R%.....h....";.^WU.....H.....S.j..M:..=K..\B.6"f.....z.....$...%w.?$-....9.:u....u.l..Tt..s.....lY...J.6oN..y...1,l.Yx..lu..}.e...Og..d...Xv.. ...iF.]..x.N..#%,y.&..,*$.^.n...\.K.P.J.x...H$..-.....p.....t.v...gD^....?..6o.....e....,f.)..h...P...<.:.E...X..p....U.?.[m....l.Y.S..p..%..K.,U..3U.qFZo.*...U...3..3.]\.C.#..9T.8P`8..... P...R;..r..J.*...u.j..^vnf.v.... .pw...Z.(.6%$U.[.|....!mU\}./..i,..7D.....:t'.a;.W(.."G....q.-.Z.....;J..0.&/.5. .T.....w..;...t...H.t.<y ..@xx .JA.U.t..;g....@..... .t.....<.5(^.|s..Ko.O.x.... .!.....lHF.....So{.%..V...7..aA$....C;,"(.J..EE..@.....vOB.,V..../....B#.r+./-t.(.N.S...R.Z$4...4i.c.}t...#3`.....s..;.O,.|..W.A.f.w.

Chrome Cache Entry: 96	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	2850
Entropy (8bit):	4.051516722834175
Encrypted:	false
SSDEEP:	48:D3q3faMFAAb13RPHEKc1wjRdaGRjbvazdR4zdR/8nqAdxZvluYZnYWg:DgfaMFAAdRvEKGsP1RPvagn8JVvluYZ+
MD5:	20B87CB3FB34ABB97E6511D77497C24E
SHA1:	9E665DADB7371C9C8B012E2E3E825B36C83C4815
SHA-256:	D64518569E417F44573613D6BC0B2C66B09E45ED686D2D3AE85DC77C0EB4E126
SHA-512:	8AA3840AFED40F078ACF74BF844BBE0A60C7CE47F74E354695043F7B1125FA296F09EAC90C29523624DB7C146B93431B335D1CCB02A460D5FB5529B50BF14A5C
Malicious:	false
URL:	http://https://www.gstatic.com/ac/cb/youtube_logo_v2.svg
Preview:	<svg class="external-icon" viewBox="0 0 200 60" xmlns="http://www.w3.org/2000/svg"><path fill="red" d="M63 14.87a7.885 7.885 0 0 0-5.56-5.56C52.54 8 32.88 8 32.88 8S13.23 8 8.32 9.31c-2.7.72-4.83 2.85-5.56 5.56C1.45 19.77 1.45 30 1.45 30s0 10.23 1.31 15.13c.72 2.7 2.85 4.83 5.56 5.56C13.23 52 32.88 52 32.88 52s19.66 0 24.56-1.31c2.7-.72 4.83-2.85 5.56-5.56C64.31 40.23 64.31 30 64.31 30s0-10.23-1.31-15.13z"/><path fill="#FFF" d="M26.6 39.43 42.93 30 26.6 20.57z"/><g fill="#282828"><path d="M92.69 48.03c-1.24-.84-2.13-2.14-2.65-3.91s-.79-4.12-.79-7.06v-4c0-2.97.3-5.35.9-7.15.6-1.8 1.54-3.11 2.81-3.93 1.27-.82 2.94-1.24 5.01-1.24 2.04 0 3.67.42 4.9 1.26 1.23.84 2.13 2.15 2.7 3.93.57 1.78.85 4.16.85 7.12v4c0 2.94-.28 5.3-.83 7.08-.55 1.78-1.45 3.09-2.7 3.91-1.24.82-2.93 1.24-5.06 1.24-2.18.01-3.9-.41-5.14-1.25zm6.97-4.32c.34-.9.52-2.37.52-4.4v-8.59c0-1.98-.17-3.42-.52-4.34-.34-.91-.95-1.37-1.82-1.37-.84 0-1.43.46-1.78 1.37-.34.91-.52 2.36-.52 4.34v8.59c0 2.04.163.51.49 4.4.33.9.93 1.35 1.

Chrome Cache Entry: 97	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	601
Entropy (8bit):	4.551410752368194
Encrypted:	false
SSDEEP:	12:t47N9U/vmRPpBun/jvWx7OBOoUMiG3HPH8cHKwjSJUNUCQ6UroflOC2Lb:t4jU/viBevSOBOqiO1qQOUeCxU04C2Lb
MD5:	06CA4E01665E02F80E9EB7B7863B4249
SHA1:	EA9347732D4AB9DEC8F98176FF969B591E32E7C3
SHA-256:	542215DA65DE92219030902CF4CD607FBBFDD4824B8A658FF0512201004CCEBC
SHA-512:	F6DE44E685590B5225A004D08C4B66B78154668966D2C13ED23D90E7E3875E61973635763676E6C7A97CF19AFCD3105151E6E9200B0285DB8EE8E2A7F8A27B5C
Malicious:	false
URL:	http://https://fonts.gstatic.com/s/i/short-term/release/youtube_outline/svg/sparkle_24px.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" enable-background="new 0 0 24 24" height="24" viewBox="0 0 24 24" width="24"><path d="M9.91,8.7l0.6,2.12l0.15,0.54l0.54,0.15l2.12,0.6l-2.12,0.6l-0.54,0.15l-0.15,0.54l-0.6,2.12l-0.6-2.12l-0.15-0.54 L8.62,12.7l-2.12-0.6l2.12-0.6l0.54-0.15l0.15-0.54L9.91,8.7 M9.91,5.01l-1.56,5.53L2.83,12.1l5.53,1.56l1.56,5.53l1.56-5.53 L17,12.1l-5.53-1.56L9.91,5.01L9.91,5.01z M16.72,16.81l-2.76,0.78l2.76,0.78l0.78,2.76l0.78-2.76l2.76-0.78l-2.76-0.78l-0.78-2.76 L16.72,16.81z M17.5,2.96l-0.78,2.76L13.96,6.5l2.76,0.78l0.78,2.76l0.78-2.76l2.76-0.78l-2.76-0.78L17.5,2.96z"/></svg>

Chrome Cache Entry: 98	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Web Open Font Format (Version 2), TrueType, length 15552, version 1.0
Category:	downloaded
Size (bytes):	15552
Entropy (8bit):	7.983966851275127
Encrypted:	false
SSDEEP:	384:HDKhlQ8AGL0dgUoEGBQTc7r6QYMkyr/iobA2E4/jKcJZI7lhzi:jslQ+LhUoTB0Qr6Qjkg/DmcJufzi
MD5:	285467176F7FE6BB6A9C6873B3DAD2CC
SHA1:	EA04E4FF5142DDD69307C183DEF721A160E0A64E
SHA-256:	5A8C1E7681318CAA29E9F44E8A6E271F6A4067A2703E9916DFD4FE9099241DB7
SHA-512:	5F9BB763406EA8CE978EC675BD51A0263E9547021EA71188DBD62F0212EB00C1421B750D3B94550B50425BEBFF5F881C41299F6A33BBFA12FB1FF18C12BC7FF1
Malicious:	false

URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Preview:	wOF2.....<.....<Z.....d..z.J.`..L.\..<.....<.....^...x.6.$..6. .... ..S..}%.....\|....x..[j.E...d..-A...]=sjf$X.o.5.....V....i?}.\...;...V.....5..mO=,[.B..d'..=..M...q...8..U'..N..G...[..8....Jp..xP...'.?....}.-.1F.C.....%z..#...Q...~.~..3.....r.Xk..v.*.7t.+bw...f..b...q.W..'E.....O..a..Hl.....Y.B..i.K.0.:.d.E.Lw....Q..~.6.}B...bT.F.,<./....Qu....|...H....Fk.*-..H..p4.$.....{.2.....".T'.....Va.6+.9uv....RW..U$8...p.....H5...B..N..V...{.1....5}p.q6..T...U.P.N...U...!.w..?..ml..8q.}.... >.Z.K.....tq..}.><Ok..w.. ..v....W...{....o...."+#+,..vdt...p.WKK:.p1...3`. 3.....Q.].V.$}.....:.S..bb!l...c.of.2uq.n.MaJ..Cf.....w.$.9C...sj.=...=.Z7...h.w M.D..A.t.....]..GVpL...U(.+.)m..e)..H.}i.o.L...S.r..m..Ko....i..M..J..84.=.....S..@.....Z.V.E..b...0.....@h>...."$.?...../..?.....?.J.a,..|..d...|`.m5..b..LWc...L...?.G.].i...Q..1.:..LJV.J...bU.2.:\.kt.....t.....k....B..i.z+.....A.....

Chrome Cache Entry: 99	
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:wIJct3xIAxG/7nvWDtZcdYLtX7B6QXL3aqG8Q:wIJct+A47v+rcqIBPG9B
MD5:	F3418A443E7D841097C714D69EC4BCB8
SHA1:	49263695F6B0CDD72F45CF1B775E660FDC36C606
SHA-256:	6DA56208801596342l3E197FAFCA1DDE0272153BE3E4590818533FAB8D040770
SHA-512:	82D017C4B7EC8E0C46E8B75DA0CA6A52FD8BCE7FCF4E556CBDF16B49FC81BE9953FE7E25A05F63ECD41C7272E8BB0A9FD9AEDF0AC06CB6032330B096B3702563
Malicious:	false
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.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.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.035579968614001
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	JrE5qsYZD8.exe
File size:	1'166'336 bytes
MD5:	3143cd8f56bf599b3cfddaf9152d445d
SHA1:	33b83cd5d719be2acd908834ce7336d805b35c6a
SHA256:	5f4a7d44b849b744b38f11fbb131743324c84705ec16ae7a1f0789f4f35e49c2
SHA512:	7f2066faa7f687aa984d26837106f6fd09028cc37877906ba1a9a5bb6ea4adc7ad791fee77bac1abcb97916c08eab347c0804f3d8ed3b338fef1b933a1759fdd
SSDEEP:	24576:oqDEvCTbMWu7rQYlBQcBiT6rprG8auh2+b+HdiJUX:oTvC/MTQYxsWR7auh2+b+HoJU
TLSH:	1F45BF027391C062FF9B92734F5AF6115BBC69260123E61F13981DBABE701B1563E7A3
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....j:.....j:..C...j:.....@.*.....n.....~.....{.....{.....{.....z....

File Icon

Icon Hash:	aaf3e3e3938382a0

Static PE Info

General

Entrypoint:	0x420577
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x662A22A8 [Thu Apr 25 09:30:16 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	948cc502fe9226992dce9417f952fce3

Entrypoint Preview

Instruction
call 00007F7D6128D7D3h
jmp 00007F7D6128D0DFh
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F7D6128D2BDh
mov dword ptr [esi], 0049FDF0h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 0049FDF8h
mov dword ptr [ecx], 0049FDF0h
ret
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F7D6128D28Ah
mov dword ptr [esi], 0049FE0Ch
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 0049FE14h
mov dword ptr [ecx], 0049FE0Ch
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 0049FDD0h
and dword ptr [eax], 00000000h
and dword ptr [eax+04h], 00000000h

Instruction
push eax
mov eax, dword ptr [ebp+08h]
add eax, 04h
push eax
call 00007F7D6128FE7Dh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 0049FDD0h
push eax
call 00007F7D6128FEC8h
pop ecx
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 0049FDD0h
push eax
call 00007F7D6128FEB1h
test byte ptr [ebp+08h], 00000001h
pop ecx

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc8e64	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x4617c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x11b000	0x7594	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb0ff0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc3400	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb1010	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9c000	0x894	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x9ab1d	0x9ac00	0a1473f3064dcbc32ef93c5c8a90f3a6	False	0.565500681542811	data	6.668273581389308	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x9c000	0x2fb82	0x2fc00	c9cf2468b60bf4f80f136ed54b3989fb	False	0.35289185209424084	data	5.691811547483722	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xcc000	0x706c	0x4800	53b9025d545d65e23295e30afdbd16d9	False	0.04356553819444445	DOS executable (block device driver @\273\)	0.5846666986982398	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xd4000	0x4617c	0x46200	ceae9781e1202fcb6785525fa0f3aef5	False	0.9065807430926917	data	7.844097112017699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x11b000	0x7594	0x7600	c68ee8931a32d45eb82dc450ee40efc3	False	0.7628111758474576	data	6.7972128181359786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0xd45a8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain	0.7466216216216216
RT_ICON	0xd46d0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128, 16 important colors	English	Great Britain	0.3277027027027027
RT_ICON	0xd47f8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain	0.3885135135135135
RT_ICON	0xd4920	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 0	English	Great Britain	0.3333333333333333
RT_ICON	0xd4c08	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 0	English	Great Britain	0.5
RT_ICON	0xd4d30	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	English	Great Britain	0.2835820895522388
RT_ICON	0xd5bd8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	English	Great Britain	0.37906137184115524
RT_ICON	0xd6480	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	English	Great Britain	0.23699421965317918
RT_ICON	0xd69e8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	English	Great Britain	0.13858921161825727
RT_ICON	0xd8f90	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	English	Great Britain	0.25070356472795496
RT_ICON	0xda038	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	English	Great Britain	0.3173758865248227
RT_MENU	0xda4a0	0x50	data	English	Great Britain	0.9
RT_STRING	0xda4f0	0x594	data	English	Great Britain	0.3333333333333333
RT_STRING	0xdaa84	0x68a	data	English	Great Britain	0.2735961768219833
RT_STRING	0xdb110	0x490	data	English	Great Britain	0.3715753424657534
RT_STRING	0xdb5a0	0x5fc	data	English	Great Britain	0.3087467362924282
RT_STRING	0xdbb9c	0x65c	data	English	Great Britain	0.34336609336609336
RT_STRING	0xdc1f8	0x466	data	English	Great Britain	0.3605683836589698
RT_STRING	0xdc660	0x158	Matlab v4 mat-file (little endian) n, numeric, rows 0, columns 0	English	Great Britain	0.502906976744186
RT_RCDATA	0xdc7b8	0x3d444	data			1.0003427004797807
RT_GROUP_ICON	0x119bfc	0x76	data	English	Great Britain	0.6610169491525424
RT_GROUP_ICON	0x119c74	0x14	data	English	Great Britain	1.25
RT_GROUP_ICON	0x119c88	0x14	data	English	Great Britain	1.15
RT_GROUP_ICON	0x119c9c	0x14	data	English	Great Britain	1.25
RT_VERSION	0x119cb0	0xdc	data	English	Great Britain	0.6181818181818182
RT_MANIFEST	0x119d8c	0x3ef	ASCII text, with CRLF line terminators	English	Great Britain	0.5074478649453823

Imports

DLL	Import
WSOCK32.dll	gethostbyname, recv, send, socket, inet_ntoa, setsockopt, ntohs, WSACleanup, WSAStartup, sendto, htons, __WSAFDIsSet, select, accept, listen, bind, inet_addr, ioctlsocket, recvfrom, WSAGetLastError, closesocket, gethostname, connect

DLL	Import
VERSION.dll	GetFileVersionInfoW, VerQueryValueW, GetFileVersionInfoSizeW
WINMM.dll	timeGetTime, waveOutSetVolume, mciSendStringW
COMCTL32.dll	ImageList_ReplaceIcon, ImageList_Destroy, ImageList_Remove, ImageList_SetDragCursorImage, ImageList_BeginDrag, ImageList_DragEnter, ImageList_DragLeave, ImageList_EndDrag, ImageList_DragMove, InitCommonControlsEx, ImageList_Create
MPR.dll	WNetGetConnectionW, WNetCancelConnection2W, WNetUseConnectionW, WNetAddConnection2W
WININET.dll	HttpOpenRequestW, InternetCloseHandle, InternetOpenW, InternetSetOptionW, InternetCrackUrlW, HttpQueryInfoW, InternetQueryOptionW, InternetConnectW, HttpSendRequestW, FtpOpenFileW, FtpGetFileSize, InternetOpenUrlW, InternetReadFile, InternetQueryDataAvailable
PSAPI.DLL	GetProcessMemoryInfo
IPHLPAPI.DLL	IcmpSendEcho, IcmpCloseHandle, IcmpCreateFile
USERENV.dll	DestroyEnvironmentBlock, LoadUserProfileW, CreateEnvironmentBlock, UnloadUserProfile
UxTheme.dll	IsThemeActive
KERNEL32.dll	DuplicateHandle, CreateThread, WaitForSingleObject, HeapAlloc, GetProcessHeap, HeapFree, Sleep, GetCurrentThreadId, MultiByteToWideChar, MulDiv, GetVersionExW, IsWow64Process, GetSystemInfo, FreeLibrary, LoadLibraryA, GetProcAddress, SetErrorMode, GetModuleFileNameW, WideCharToMultiByte, lstrcpyW, lstrlenW, GetModuleHandleW, QueryPerformanceCounter, VirtualFreeEx, OpenProcess, VirtualAllocEx, WriteProcessMemory, ReadProcessMemory, CreateFileW, SetFilePointerEx, SetEndOfFile, ReadFile, WriteFile, FlushFileBuffers, TerminateProcess, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, SetFileTime, GetFileAttributesW, FindFirstFileW, FindClose, GetLongPathNameW, GetShortPathNameW, DeleteFileW, IsDebuggerPresent, CopyFileExW, MoveFileW, CreateDirectoryW, RemoveDirectoryW, SetSystemPowerState, QueryPerformanceFrequency, LoadResource, LockResource, SizeofResource, OutputDebugStringW, GetTempPathW, GetTempFileNameW, DeviceIoControl, LoadLibraryW, GetLocalTime, CompareStringW, GetCurrentThread, EnterCriticalSection, LeaveCriticalSection, GetStdHandle, CreatePipe, InterlockedExchange, TerminateThread, LoadLibraryExW, FindResourceExW, CopyFileW, VirtualFree, FormatMessageW, GetExitCodeProcess, GetPrivateProfileStringW, WritePrivateProfileStringW, GetPrivateProfileSectionW, WritePrivateProfileSectionW, GetPrivateProfileSectionNamesW, FileTimeToLocalFileTime, FileTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, GetDriveTypeW, GetDiskFreeSpaceExW, GetDiskFreeSpaceW, GetVolumeInformationW, SetVolumeLabelW, CreateHardLinkW, SetFileAttributesW, CreateEventW, SetEvent, GetEnvironmentVariableW, SetEnvironmentVariableW, GlobalLock, GlobalUnlock, GlobalAlloc, GetFileSize, GlobalFree, GlobalMemoryStatusEx, Beep, GetSystemDirectoryW, HeapReAlloc, HeapSize, GetComputerNameW, GetWindowsDirectoryW, GetCurrentProcessId, GetProcessIoCounters, CreateProcessW, GetProcessId, SetPriorityClass, VirtualAlloc, GetCurrentDirectoryW, lstrcmpiW, DecodePointer, GetLastError, RaiseException, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, InterlockedDecrement, InterlockedIncrement, ResetEvent, WaitForSingleObjectEx, IsProcessorFeaturePresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, CloseHandle, GetFullPathNameW, GetStartupInfoW, GetSystemTimeAsFileTime, InitializeSListHead, RtlUnwind, SetLastError, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, EncodePointer, ExitProcess, GetModuleHandleExW, ExitThread, ResumeThread, FreeLibraryAndExitThread, GetACP, GetDateFormatW, GetTimeFormatW, LCMapStringW, GetStringTypeW, GetFileType, SetStdHandle, GetConsoleCP, GetConsoleMode, ReadConsoleW, GetTimeZoneInformation, FindFirstFileExW, IsValidCodePage, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableA, SetCurrentDirectoryW, FindNextFileW, WriteConsoleW
USER32.dll	GetKeyboardLayoutNameW, IsCharAlphaW, IsCharAlphaNumericW, IsCharLowerW, IsCharUpperW, GetMenuStringW, GetSubMenu, GetCaretPos, IsZoomed, GetMonitorInfoW, SetWindowLongW, SetLayeredWindowAttributes, FlashWindow, GetClassLongW, TranslateAcceleratorW, IsDialogMessageW, GetSysColor, InflateRect, DrawFocusRect, DrawTextW, FrameRect, DrawFrameControl, FillRect, PtInRect, DestroyAcceleratorTable, CreateAcceleratorTableW, SetCursor, GetWindowDC, GetSystemMetrics, GetActiveWindow, CharNextW, wsprintfW, RedrawWindow, DrawMenuBar, DestroyMenu, SetMenu, GetWindowTextLengthW, CreateMenu, IsDlgButtonChecked, DefDlgProcW, CallWindowProcW, ReleaseCapture, SetCapture, PeekMessageW, GetInputState, UnregisterHotKey, CharLowerBuffW, MonitorFromPoint, MonitorFromRect, LoadImageW, mouse_event, ExitWindowsEx, SetActiveWindow, FindWindowExW, EnumThreadWindows, SetMenuDefaultItem, InsertMenuItemW, IsMenu, ClientToScreen, GetCursorPos, DeleteMenu, CheckMenuRadioItem, GetMenuItemID, GetMenuItemCount, SetMenuItemInfoW, GetMenuItemInfoW, SetForegroundWindow, IsIconic, FindWindowW, SystemParametersInfoW, LockWindowUpdate, SendInput, GetAsyncKeyState, SetKeyboardState, GetKeyboardState, GetKeyState, VkKeyScanW, LoadStringW, DialogBoxParamW, MessageBeep, EndDialog, SendDlgItemMessageW, GetDlgItem, SetWindowTextW, CopyRect, ReleaseDC, GetDC, EndPaint, BeginPaint, GetClientRect, GetMenu, DestroyWindow, EnumWindows, GetDesktopWindow, IsWindow, IsWindowEnabled, IsWindowVisible, EnableWindow, InvalidateRect, GetWindowLongW, GetWindowThreadProcessId, AttachThreadInput, GetFocus, GetWindowTextW, SendMessageTimeoutW, EnumChildWindows, CharUpperBuffW, GetClassNameW, GetParent, GetDlgCtrlID, SendMessageW, MapVirtualKeyW, PostMessageW, GetWindowRect, SetUserObjectSecurity, CloseDesktop, CloseWindowStation, OpenDesktopW, RegisterHotKey, GetCursorInfo, SetWindowPos, CopyImage, AdjustWindowRectEx, SetRect, SetClipboardData, EmptyClipboard, CountClipboardFormats, CloseClipboard, GetClipboardData, IsClipboardFormatAvailable, OpenClipboard, BlockInput, TrackPopupMenuEx, GetMessageW, SetProcessWindowStation, GetProcessWindowStation, OpenWindowStationW, GetUserObjectSecurity, MessageBoxW, DefWindowProcW, MoveWindow, SetFocus, PostQuitMessage, KillTimer, CreatePopupMenu, RegisterWindowMessageW, SetTimer, ShowWindow, CreateWindowExW, RegisterClassExW, LoadIconW, LoadCursorW, GetSysColorBrush, GetForegroundWindow, MessageBoxA, DestroyIcon, DispatchMessageW, keybd_event, TranslateMessage, ScreenToClient
GDI32.dll	EndPath, DeleteObject, GetTextExtentPoint32W, ExtCreatePen, StrokeAndFillPath, GetDeviceCaps, SetPixel, CloseFigure, LineTo, AngleArc, MoveToEx, Ellipse, CreateCompatibleBitmap, CreateCompatibleDC, PolyDraw, BeginPath, Rectangle, SetViewportOrgEx, GetObjectW, SetBkMode, RoundRect, SetBkColor, CreatePen, SelectObject, StretchBlt, CreateSolidBrush, SetTextColor, CreateFontW, GetTextFaceW, GetStockObject, CreateDCW, GetPixel, DeleteDC, GetDIBits, StrokePath
COMDLG32.dll	GetSaveFileNameW, GetOpenFileNameW

DLL	Import
ADVAPI32.dll	GetAce, RegEnumValueW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyExW, RegSetValueExW, RegOpenKeyExW, RegCloseKey, RegQueryValueExW, RegConnectRegistryW, InitializeSecurityDescriptor, InitializeAcl, AdjustTokenPrivileges, OpenThreadToken, OpenProcessToken, LookupPrivilegeValueW, DuplicateTokenEx, CreateProcessAsUserW, CreateProcessWithLogonW, GetLengthSid, CopySid, LogonUserW, AllocateAndInitializeSid, CheckTokenMembership, FreeSid, GetTokenInformation, RegCreateKeyExW, GetSecurityDescriptorDacl, GetAclInformation, GetUserNameW, AddAce, SetSecurityDescriptorDacl, InitiateSystemShutdownExW
SHELL32.dll	DragFinish, DragQueryPoint, ShellExecuteExW, DragQueryFileW, SHEmptyRecycleBinW, SHGetPathFromIDListW, SHBrowseForFolderW, SHCreateShellItem, SHGetDesktopFolder, SHGetSpecialFolderLocation, SHGetFolderPathW, SHFileOperationW, ExtractIconExW, Shell_NotifyIconW, ShellExecuteW
ole32.dll	CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, ProgIDFromCLSID, CLSIDFromProgID, OleSetMenuDescriptor, MkParseDisplayName, OleSetContainedObject, CoCreateInstance, IIDFromString, StringFromGUID2, CreateStreamOnHGlobal, OleInitialize, OleUninitialize, CoInitialize, CoUninitialize, GetRunningObjectTable, CoGetInstanceFromFile, CoGetObject, CoInitializeSecurity, CoCreateInstanceEx, CoSetProxyBlanket
OLEAUT32.dll	CreateStdDispatch, CreateDispTypeInfo, UnRegisterTypeLib, UnRegisterTypeLibForUser, RegisterTypeLibForUser, RegisterTypeLib, LoadTypeLibEx, VariantCopyInd, SysReAllocString, SysFreeString, VariantChangeType, SafeArrayDestroyData, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayAllocData, SafeArrayAllocDescriptorEx, SafeArrayCreateVector, SysStringLen, QueryPathOfRegTypeLib, SysAllocString, VariantInit, VariantClear, DispCallFunc, VariantTimeToSystemTime, VarR8FromDec, SafeArrayGetVartype, SafeArrayDestroyDescriptor, VariantCopy, OleLoadPicture

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Network Behavior

Network Port Distribution

Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 15:50:49.250514030 CEST	49673	443	192.168.2.6	173.222.162.64
May 8, 2024 15:50:49.250516891 CEST	49674	443	192.168.2.6	173.222.162.64
May 8, 2024 15:50:49.578679085 CEST	49672	443	192.168.2.6	173.222.162.64
May 8, 2024 15:50:53.420118093 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.420146942 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.420213938 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.420655966 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.420667887 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.756967068 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.757277012 CEST	49705	443	192.168.2.6	142.251.33.78

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 15:50:53.757297993 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.757700920 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.757858992 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.758414030 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.758466959 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.759371042 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.759430885 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.759542942 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.800122976 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.813519001 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:53.813530922 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:53.860759020 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.123188972 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.123330116 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.123395920 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.123411894 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.123595953 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.131777048 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.136140108 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.140578032 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.143635988 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.151976109 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.154233932 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.163394928 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.165956974 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.174912930 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.174942970 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.175086021 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.175096989 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.175451994 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.186371088 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.186451912 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.285031080 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.287072897 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.290613890 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.290657997 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.290671110 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.290678978 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.290723085 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.302135944 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.302207947 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.313661098 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.313889027 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.325058937 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.325093031 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.325294018 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.325303078 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.327366114 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.336546898 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.336627007 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.347995996 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.348064899 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.348077059 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.359431982 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.360019922 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.360028028 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.370912075 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.371372938 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.371381044 CEST	443	49705	142.251.33.78	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 15:50:54.382405043 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.383390903 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.383395910 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.398082018 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.398111105 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.398142099 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.398158073 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.398667097 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.408628941 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.419107914 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.419137001 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.419167042 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.419177055 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.421365023 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.429583073 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.440160036 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.440187931 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.440373898 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.440382957 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.441459894 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.450597048 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.458710909 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.458745956 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.459750891 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.459760904 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.465356112 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.466406107 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.473659039 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.473701954 CEST	443	49705	142.251.33.78	192.168.2.6
May 8, 2024 15:50:54.476710081 CEST	49705	443	192.168.2.6	142.251.33.78
May 8, 2024 15:50:54.476733923 CEST	443	49705	142.251.33.78	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 15:50:52.340811014 CEST	61024	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:52.348773956 CEST	49195	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:52.505469084 CEST	53	61024	1.1.1.1	192.168.2.6
May 8, 2024 15:50:52.513747931 CEST	53	49195	1.1.1.1	192.168.2.6
May 8, 2024 15:50:52.517348051 CEST	53	50694	1.1.1.1	192.168.2.6
May 8, 2024 15:50:52.520128965 CEST	53	60207	1.1.1.1	192.168.2.6
May 8, 2024 15:50:53.232675076 CEST	59374	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:53.232878923 CEST	59097	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:53.403157949 CEST	53	59097	1.1.1.1	192.168.2.6
May 8, 2024 15:50:53.419620037 CEST	53	59374	1.1.1.1	192.168.2.6
May 8, 2024 15:50:53.695355892 CEST	53	54953	1.1.1.1	192.168.2.6
May 8, 2024 15:50:55.002048969 CEST	53	57436	1.1.1.1	192.168.2.6
May 8, 2024 15:50:55.003134012 CEST	53	51779	1.1.1.1	192.168.2.6
May 8, 2024 15:50:55.846317053 CEST	53	59334	1.1.1.1	192.168.2.6
May 8, 2024 15:50:56.495716095 CEST	58631	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:56.495851994 CEST	60395	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:56.658179045 CEST	53	58631	1.1.1.1	192.168.2.6
May 8, 2024 15:50:56.658468962 CEST	53	60395	1.1.1.1	192.168.2.6
May 8, 2024 15:50:57.038067102 CEST	53	51909	1.1.1.1	192.168.2.6
May 8, 2024 15:50:59.516068935 CEST	53285	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:59.516773939 CEST	61337	53	192.168.2.6	1.1.1.1
May 8, 2024 15:50:59.682924986 CEST	53	53285	1.1.1.1	192.168.2.6
May 8, 2024 15:50:59.683603048 CEST	53	61337	1.1.1.1	192.168.2.6
May 8, 2024 15:51:10.692768097 CEST	53	50673	1.1.1.1	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 8, 2024 15:51:29.518414974 CEST	55365	53	192.168.2.6	1.1.1.1
May 8, 2024 15:51:29.518583059 CEST	51242	53	192.168.2.6	1.1.1.1
May 8, 2024 15:51:29.681087971 CEST	53	55365	1.1.1.1	192.168.2.6
May 8, 2024 15:51:29.681231022 CEST	53	51242	1.1.1.1	192.168.2.6
May 8, 2024 15:51:29.732002974 CEST	53	57549	1.1.1.1	192.168.2.6
May 8, 2024 15:51:51.883784056 CEST	53	56813	1.1.1.1	192.168.2.6
May 8, 2024 15:51:52.105643034 CEST	53	61748	1.1.1.1	192.168.2.6
May 8, 2024 15:52:01.378365040 CEST	65130	53	192.168.2.6	1.1.1.1
May 8, 2024 15:52:01.378546000 CEST	65502	53	192.168.2.6	1.1.1.1
May 8, 2024 15:52:01.543975115 CEST	53	65130	1.1.1.1	192.168.2.6
May 8, 2024 15:52:01.549249887 CEST	53	65502	1.1.1.1	192.168.2.6
May 8, 2024 15:52:19.914638996 CEST	53	62637	1.1.1.1	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 8, 2024 15:50:52.340811014 CEST	192.168.2.6	1.1.1.1	0x6435	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.348773956 CEST	192.168.2.6	1.1.1.1	0x9dc0	Standard query (0)	www.youtube.com	65	IN (0x0001)	false
May 8, 2024 15:50:53.232675076 CEST	192.168.2.6	1.1.1.1	0x6408	Standard query (0)	consent.youtube.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:53.232878923 CEST	192.168.2.6	1.1.1.1	0x4614	Standard query (0)	consent.youtube.com	65	IN (0x0001)	false
May 8, 2024 15:50:56.495716095 CEST	192.168.2.6	1.1.1.1	0x6142	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:56.495851994 CEST	192.168.2.6	1.1.1.1	0xd132	Standard query (0)	www.google.com	65	IN (0x0001)	false
May 8, 2024 15:50:59.516068935 CEST	192.168.2.6	1.1.1.1	0x8029	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:59.516773939 CEST	192.168.2.6	1.1.1.1	0x7239	Standard query (0)	www.google.com	65	IN (0x0001)	false
May 8, 2024 15:51:29.518414974 CEST	192.168.2.6	1.1.1.1	0xabad	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:51:29.518583059 CEST	192.168.2.6	1.1.1.1	0x1fde	Standard query (0)	play.google.com	65	IN (0x0001)	false
May 8, 2024 15:52:01.378365040 CEST	192.168.2.6	1.1.1.1	0x8196	Standard query (0)	consent.youtube.com	A (IP address)	IN (0x0001)	false
May 8, 2024 15:52:01.378546000 CEST	192.168.2.6	1.1.1.1	0x4aec	Standard query (0)	consent.youtube.com	65	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.250.69.206	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.251.215.238	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.250.217.110	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.251.33.78	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		172.217.14.206	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.251.211.238	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		172.217.14.238	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.251.33.110	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.505469084 CEST	1.1.1.1	192.168.2.6	0x6435	No error (0)	youtube-ui.l.google.com		142.250.217.78	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:52.513747931 CEST	1.1.1.1	192.168.2.6	0x9dc0	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
May 8, 2024 15:50:52.513747931 CEST	1.1.1.1	192.168.2.6	0x9dc0	No error (0)	youtube-ui.l.google.com			65	IN (0x0001)	false
May 8, 2024 15:50:53.419620037 CEST	1.1.1.1	192.168.2.6	0x6408	No error (0)	consent.youtube.com		142.251.33.78	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:56.658179045 CEST	1.1.1.1	192.168.2.6	0x6142	No error (0)	www.google.com		142.251.215.228	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:56.658468962 CEST	1.1.1.1	192.168.2.6	0xd132	No error (0)	www.google.com			65	IN (0x0001)	false
May 8, 2024 15:50:59.682924986 CEST	1.1.1.1	192.168.2.6	0x8029	No error (0)	www.google.com		142.251.215.228	A (IP address)	IN (0x0001)	false
May 8, 2024 15:50:59.683603048 CEST	1.1.1.1	192.168.2.6	0x7239	No error (0)	www.google.com			65	IN (0x0001)	false
May 8, 2024 15:51:29.681087971 CEST	1.1.1.1	192.168.2.6	0xabad	No error (0)	play.google.com		142.251.215.238	A (IP address)	IN (0x0001)	false
May 8, 2024 15:52:01.543975115 CEST	1.1.1.1	192.168.2.6	0x8196	No error (0)	consent.youtube.com		142.251.33.78	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- consent.youtube.com
- fs.microsoft.com
- https:
  - www.google.com
  - play.google.com
- slscr.update.microsoft.com

HTTPS Connections

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 8, 2024 15:51:10.155211926 CEST	173.222.162.64	443	192.168.2.6	49698	CN=r.bing.com, O=Microsoft Corporation, L=Redmond, ST=WA, C=US CN=Microsoft Azure ECC TLS Issuing CA 05, O=Microsoft Corporation, C=US	CN=Microsoft Azure ECC TLS Issuing CA 05, O=Microsoft Corporation, C=US CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Oct 18 22:32:40 CEST 2023	Fri Jun 28 01:59:59 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-16-23-65281,29-23-24,0	28a2c9bd18a11de089ef85a160da29e4
					CN=Microsoft Azure ECC TLS Issuing CA 05, O=Microsoft Corporation, C=US	CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Aug 12 02:00:00 CEST 2020	Fri Jun 28 01:59:59 CEST 2024		

Statistics

Behavior

Click to jump to process

System Behavior

All data are 0.

Disassembly

No disassembly